Palo Alto Networks Certified Cybersecurity Entry Level Technician (PCCET)

Study Guide

June 2022

Table of Contents

How to Use This Study Guide 2
About the PCCET Exam 2
Exam Format 2
How to Take This Exam 3
Disclaimer 3
Audience and Qualifications 3
Skills Required 3
Recommended Training 3
Domain 1: Fundamentals Of Cybersecurity 3
1.1 Distinguish between Web 2.0 and 3.0 applications and services 4
1.1.1 References 12
1.2 Describe port-scanning methodologies and their impact 12
1.2.1 Non-standard ports 12
1.2.2 Identify applications by their port number 12
1.2.3 References 13
1.3 Recognize applications used to circumvent port-based firewalls 13
1.3.1 References 14
1.4 Differentiate between common cloud computing service models 14
1.4.1 SaaS 14
1.4.2 PaaS 15
1.4.3 IaaS 15
1.4.4 References 15
1.5 Describe the business processes of supply-chain management 15
1.5.1 References 16
1.6 Describe the vulnerabilities associated with data being stored in the SaaS environment 16
1.6.1 Describe roles within a SaaS environment 17
1.6.2 Describe security controls for SaaS applications 17
1.6.3 References 18
1.7 Describe the impact of governance, regulation, and compliance 18
1.7.1 Differentiate between compliance and security 18
1.7.2 Identify major cybersecurity laws and their implications 19
1.7.3 References 21
1.8 Describe the tactics of the MITRE ATT&CK framework 21
1.8.1 Identify a leading indicator of a compromise 22
1.8.2 Describe how to use CVE 22
1.8.3 Describe how to use CVS 23
1.8.4 References 23
1.9 Identify the different attacker profiles and motivations 24
1.9.1 Describe the different value levels of the information that need protection (political, financial, etc.) 24
1.9.2 References 24

1.10 Describe the different phases and events of the cyberattack lifecycle **25**
1.10.1 Describe the purpose of command and control (C2) 28
1.10.2 References 29
1.11 Identify the characteristics, capabilities, and appropriate actions for different types of malware and ransomware **29**
1.12 Differentiate between vulnerabilities and exploits **32**
1.12.1 Differentiate between various business email compromise attacks 33
1.12.2 Identify different methodologies for social engineering 34
1.12.3 Identify the chain of events that result from social engineering 34
1.12.4 References 34
1.13 Identify what chain of events follows an attack **35**
1.13.1 References 35
1.14 Differentiate between the functional aspects of bots and botnets **35**
1.14.1 Describe the type of IoT devices that are part of a botnet attack 35
1.14.2 References 39
1.15 Differentiate the TCP/IP roles in DDoS attacks **39**
1.15.1 Differentiate between DoS and DDoS 39
1.15.2 References 42
1.16 Describe advanced persistent threats **42**
1.16.1 References 43
1.17 Describe risks with Wi-Fi networks **44**
1.17.1 Differentiate between common types of Wi-Fi attacks 44
1.17.2 Describe how to monitor your Wi-Fi network 46
1.17.3 References 49
1.18 Describe perimeter-based network security **50**
1.18.1 Identify the types of devices used in perimeter defense 50
1.19 Describe the Demilitarized Zone (DMZ) **51**
1.20 Describe the transition from a trusted network to an untrusted network **52**
1.20.1 Differentiate between North-South and East-West zones 53
1.20.2 References 53
1.21 Describe Zero Trust **53**
1.21.1 Identify the benefits of the Zero Trust model 54
1.21.2 Identify the design principles for Zero Trust 54
1.21.3 Describe a microperimeter 54
1.21.4 Differentiate between Trust and Untrust zones 55
1.21.5 References 55
1.22 Describe the integration of services for network, endpoint, and cloud **55**
1.22.1 References 58
1.23 Identify the capabilities of an effective Security Operating Platform **58**
1.23.1 Describe the components of the Security Operating Platform 59
1.23.2 References 60
1.24 Summary of key ideas **60**
Domain 2 Network Security Components **61**

2.1 Differentiate between hubs, switches, and routers **61**
2.1.1 Given a network diagram, identify the icons for hubs, switches, and routers 62
2.1.2 References 62
2.2 Describe the use of VLANs **62**
2.3 Differentiate between routed and routing protocols **62**
2.4 Differentiate between static and dynamic routing protocols **62**
2.4.1 Differentiate between link state and distance vector 63
2.5 Identify the borders of collision and broadcast domains **65**
2.6 Differentiate between different types of area networks **65**
2.6.1 WAN 65
2.6.2 LAN 65
2.7 Describe the advantages of SD-WAN **66**
2.8 Describe the purpose of the Domain Name System (DNS) **68**
2.8.1 Describe how DNS record types are used 68
2.8.2 Identify a fully qualified domain name (FQDN) 69
2.8.3 Describe the DNS hierarchy 69
2.9 Differentiate between categories of IoT devices **70**
2.9.1 Identify the known security risks and solutions associated with IoT 72
2.9.1 References 74
2.10 Identify IoT connectivity technologies **74**
2.11 Differentiate between IPv4 and IPv6 addresses **75**
2.11.1 Describe binary-to-decimal conversion 75
2.11.2 Describe IPv4 CIDR notation 76
2.11.3 Describe IPv4 classful subnetting 76
2.11.4 Given a scenario, identify the proper subnet mask 77
2.11.5 Describe the purpose of subnetting 77
2.11.6 Describe the structure of IPv4 and IPv6 77
2.11.7 Describe the purpose of IPv4 and IPv6 addressing 78
2.12 Describe the purpose of a default gateway **82**
2.13 Describe the role of NAT **83**
2.14 Describe OSI and TCP/IP models **83**
2.14.1 Identify the order of the layers of both OSI and TCP/IP models 83
2.14.2 Compare the similarities of some OSI and TCP/IP layers 84
2.14.3 Identify the protocols and functions of each OSI layer 84
2.15 Describe the data-encapsulation process **88**
2.15.1 Describe the PDU format used at different layers 88
2.16 Identify the characteristics of various types of network firewalls **89**
2.16.1 Traditional firewalls 89
2.16.2 Next-generation firewalls 89
2.16.3 Differentiate between NGFWs and traditional firewalls 90
2.17 Describe the application of NGFW deployment options (i.e., PA-,VM- and CN-Series) **91**
2.18 Differentiate between intrusion detection systems and intrusion prevention systems **92**
2.18.1 Differentiate between knowledge-based and behavior-based systems 93

2.18.2 References 93
2.19 Describe virtual private networks 93
2.19.1 Describe when to use VPNs 93
2.20 Differentiate between the different tunneling protocols 93
2.21 Describe the purpose of data loss prevention 97
2.21.1 Classify different types of data (e.g., sensitive, inappropriate) 98
2.21.2 References 99
2.22 Differentiate the various types of security functions from those integrated into UTM devices 99
2.23 Describe endpoint security standards 99
2.23.1 Describe the advantages of endpoint security 100
2.23.2 Describe host-based intrusion detection/prevention systems 100
2.23.3 Differentiate between signature-based and behavioral-based malware protection 101
2.23.4 Describe application block and allow listing 103
2.23.5 Describe the concepts of false-positive and false-negative alerts 104
2.23.6 Describe the purpose of anti-spyware software 104
2.23.7 Reference 104
2.24 Identify differences in managing wireless devices compared to other endpoint devices 105
2.25 Describe the purpose of identity and access management 105
2.25.1 Single- and Multi-factor authentication 106
2.25.2 Separation of duties and impact on privileges 107
2.25.3 RBAC, ABAC, DAC, and MAC 107
2.25.4 User profiles 108
2.25.5 References 108
2.26 Describe the integration of NGFWs with the cloud, networks, and Endpoints 108
2.27 Describe App-ID, User-ID, and Content-ID 109
2.28 Describe Palo Alto Networks firewall subscription services 117
2.28.1 WildFire 117
2.28.2 URL Filtering 120
2.28.3 Threat Prevention 121
2.28.4 DNS Security 121
2.28.5 IoT Security 122
2.28.6 SD-WAN 123
2.28.7 Advanced Threat Prevention 124
2.28.8 Advanced URL Filtering 124
2.28.9 GlobalProtect 124
2.28.10 Enterprise DLP 126
2.28.11 SaaS Security Inline 127
2.28.12 Virtual Systems 128
2.28.13 References 128
2.29 Describe network security management 129
2.29.1 Identify the deployment modes of Panorama 129
2.29.2 Describe the three components of Best Practice Assessment (BPA) 130

2.29.3 References 130
2.30 Summary of key ideas 130
Domain 3: Cloud Technologies 130
3.1 Describe the NIST cloud service and deployment models 130
3.2 Recognize and list cloud security challenges 132
3.2.1 Describe the vulnerabilities in a shared community environment 132
3.2.2 Describe cloud security responsibilities 132
3.2.3 Describe cloud multitenancy 138
3.2.4 Differentiate between security tools in various cloud environments 139
3.2.5 Describe identity and access management controls for cloud resources 140
3.2.6 Describe different types of cloud security alerts and notifications 141
3.2.7 Reference 141
3.3 Identify the four Cs of cloud native security 141
3.4 Describe the purpose of virtualization in cloud computing 146
3.4.1 Describe the types of hypervisors 146
3.4.2 Describe characteristics of various cloud providers 146
3.4.3 Describe economic benefits of cloud computing and virtualization 146
3.4.4 Describe the security implications of virtualization 147
3.4.5 Reference 147
3.5 Explain the purpose of containers in application deployment 147
3.5.1 Differentiate containers versus virtual machines 147
3.5.2 Describe Container as a Service 148
3.5.3 Differentiate a hypervisor from a Docker Container 149
3.5.4 Reference 149
3.6 Describe how serverless computing is used 149
3.7 Describe DevOps 150
3.8 Describe DevSecOps 151
3.9 Illustrate the continuous integration/continuous delivery pipeline 151
3.10 Explain governance and compliance related to deployment of SaaS applications 151
3.10.1 Describe security compliance to protect data 151
3.10.2 Describe privacy regulations globally 153
3.10.3 Describe security compliance between local policies and SaaS Applications 153
3.11 Describe the cost of maintaining a physical data center 154
3.11.1 References 155
3.12 Differentiate between data-center security weaknesses of traditional solutions versus cloud environments 155
3.13 Differentiate between east-west and north-south traffic patterns 156
3.14 Describe the four phases of hybrid data-center security 158
3.15 Describe how data centers can transform their operations incrementally 160
3.16 Describe the cloud-native security platform 160
3.17 Identify the four pillars of Prisma Cloud application security 163
3.18 Describe the concept of SASE 163
3.19 Describe the SASE layer 164

3.19.1 Describe sanctioned, tolerated, and unsanctioned SaaS applications 171
3.19.2 List how to control sanctioned SaaS usage 173
3.20 Describe the network-as-a-service layer 174
3.21 Describe how Prisma Access provides traffic protection 174
3.21 Reference 174
3.22 Describe Prisma Cloud Security Posture Management (CSPM) 174
3.22 Reference 177
3.23 Summary of key ideas 177
Domain 4: Elements of Security Operations 177
4.1 Describe the main elements included in the development of SOC business objectives 177
4.1.1 Reference 178
4.2 Describe the components of SOC business management and operations 178
4.3 List the six essential pillars of effective security operations 181
4.3.1 References 183
4.4 Describe the four SecOps functions 183
4.4.1 Identify 183
4.4.2 Investigate 184
4.4.3 Mitigate 184
4.4.4 Improve 185
4.5 Describe SIEM 186
4.5.1 References 187
4.6 Describe the purpose of security orchestration, automation, and response (SOAR) 187
4.6.1 References 190
4.7 Describe the analysis tools used to detect evidence of a security compromise 190
4.8 Describe how to collect security data for analysis 190
4.9 Describe the use of analysis tools within a security operations environment 192
4.9.1 References 193
4.10 Describe the responsibilities of a security operations engineering team 193
4.11 Describe the Cortex platform in a security operations environment and the purpose of Cortex XDR for various endpoints 194
4.11.1 References 195
4.12 Describe how Cortex XSOAR improves security operations efficiency 195
4.13 Describe how Cortex Data Lake improves security operations visibility 195
4.14 Describe how XSIAM can be used to accelerate SOC threat response 196
4.14.1 References 196
4.15 Summary of key ideas 196
Appendix: Glossary 197
Continuing Your Learning Journey with Palo Alto Networks 215

How to Use This Study Guide

Welcome to the Palo Alto Networks PCCET Study Guide. The purpose of this guide is to help you prepare for your Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) exam and achieve your PCCET credential.

You can read through this study guide from start to finish, or you may jump straight to topics you would like to study. Hyperlinked cross-references will help you locate important definitions and background information from earlier sections.

About the PCCET Exam

The PCCET certification validates the knowledge required for entry-level network security positions, whose technical requirements change as quickly as the technology upon which it is based. PCCET-certified individuals have detailed knowledge about the latest trends in networks based cyberattacks and about cutting-edge technologies available to prevent the cyberattacks.

More information is available from the Palo Alto Networks public page at:
https://www.paloaltonetworks.com/services/education/certification

PCCET technical documentation is located at:
https://beacon.paloaltonetworks.com/

Exam Format

The test format is 90-100 multiple-choice items. Candidates will have five minutes to complete the Non-Disclosure Agreement (NDA), 80 minutes to complete the questions, and five minutes to complete a survey at the end of the exam.

The approximate distribution of items by topic (Exam Domain) and topic weightings are shown in the following table.

This exam is based on Product version.

Exam Domain	Weight (%)
Fundamentals of Cybersecurity	30%
Network Security Components	30%
Cloud Technologies	20%
Elements of Security Operations	20%
TOTAL	**100%**

How to Take This Exam

The exam is available through the third-party Pearson VUE testing platform.
To register for the exam, visit: https://home.pearsonvue.com/paloaltonetworks

Disclaimer

This study guide is intended to provide information about the objectives covered by this exam, related resources, and recommended courses. The material contained within this study guide is not intended to guarantee that a passing score will be achieved on the exam. Palo Alto Networks recommends that candidates thoroughly understand the objectives indicated in this guide and use the resources and courses recommended in this guide where needed to gain that understanding.

Audience and Qualifications

The PCCET certification is designed for students, the emergent workforce, skilled labor trying to transition into cybersecurity, hiring managers looking to hire entry-level technical help, technical professionals, educators and any non-technical individuals interested in validating comprehensive knowledge on current cybersecurity tenets.

Skills Required

- You understand basic networking concepts (subnetting; protocols; differences between network components such as routers, switches, and hubs; etc).

Recommended Training

Cyber Security Foundation digital learning courses:

- Introduction to Cybersecurity (www.paloaltonetworks.com/EDU-001)
- Fundamentals of Network Security (www.paloaltonetworks.com/EDU-010)
- Fundamentals of Cloud Security (www.paloaltonetworks.com/EDU-040)
- Fundamentals of Security Operations Center (SOC) (www.paloaltonetworks.com/EDU-070)

Palo Alto Networks Cyber Security Academy Cybersecurity Survival Guide -
https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide

PCCET Study Guide -
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pccet-study-guide.pdf

Domain 1: Fundamentals Of Cybersecurity

The modern cybersecurity landscape is a rapidly evolving, hostile environment filled with advanced threats and increasingly sophisticated threat actors. This section describes computing trends that are shaping the cybersecurity landscape, application frameworks and attack (or threat) vectors, cloud computing and SaaS application security challenges, various information security and data protection regulations and standards, and some recent cyberattack examples.

Note: The terms “enterprise” and “business” are used throughout this guide to describe organizations, networks, and applications in general. The use of these terms is not intended to exclude other types of organizations, networks, or applications, and should be understood to include not only large businesses and enterprises but also small and medium-size businesses (SMBs), government, state-owned enterprises (SOEs), public services, military, healthcare, and nonprofits, among others.

Key Terms

- An **attack** (or threat) vector is a path or tool that an attacker uses to target a network.

1.1 Distinguish between Web 2.0 and 3.0 applications and services

The nature of enterprise computing has changed dramatically over the past decade. Core business applications now are commonly installed alongside Web 2.0 apps on a variety of endpoints, and networks that were originally designed to share files and printers are now used to collect massive volumes of data, exchange real-time information, transact online business, and enable global collaboration.
Many Web 2.0 apps are available as software-as-a-service (SaaS), web-based, or mobile apps that can be easily installed by end users or that can be run without installing any local programs or services on the endpoint.

Key Idea

- The use of Web 2.0 apps in the enterprise is sometimes referred to as Enterprise 2.0, although not all Web 2.0 apps are considered to be Enterprise 2.0 applications.

Key Terms

- **Web 2.0** is a term popularized by Tim O'Reilly and Dale Dougherty that unofficially refers to a new era of the World Wide Web, which is characterized by dynamic or user-generated content, interaction, and collaboration, and the growth of social media.
- An **endpoint** is a computing device such as a desktop or laptop computer, handheld scanner, internet of things (IoT) device or sensor (such as an autonomous vehicle, smart appliance, smart meter, smart TV, or wearable device), point-of-sale (POS) terminal, printer, satellite radio, security or video conferencing camera, self-service kiosk, smartphone, tablet, or Voice over Internet Protocol (VoIP) phone. Although endpoints can include servers and network equipment, the term is generally used to describe end-user devices.
- The **internet of things (IoT)** is the network of physical smart objects that are embedded with electronics, software, sensors, and network connectivity to collect and share data.
- **Voice over IP (VoIP)**, or IP telephony, is technology that provides voice communication over an IP-based network.
- **Software as a service (SaaS)** is a category of cloud computing services in which the customer is provided access to a hosted application that is maintained by the service provider.
- **Enterprise 2.0** is a term introduced by Andrew McAfee and defined as "the use of emergent social software platforms within companies, or between companies and their partners or customers."

Typical core business applications include:

- **Accounting software** is used to process and record accounting data and transactions such as accounts payable, accounts receivable, payroll, trial balances, and general ledger (GL) entries. Examples of accounting software include Intacct, Microsoft Dynamics AX and GP, NetSuite, QuickBooks, and Sage.
- **Business intelligence (BI) and business analytics software** consists of tools and techniques used to surface large amounts of raw unstructured data from a variety of sources (such as data warehouses and data marts). BI and business analytics software performs a variety of functions, including business performance management, data mining, event processing, and predictive analytics. Examples of BI and analytics software include IBM Cognos, MicroStrategy, Oracle Hyperion, and SAP.
- **Content management systems (CMS) and enterprise content management (ECM)** systems are used to store and organize files from a central management interface, with features such as indexing, publishing, search, workflow management, and versioning. Examples of CMS and ECM software include EMC Documentum, HP Autonomy, Microsoft SharePoint, and OpenText.
- **Customer relationship management (CRM)** software is used to manage an organization's customer (or client) information, including lead validation, past sales, communication and interaction logs, and service history. Examples of CRM suites include Microsoft Dynamics CRM, Salesforce.com, SugarCRM, and ZOHO.
- **Database management systems (DBMS)** are used to administer databases, including the schemas, tables, queries, reports, views, and other objects that comprise a database. Examples of DBMS software include Microsoft SQL Server, MySQL, NoSQL, and Oracle Database.

- **Enterprise resource planning (ERP)** systems provide an integrated view of core business processes, such as product and cost planning, manufacturing or service delivery, inventory management, and shipping and payment. Examples of ERP software include NetSuite, Oracle's JD Edwards EnterpriseOne and PeopleSoft, and SAP.
- **Enterprise asset management (EAM)** software is used to manage an organization's physical assets throughout their entire lifecycle, including acquisition, upgrade, maintenance, repair, replacement, decommissioning, and disposal. EAM is commonly implemented as an integrated module of ERP systems. Examples of EAM software include IBM Maximo, Infor EAM, and SAP.
- **Supply chain management (SCM)** software is used to manage supply chain transactions, supplier relationships, and various business processes, such as purchase order processing, inventory management, and warehouse management. SCM software is commonly integrated with ERP systems. Examples of SCM software include Fishbowl Inventory, Freightview, Infor Supply Chain Management, and Sage X3.
- **Web content management (WCM)** software is used to manage website content, including administration, authoring, collaboration, and publishing. Examples of web content management software include Drupal, IBM FileNet, Joomla, and WordPress.

Common Web 2.0 apps and services (many of which also are SaaS apps) include:

- **File sync and sharing services** are used to manage, distribute, and provide access to online content, such as documents, images, music, software, and video. Examples include Apple iCloud, Box, Dropbox, Google Drive, Microsoft OneDrive, Spotify, and YouTube.
- **Instant messaging (IM)** is used to exchange short messages in real time. Examples include Facebook Messenger, Skype, Snapchat, and WhatsApp.
- **Microblogging** web services allow a subscriber to broadcast short messages to other subscribers. Examples include Tumblr and Twitter.
- **Office productivity suites** consist of cloud-based word processing, spreadsheet, and presentation software. Examples include Google Apps and Microsoft Office 365.
- **Remote access software** is used for remote sharing and control of an endpoint, typically for collaboration or troubleshooting. Examples include LogMeIn and TeamViewer.
- **Remote team meeting software** is used for audio conferencing, video conferencing, and screen sharing. Examples include Adobe Connect, Microsoft Teams, and Zoom.
- **Social curation** shares collaborative content about particular topics. Social bookmarking is a type of social curation. Examples include Instagram, Pinterest, and Reddit.
- **Social networks** are used to share content with business or personal contacts. Examples include Facebook, Google Currents, and LinkedIn.
- **Web-based email** is an internet email service that typically is accessed via a web browser. Examples include Gmail, Outlook.com, and Yahoo! Mail.
- **Wikis** enable users to contribute, collaborate, and edit site content. Examples include Socialtext and Wikipedia.

According to research from McKinsey & Company and the Association for Information and Image Management (AIIM), many organizations are recognizing significant benefits from the use of Enterprise 2.0 applications and technologies, including better collaboration, increased knowledge sharing, and reduced expenses (for example, for travel, operations, and communications). Thus, enterprise infrastructures (systems, applications, and networks) are rapidly converging with personal and Web 2.0

technologies and apps, making identifying where the internet begins and the enterprise infrastructure ends practically impossible. This convergence is being driven by several important trends, including:

- **Cloud computing**: Cloud computing now is more pervasive than ever. According to the RightScale 2019 State of the Cloud Report from Flexera, public and private cloud adoption is now at 94 percent for enterprises (1,000+ employees) and SMBs (fewer than 1,000 employees), and those companies run a majority of their workloads (about 79 percent) in the cloud. Also, 84 percent of enterprises and 61 percent of SMBs have a multicloud strategy leveraging an average of nearly five public and/or private clouds. Similarly, the Enterprise Strategy Group RightScale report found that production server workloads increasingly run on a mix of cloud-ready architectures, including virtual machines (34 percent), containers (23 percent), and serverless (15 percent).
- **Consumerization**: The process of consumerization occurs as end users increasingly find personal technology and apps that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use than enterprise IT solutions.
- **Bring your own device (BYOD)**: Closely related to consumerization is BYOD, a policy trend in which organizations permit end users to use their own personal devices, primarily smartphones and tablets, for work-related purposes. BYOD relieves organizations from the cost of providing equipment to employees but creates a management challenge because of the vast number and type of devices that must be supported.
- **Bring your own apps (BYOA):** Web 2.0 apps on personal devices are increasingly being used for work-related purposes. As the boundary between work and personal lives becomes less distinct, end users are practically demanding that these same apps be available to them in their workplaces.
- **Mobile computing**: The appetite for rapid, on-demand access to apps and data from anywhere, at any time, on any device is growing. There are approximately more than 8 billion mobile subscriptions worldwide, and total mobile monthly data traffic (including audio, file sharing, social networking, software uploads and downloads, video, web browsing, and other sources) is about 40 exabytes!
- **5G cellular wireless**: Each new generation of wireless connectivity has driven many innovations, and the move to the fifth-generation of cellular wireless (5G) is well under way, with mobile network operators announcing 5G pilot trials and commercialization plans as they expand their geographic footprints. The latest 5G applications are consumer-driven, help governments implement 5G for smart city rollouts, and bring 5G service experience to the public by seamlessly covering major sports events, among others. The promise of intelligent connectivity will drive massive adoption of the internet of things (IoT) and could transform industries. We're now describing the Enterprise of Things: networked industrial devices, sensors, networks, and apps that connect businesses. As today's enterprises undergo digital transformation, they'll be looking for 5G networks to drive true Industry 4.0 transformation, leveraging automation, artificial intelligence (AI), and IoT.
- **Content delivery networks (CDN)**: Enterprises are using content delivery networks such as Akamai, Amazon CloudFront, and Limelight networks to distribute their web products and services to customers worldwide. The use of CDNs will become even more prominent as 5G adoption continues to expand.

Key Terms

- **Public cloud** is a cloud computing deployment model that consists of a cloud infrastructure that is open to use by the general public.
- **Private cloud** is a cloud computing model that consists of a cloud infrastructure used exclusively by a single organization.
- **Multicloud** is an enterprise cloud environment (or strategy) consisting of two or more public and/or private clouds.
- A **virtual machine (VM)** is an emulation of a physical (hardware) computer system, including CPU, memory, disk, operating system, and network interfaces.
- A **container** is a standardized, executable, and lightweight software code package that contains all the necessary components to run a given application (or applications). The components typically include code, runtime, system tools and libraries, and configuration settings in an isolated and virtualized environment. Packaging the components this way provides agility and portability of the application workloads.
- **"Serverless"** generally refers to an operational model in cloud computing in which applications rely on managed services that abstract away the need to manage, patch, and secure infrastructure and virtual machines. Serverless applications rely on a combination of managed cloud services and function-as-a-service (FaaS) offerings.
- **Artificial intelligence (AI)** is the ability of a system or application to interact with and learn from its environment, and to automatically perform actions accordingly, without requiring explicit programming.
- A **content delivery network (CDN)** is a network of distributed servers that distributes cached web pages and other static content to a user from a geographic location that is physically closest to the user.

For many, the vision of Web 3.0 is to return the power of the internet to individual users, in much the same way that the original Web 1.0 was envisioned. To some extent, Web 2.0 has become shaped and characterized, if not controlled, by governments and large corporations dictating the content that is made available to individuals and raising many concerns about individual security, privacy, and liberty. Specific technologies that are evolving and beginning to form the foundations of Web 3.0 include:

- AI and machine learning are two related technologies that enable systems to understand and act on information in much the same way that a human might use information. AI acquires and applies knowledge to find the most optimal solution, decision, or course of action. Machine learning is a subset of AI that applies algorithms to large datasets to discover common patterns in the data that then can be used to improve the performance of the system.
- Blockchain is essentially a data structure containing transactional records (stored as blocks) that ensures security and transparency through a vast, decentralized peer-to-peer network with no single controlling authority. Cryptocurrency, such as Bitcoin, is an example of a blockchain application.
- Data mining enables patterns to be discovered in large datasets through the use of machine learning, statistical analysis, and database technologies.
- Mixed reality includes technologies such as virtual reality (VR), augmented reality (AR), and extended reality (XR) that deliver an immersive and interactive physical and digital sensory experience in real time.
- Natural language search is the ability to understand human spoken language and context to find information, as opposed to a Boolean search, for example.

Key Terms

- **Machine learning** is a subset of AI that applies algorithms to large datasets to discover common patterns in the data that can then be used to improve the performance of a system.
- **Boolean** refers to a system of algebraic notation used to represent logical propositions.

Organizations often are unsure of the potential business benefits, and the inherent risks, of new trends such as Web 2.0 and Web 3.0, and therefore either:

- Implicitly allow personal technologies and apps by simply ignoring their use in the workplace, or
- Explicitly prohibit their use but then are unable to effectively enforce such policies with traditional firewalls and security technologies

Regardless of whether personal technologies and apps are implicitly allowed (and ignored) or explicitly prohibited (but not enforced), the adverse results of ineffective policies include:

- **Lost productivity** because users must either find ways to integrate these unsupported technologies and apps (when allowed) with the enterprise infrastructure or use applications that are unfamiliar to them or less efficient (when personal technologies and apps are prohibited)
- **Potential disruption of critical business operations** because of underground or back-channel processes that are used to accomplish specific workflow tasks or to circumvent controls, and are known to only a few users and are fully dependent on their use of personal technologies and apps
- **Exposure to additional risks** for the enterprise due to unknown, and therefore unpatched, vulnerabilities in personal technologies and apps, and a perpetual wait-and-see game between employees that circumvent controls (for example, with external proxies, encrypted tunnels, and remote desktop applications) and security teams that manage these risks.
- **Penalties can be levied against organizations for non-compliance of regulations from groups such as** the EU General Data Protection Regulation (GDPR), the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

As these trends continue to blur the distinction between the internet and the enterprise network, new security challenges and risks emerge, including:

- New application threat vectors
- Turbulence in the cloud
- SaaS application risks

1.1.1 References

- "Flexera 2020 State of the Cloud Report", https://www.flexera.com/2019-cloud-report.
- Cahill, Doug. "Leveraging DevSecOps to Secure Cloud-native Applications." Enterprise Strategy Group. December 9, 2019, https://www.esg-global.com/research/esg-master-survey-results-leveraging-devsecops-to-secure-cloud-native-applications
- "Ericsson Mobility Report, November 2020." Ericsson. November 2020, https://www.ericsson.com/en/mobility-report/reports/november-2019
- Expert System. 2020. "The 5 Main Features of Web 3.0." Accessed April 30, 2020, http://www.expertsystem.com/web-3-0/

1.2 Describe port-scanning methodologies and their impact

A port scan is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system's firewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

1.2.1 Non-standard ports

Ports vary in their services offered. They are numbered from 0 to 65535, but certain ranges are more frequently used. Ports 0 to 1023 are identified as the "well-known ports" or standard ports and have been assigned services by the Internet Assigned Numbers Authority (IANA). Some of the most prominent ports and their assigned services include:

- **Port 20 (udp)** – File Transfer Protocol (FTP) for data transfer
- **Port 22 (tcp)** – Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding
- **Port 23 (tcp)** – Telnet protocol for unencrypted text commutations
- **Port 53 (udp)** – Domain Name System (DNS) translates names of all computers on internet to IP addresses
- **Port 80 (tcp)** – World Wide Web HTTP

There are standard services offered on ports after 1023 as well, and ports that, if open, indicate an infected system due to its popularity with some far-reaching Trojans and viruses.

1.2.2 Identify applications by their port number

A port scan sends a carefully prepared packet to each destination port number. The basic techniques that port scanning software is capable of include:

- **Vanilla**– the most basic scan; an attempt to connect to all 65,536 ports one at a time. A vanilla scan is a full connect scan, meaning it sends a SYN flag (request to connect) and upon receiving a SYN-ACK (acknowledgement of connection) response, sends back an ACK flag. This SYN, SYN-ACK, ACK exchange comprises a TCP handshake. Full connect scans are accurate, but very easily detected because full connections are always logged by firewalls.
- **SYN Scan**– Also referred to as a half-open scan, it only sends a SYN, and waits for a SYN-ACK response from the target. If a response is received, the scanner never responds. Since the TCP connection was not completed, the system doesn't log the interaction, but the sender has learned if the port is open or not.
- **XMAS and FIN Scans**– an example of a suite of scans used to gather information without being logged by the target system. In a FIN scan, an unsolicited FIN flag (used normally to end an established session) will be sent to a port. The system's response to this random flag can reveal the state of the port or insight about the firewall. For example, a closed port that receives an unsolicited FIN packet, will respond with a RST (an instantaneous abort) packet, but an open port will ignore it. An XMAS scan simply sends a set of all the flags, creating a nonsensical interaction. The system's response can be interpreted to better understand the system's ports and firewall.
- **FTP Bounce Scan**– allows for the sender's location to be disguised by bouncing the packet through an FTP server. This is also designed for the sender to go undetected.
- **Sweep scan**– pings the same port across a number of computers to identify which computers on the network are active. This does not reveal information about the port's state, instead it tells the sender which systems on a network are active. Thus, it can be used as a preliminary scan.

Scans that are developed for the sender to go undetected by a receiving system's log are known as stealth scans and are of particular interest to attackers. Despite its popularity in this area, port scanning is a valuable tool for fingerprinting a network and for a penetration tester to assess the strength of network security.

1.2.3 References

- Port Scan, https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan

1.3 Recognize applications used to circumvent port-based firewalls

Exploitation of vulnerabilities in core business applications has long been an attack vector, but threat actors are constantly developing new tactics, techniques, and procedures (TTPs). Enterprise security teams that want to effectively protect their networks and cloud environment must not only manage the risks associated with a relatively limited, known set of core applications, but they must also manage the risks associated with an ever-increasing number of known and unknown cloud-based applications. Cloud-based application consumption models have revolutionized the way organizations do business, and applications such as Microsoft Office 365 and Salesforce are being consumed and updated entirely in the cloud.

Classification of applications as either “good” (to be allowed) or “bad” (to be blocked) in a clear and consistent manner has also become increasingly difficult. Many applications are clearly good (low risk, high reward) or clearly bad (high risk, low reward), but most are somewhere in between, depending on how the application is being used.

For example, many organizations use social networking applications such as Facebook for important business functions, such as recruiting, research and development, marketing, and consumer advocacy. However, these same applications can be used to leak sensitive information or cause damage to an organization’s public image, whether inadvertently or maliciously.

Many applications are designed to circumvent traditional port-based firewalls so that they can be easily installed and accessed on any device, anywhere and anytime, using techniques such as:

- **Port hopping**, in which ports and protocols are randomly changed during a session.
- **Using non-standard ports**, such as running Yahoo! Messenger over TCP port 80 (HTTP) instead of the standard TCP port for Yahoo! Messenger (5050).
- **Tunneling within commonly used services**, such as when peer-to-peer (P2P) file sharing or an instant messenger (IM) client such as Meebo is running over HTTP.
- **Hiding within SSL encryption**, which masks the application traffic, for example, over TCP port 443 (HTTPS). More than half of all web traffic is now encrypted.

Many traditional client-server business applications also are being redesigned for web use and employ these same techniques for ease of operation while minimizing disruptions. For example, both remote procedure call (RPC) and Microsoft SharePoint use port hopping because it is critical to how the protocol or application (respectively) functions, rather than as a means to evade detection or enhance accessibility.

Key Terms

- **Remote procedure call (RPC)** is an inter-process communication (IPC) protocol that enables an application to be run on a different computer or network rather than the local computer on which it is installed.

Applications also can be hijacked and repurposed by malicious actors, such as was done in the 2014 Heartbleed attack. According to an April 2014 Palo Alto Networks article:

- *"The story of Heartbleed's impact has been focused on the compromise of HTTPS-enabled websites and web applications, such as Yahoo!, Google, Dropbox, Facebook, online banking, and the thousands of other vulnerable targets on the web. These are of huge impact, but those sites will all be updated quickly....*
- *"For security professionals, [the initial Heartbleed attack] is only the tip of the iceberg. The vulnerability puts the tools once reserved for truly advanced threats into the hands of the average attacker – notably, the ability to breach organizations, and move laterally within them. Most enterprises of even moderate size do not have a good handle on what services they are running internally using SSL encryption. Without this baseline knowledge, it is extremely difficult for security teams to harden their internal attack surface against the credential and data stealing tools Heartbleed enables. All footholds for the attacker with an enterprise network are suddenly of equal value."*

As new applications are increasingly web-enabled and browser-based, HTTP and HTTPS now account for about two-thirds of all enterprise network traffic. Traditional port-based firewalls and other security infrastructure cannot distinguish whether these applications, riding on HTTP and HTTPS, are being used for legitimate business purposes.

1.3.1 References

- Simkin, Scott. "Real-world Impact of Heartbleed (CVE-2014-0160): The Web is Just the Start." Palo Alto Networks. April 2014, https://researchcenter.paloaltonetworks.com/2014/04/real-world-impact-heartbleed-cve-2014-0160-web-just-start

1.4 Differentiate between common cloud computing service models

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner.
NIST defines three distinct cloud computing service models:

1.4.1 SaaS

Software as a service (SaaS): Customers are provided access to an application running on a cloud infrastructure. The application is accessible from various client devices and interfaces, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer may have access to limited user-specific application settings, and security of the customer data still is the responsibility of the customer.

1.4.2 PaaS

Platform as a service (PaaS): Customers can deploy supported applications onto the provider's cloud infrastructure, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over the deployed applications and limited configuration settings for the application-hosting environment. The company owns the deployed applications and data, and therefore it is responsible for the security of those applications and data.

1.4.3 IaaS

Infrastructure as a service (IaaS): Customers can provision processing, storage, networks, and other computing resources, and deploy and run operating systems and applications. However, the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, along with some networking components.

1.4.4 References

- Cloud Security Service, Cloud Storage and Cloud Technology, https://www.paloaltonetworks.com/cyberpedia/cloud-security-service-cloud-storage-and-cloud-technology

1.5 Describe the business processes of supply-chain management

Supply chain management (SCM) software is used to manage supply chain transactions, supplier relationships, and various business processes, such as purchase order processing, inventory management, and warehouse management. SCM software is commonly integrated with ERP systems. Examples of SCM software include Fishbowl Inventory, Freightview, Infor Supply Chain Management, and Sage X3.

Around the world, governments as well as private sector organizations are focused on identifying and mitigating risks to the information and communications technology (ICT) supply chain. In fact, efforts to disrupt or exploit supply chains have become, in the words of a senior US Homeland Security Department official, a "principal attack vector" for adversarial nations seeking to take advantage of vulnerabilities for espionage, sabotage or other malicious activities. In this environment, strong supply chain security practices are a differentiator for critical infrastructure organizations. But what, exactly, does a strong supply chain security program look like? Recently, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) published a case study highlighting how Palo Alto Networks uses supply chain best practices.

The case study identified several best practices that collectively contribute to the overall supply chain security efforts of Palo Alto Networks. Among them:

- An organizational focus on end-to-end risk management. We identify supply chain risks across our entire product lifecycle – design, sourcing, manufacturing, fulfillment and service – and take proactive action to ensure the integrity of our products. Risk assessments are performed early in the product development lifecycle to help determine the feasibility of product design decisions.
- Strong supplier management, focused on security requirements as well as establishing collaborative relationships to ensure a complete view of suppliers' security posture.
- Hardware manufacturing and order fulfillment processes that enable us to more easily manage personnel and facility and product security. In fact, we regularly consider geopolitical implications when making decisions to forgo suppliers and manufacturing locations because it's simply the right decision for product security.

- Active engagement in public-private partnerships designed to increase collaboration between public and private sector organizations and make recommendations for enhancing supply chain security, such as our executive committee role on the DHS ICT Supply Chain Risk Management Task Force.
- Finally, overlaying these practices is executive management buy-in. Supply chain risk management is a team sport spanning operations, product management, and other corporate functions. Strong coordination is critical to our success.

1.5.1 References

- NIST Highlights Palo Alto Networks Supply Chain Best Practices, https://www.paloaltonetworks.com/blog/2020/06/policy-supply-chain-best-practices/

1.6 Describe the vulnerabilities associated with data being stored in the SaaS environment

1.6.1 Describe roles within a SaaS environment

A role defines the type of access that an administrator has to the firewall. The Administrator Types are:

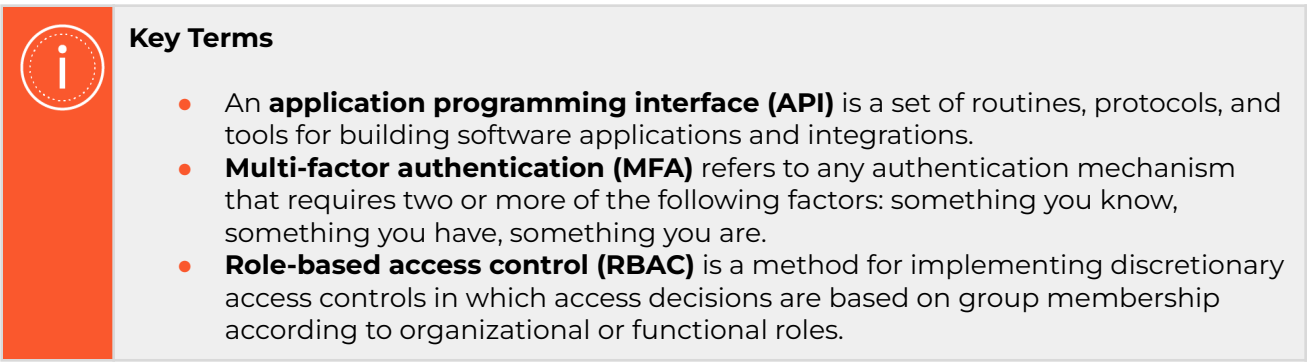
- Role Based- This allows custom roles you can configure for more granular access control over the functional areas of the web interface, CLI, and XML API. For example, you can create an Admin Role profile for your operations staff that provides access to the firewall and network configuration areas of the web interface, then create a separate profile for your security administrators that provides access to security policy definitions, logs, and reports. On a firewall with multiple virtual systems, you can select whether the role defines access for all virtual systems or specific virtual systems. When new features are added to the product, you must update the roles with corresponding access privileges because the firewall does not automatically add new features to custom role definitions.
- Dynamic- These include built-in roles that provide access to the firewall. When new features are added, the firewall automatically updates the definitions of dynamic roles; you never need to manually update them..

1.6.2 Describe security controls for SaaS applications

Data is located everywhere in today's enterprise networks, including in many locations that are not under the organization's control. New data security challenges emerge for organizations that permit SaaS use in their networks.
With SaaS applications, data often is stored where the application resides: in the cloud. Thus, the data is no longer under the organization's control and visibility therefore often is lost. SaaS vendors do their best to protect the data in their applications, but it is ultimately not their responsibility. Just as in any other part of the network, the IT team is responsible for protecting and controlling the data, regardless of its location.

The average employee uses at least eight applications, but as employees add and use more SaaS apps that connect to the corporate network, the risk of sensitive data being stolen, exposed, or compromised increases. You must consider the security of the apps, which data they have access to, and how employees are using them. Here are several best practices for securing sensitive data in SaaS apps:

- **Discover employee use of unvetted SaaS applications**. As SaaS adoption rapidly expands, manual discovery of SaaS use in the enterprise becomes increasingly untenable. Instead, to quickly identify risk and extend appropriate security controls, your organization needs an automated way to continuously discover all SaaS applications in use by employees.
- **Protect sensitive data in SaaS applications**. Implement advanced DLP capabilities using an application programming interface (API)-based approach to scan for sensitive information stored within SaaS applications. Compared to inline, an API-based approach provides deeper context and allows for automatic remediation of data-risk violations.
- **Secure your weakest link: SaaS users**. Start with user training and interactive coaching to identify and help change risky behavior. Then, give your security team tools to help them monitor and govern SaaS application permissions. Look for a solution with robust access controls, including:
    - Multi-factor authentication (MFA)
    - Role-based access control (RBAC)
    - Protection for administrative accounts
    - User access monitoring that can detect malicious or risky behavior
- **Enforce compliance requirements in the cloud**. Create and enforce a consistent, granular security policy for compliance that covers all SaaS applications used by your organization. Security policy enforcement should include automating compliance and reporting for all relevant regulatory requirements across your SaaS applications.
- **Reduce risk from unmanaged devices**. Deploy a security product that differentiates access between managed and unmanaged devices to protect against the increased security risks inherent with personal devices. For instance, you could allow downloads to managed devices but block them for unmanaged devices while enabling access to core functionality.
- **Control data sharing from SaaS applications**. Use an inline approach to gain visibility into sensitive data flowing into high-risk, unsanctioned applications. Create and enforce DLP policies that control data-sharing activities in the SaaS applications employees use.
- **Stop SaaS-borne malware threats**. Implement threat prevention technology that works with your SaaS security to block malware and stop threats from spreading through SaaS applications, thus eliminating a new insertion point for malware.



Key Terms

- An **application programming interface (API)** is a set of routines, protocols, and tools for building software applications and integrations.
- **Multi-factor authentication (MFA)** refers to any authentication mechanism that requires two or more of the following factors: something you know, something you have, something you are.
- **Role-based access control (RBAC)** is a method for implementing discretionary access controls in which access decisions are based on group membership according to organizational or functional roles.

1.6.3 References

- "2019 SaaS Trends." Blissfully. 2019, https://blissfully.com/saas-trends/2019-annual/

1.7 Describe the impact of governance, regulation, and compliance

1.7.1 Differentiate between compliance and security

You should understand that compliance and security are not the same thing. An organization can be fully compliant with the various cybersecurity laws and regulations that are applicable for that organization, yet still not be secure. Conversely, an organization can be secure yet not be fully compliant. As if to underscore this point, the compliance and security functions in many organizations are separate.

Compliance is based on the type of data held and stored by the company and what regulatory requirements (frameworks) apply to its protection. Compliance means ensuring that the organization complies with the minimum security-related requirements.
Security is a clear set of technological programs and tools and processes in place to protect and secure business information and technology assets.

1.7.2 Identify major cybersecurity laws and their implications

A rapidly and ever-increasing number of international, multinational, federal, regional, state, and local laws and regulations mandate numerous cybersecurity and data protection requirements for businesses and organizations worldwide. Various industry directives, such as the Payment Card Industry Data Security Standard (PCI DSS), also establish their own cybersecurity standards and best practices for businesses and organizations operating under their purview.
This complex regulatory environment is further complicated by the fact that many laws and regulations are obsolete, ambiguous, not uniformly supported by international communities, and/or inconsistent with other applicable laws and regulations, thus requiring legal interpretation to determine relevance, intent, and/or precedence. As a result, businesses and organizations in every industry struggle to achieve and maintain compliance.
Pertinent examples (neither comprehensive nor exhaustive) of current cybersecurity laws and regulations include:

- **Australian Privacy Principles**: The Privacy Act 1988 establishes standards for collecting and handling personal information, referred to as the Australian Privacy Principles (APP).
- **California Consumer Privacy Act (CCPA)**: This privacy rights and consumer protection statute for residents of California was enacted in 2018 and became effective on January 1, 2020.
- **Canada Personal Information Protection and Electronic Documents Act (PIPEDA)**: PIPEDA defines individual rights with respect to the privacy of their personal information and governs how private sector organizations collect, use, and disclose personal information in the course of business.
- **EU Network and Information Security (NIS) Directive**: An EU directive that imposes network and information security requirements for banks, energy companies, healthcare providers, and digital service providers, among others.
- **European Union (EU) General Data Protection Regulation (GDPR)**: The GDPR applies to any organization that does business with EU residents. It strengthens data protection for EU residents and addresses the export of personal data outside the EU.

- **North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)**: NERC CIP defines cybersecurity standards to protect the physical and cyber assets necessary to operate the bulk electric system (BES) – the power grid – in the United States and Canada. The standards are mandatory for all BES-generating facilities with different criteria based on a tiered classification system (high, medium, or low impact).
- **Payment Card Industry Data Security Standard (PCI DSS)**: PCI DSS applies to any organization that transmits, processes, or stores payment card (such as debit and credit cards) information. PCI DSS is mandated and administered by the PCI Security Standards Council (SSC) comprising Visa, MasterCard, American Express, Discover, and JCB.
- **U.S. Cybersecurity Enhancement Act of 2014**: This act provides an ongoing, voluntary public-private partnership to improve cybersecurity and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness.
- **U.S. Cybersecurity Information Sharing Act (CISA)**: This act enhances information sharing about cybersecurity threats by allowing internet traffic information to be shared between the U.S. government and technology and manufacturing companies.
- **U.S. Federal Exchange Data Breach Notification Act of 2015**: This act further strengthens HIPAA by requiring health insurance exchanges to notify individuals whose personal information has been compromised as the result of a data breach as soon as possible but no later than 60 days after breach discovery.
- **U.S. Federal Information Security Modernization Act (FISMA)**: Known as the Federal Information Security Management Act prior to 2014, FISMA implements a comprehensive framework to protect information systems used in federal government agencies.
- **U.S. Gramm-Leach-Bliley Act (GLBA)**: Also known as the Financial Services Modernization Act of 1999, relevant provisions of GLBA include the Financial Privacy Rule and the Safeguards Rule, which require financial institutions to implement privacy and information security policies to safeguard the non-public personal information of clients and consumers.
- **U.S. Health Insurance Portability and Accountability Act (HIPAA)**: The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information. It requires appropriate safeguards for protected health information (PHI) and applies to covered entities and their business associates.
- **U.S. National Cybersecurity Protection Advancement Act of 2015**: This act amends the Homeland Security Act of 2002 to enhance sharing of information related to cybersecurity risks and strengthens privacy and civil liberties protections.
- **U.S. Sarbanes-Oxley (SOX) Act**: This act was enacted to restore public confidence following several high-profile corporate accounting scandals, most notably Enron and Worldcom. SOX increases financial governance and accountability in publicly traded companies. Section 404 of SOX specifically addresses internal controls, including requirements to safeguard the confidentiality, integrity, and availability of IT systems.

Key Terms

- **Protected health information (PHI)** is defined by HIPAA as information about an individual's health status, provision of healthcare, or payment for healthcare that includes identifiers such as names, geographic identifiers (smaller than a state), dates, phone and fax numbers, email addresses, Social Security numbers, medical record numbers, and photographs.
- **A covered entity** is defined by HIPAA as a healthcare provider that electronically transmits PHI. These entities include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, a health plan (such as a health insurance company, health maintenance organization, company health plan, or government program, including Medicare, Medicaid, military and veterans' healthcare), or a healthcare clearinghouse.
- **A zero-day threat** is the window of vulnerability that exists from the time a new (unknown) threat is released until security vendors release a signature file or security patch for the threat.
- **Personally identifiable information (PII)** is defined by the U.S. National Institute of Standards and Technology (NIST) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity … and (2) any other information that is linked or linkable to an individual…." Examples of PII include:
  - *Name* (such as full name, maiden name, mother's maiden name, or alias)
  - *Personal identification number* (such as Social Security number, passport number, driver's license number, and financial account number or credit card number)
  - *Address information* (such as street address or email address)
  - *Telephone numbers* (such as mobile, business, and personal numbers)
  - *Personal characteristics* (such as photographs, X-rays, fingerprints, and biometric data)
  - *Information about personally owned property* (such as vehicle registration number and title information)
  - *Information that is linked or linkable to any of the preceding PII examples* (such as birthdate, birthplace, and religion, and employment, medical, education, and financial records)

1.7.3 References

Mayes, Michael. "Top 10 Ransomware Stories of 2019." CPO Magazine. December 27, 2019, https://www.cpomagazine.com/cyber-security/top-10-ransomware-stories-of2019/

1.8 Describe the tactics of the MITRE ATT&CK framework

The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objective, and assess an organization's risk. Organizations can use the framework to identify security gaps and prioritize mitigations based on risk.

MITRE's approach is focused on articulating how detections occur rather than assigning scores to vendor capabilities. MITRE categorizes each detection and capture. Detections are then organized according to each technique. Techniques may have more than one detection if the capability detects the technique in different ways, and detections they observe are included in the results. While MITRE makes every effort to capture different detections, vendor capabilities may be able to detect procedures in ways that MITRE did not capture.

For a detection to be included for a given technique, the detection must apply to that technique specifically. For example, just because a detection applies to one technique in a step or sub-step, that does not mean it applies to all techniques of that step.

Key Idea

- For proof of detection in each category, MITRE requires that the proof be provided to it, but it may not include all detection details in public results, particularly when those details are sensitive.

To determine the appropriate category for a detection, MITRE reviews the screenshot(s) provided, notes taken during the evaluation, results of follow-up questions to the vendor, and vendor feedback on draft results.

MITRE also independently tests procedures in a separate lab environment as well as reviews open-source tool detections and forensic artifacts. This testing informs what is considered a detection for each technique. After performing detection categorizations, MITRE calibrates the categories across all vendors to look for discrepancies and ensure categories are applied consistently.

1.8.1 Identify a leading indicator of a compromise

An indicator of compromise (IoC) is a network or operating system (OS) artifact that provides a high level of confidence that a computer security incident has occurred.

In many cases these are brittle and easy for adversaries to bypass by modifying malware or infrastructure. Indicators like file hashes, IP addresses, and domain names have become the focal point for many network defenders, yet each of these are trivial for an adversary to change in order to avoid detection. In addition, the defending organization needs to have access to relevant and up-to-date indicators through a threat indicator sharing program or commercial data feed, all of which may still not ensure that defenders are able to keep pace with adversary changes.

An intrusion detection program incorporating behavioral detection analytics is more resilient to attempts by adversaries to avoid signature-based detection through indicator modification. Behavioral detection approaches help identify the common behaviors that are highly likely to be performed across many adversary groups during an intrusion, and are independent of specific changes to indicators that adversaries make. This is the premise that drove the development of ATT&CK-based analytics.

1.8.2 Describe how to use CVE

Common Vulnerabilities and Exposures (CVE) is a system for referencing publicly known vulnerabilities by identifiers. The goal of the system is to make it easier to share vulnerability data across stakeholders, including software vendors, tool vendors, security practitioners, and end users.

To evaluate the extent and severity of each CVE across your endpoints, you can drill down into each CVE in Cortex XDR and view all the endpoints and applications in your environment impacted by the CVE. Cortex XDR retrieves the latest information from the NIST public database. From **Add-ons > Host Insights > Vulnerability Assessment**, select **CVEs** on the upper-right bar. For each vulnerability, Cortex XDR displays the following default and optional values:

VALUE	DESCRIPTION
Affected endpoints	The number of endpoints that are currently affected by this CVE. For excluded CVEs, the affected endpoints are **N/A**.
Applications	The names of the applications affected by this CVE.
CVE	The name of the CVE.
Description	The general NIST description of the CVE.
Excluded	Indicates whether this CVE is excluded from all endpoint and application views and filters, and from all Host Insights widgets.
Platforms	The name and version of the operating system affected by this CVE.
Severity	The severity level (Critical, High, Medium, or Low) of the CVE as ranked in the NIST database.
Severity score	The CVE severity score is based on the NIST Common Vulnerability Scoring System (CVSS). Click the score to see the full CVSS description.

Key Idea

- You can click each individual CVE to view in-depth details about it on a panel that appears on the right.

You can perform the following actions from Cortex XDR as you analyze the existing vulnerabilities:

- **View CVE details**—Left-click the CVE to view in-depth details about it on a panel that appears on the right. Use the in-panel links as needed.
- **View a complete list of all endpoints in your network impacted by a CVE**—Right-click the CVE and then select **View affected endpoints**.
- **Learn more about the applications in your network that are impacted by a CVE**—Right-click the CVE and then select **View applications**.
- **Exclude irrelevant CVEs from your endpoints and applications analysis**—Right-click the CVE and then select **Exclude**. You can add a comment if needed, as well as **Report CVE as incorrect** for further analysis and investigation by Palo Alto Networks. The CVE is grayed out, labeled **Excluded**, and no longer appears on the **Endpoints** and **Applications** views in **Vulnerability Assessment** or in the Host Insights widgets. To restore the CVE, right-click the CVE and **Undo exclusion** at any time.

1.8.3 Describe how to use CVS

The Common Vulnerability Scoring System (CVSS) offers a method for enumerating a vulnerability's key characteristics and generating a numerical score that reflects the vulnerability's severity. To assist organizations in correctly evaluating and prioritizing their vulnerability management processes, the numerical score can then be converted into a qualitative representation (such as low, medium, high, and critical).

1.8.4 References

- What is the MITRE ATT&CK Framework? https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-framework#:~:text=The%20MITRE%20ATT%26CK%E2%84%A2%20framework,and%20assess%20an%20organization's%20risk.
- MITRE ATT&CK — Courses of Action, https://xsoar.pan.dev/docs/reference/packs/courses-of-action

1.9 Identify the different attacker profiles and motivations

1.9.1 Describe the different value levels of the information that need protection (political, financial, etc.)

In modern cyber warfare you must understand the strengths, weaknesses, strategies, and tactics of your adversary, including their means and motivations.

Key Terms

- The term **hacker** was originally used to refer to anyone with highly specialized computing skills, without connoting good or bad purposes. However, common misuse of the term has redefined a hacker as someone who circumvents computer security with malicious intent, such as a cybercriminal, cyberterrorist, or hacktivist, cracker, and/or black hat.
- A **script kiddie** is someone with limited hacking and/or programming skills who uses malicious programs (malware) written by others to attack a computer or network.

Modern cyberattacks are perpetrated by far more sophisticated and dangerous adversaries, motivated by far more sinister purposes:

- **Cybercriminals**: Cybercriminals commit crimes acting independently or as part of a criminal organization to commit acts of data theft, embezzlement, fraud, and/or extortion for financial gain. According to the RAND Corporation, "In certain respects, the black market [for cybercrime] can be more profitable than the illegal drug trade," and by many estimates, cybercrime is now a money-making industry.
- **State-affiliated groups**: These organizations are sponsored by or affiliated with nation-states and have the resources to launch very sophisticated and persistent attacks, have great technical depth and focus, and are well funded. They often have military and/or strategic objectives such as the ability to disable or destroy critical infrastructure, including power grids, water supplies, transportation systems, emergency response, and medical and industrial systems. The Center for Strategic and International Studies reports that "At the nation-state level, Russia, Iran, and North Korea are using coercive cyberattacks to increase their sphere of influence, while China, Russia and Iran have conducted reconnaissance of networks critical to the operation of the U.S. power grid and other critical infrastructure without penalty."
- **Hacktivists**: Hacktivist groups (such as Anonymous) are motivated by political or social causes and typically execute denial-of-service (DoS) attacks against a target organization by defacing their websites or flooding their networks with traffic.
- **Cyberterrorists**: Terrorist organizations use the internet to recruit, train, instruct, and communicate, and to spread fear and panic to advance their ideologies. Unlike other threat actors, cyberterrorists are largely indiscriminate in their attacks, and their objectives include physical harm, death, and destruction.

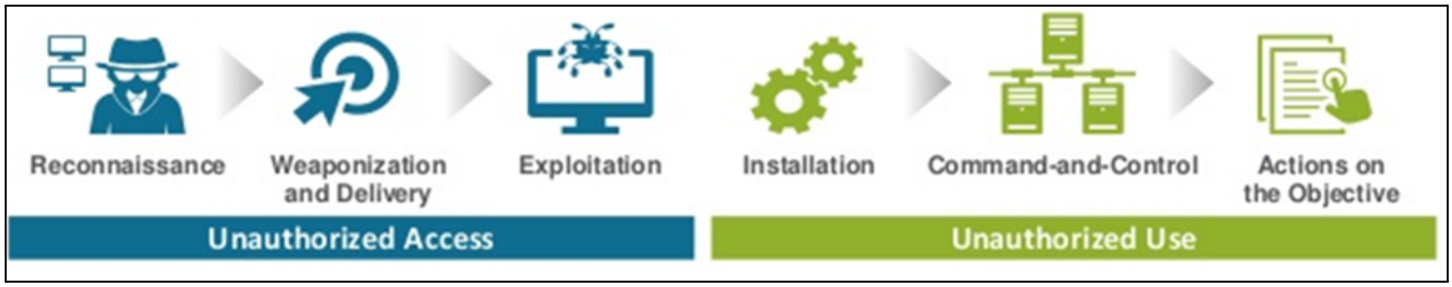
External threat actors include organized crime, state-affiliated groups, activists, former employees, and other unaffiliated or otherwise unknown attackers and account for the majority of data breaches.

1.9.2 References

- Lillian Ablon, Martin Libicki, and Andrea Golay. "Markets for Cybercrime Tools and Stolen Data." RAND Corporation, National Security Research Division. 2014, https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_R R610.pdf
- Zheng, Denise E. "Global Forecast 2016: Disrupting the Cyber Status Quo." Center for Strategic and International Studies. November 16, 2015, https://www.csis.org/analysis/disrupting-cyber-status-quo
- "2019 Data Breach Investigations Report." Verizon Enterprise Solutions. 2019, https://www.enterprise.verizon.com/resources/reports/dbir/

1.10 Describe the different phases and events of the cyberattack lifecycle

Modern cyberattack strategy has evolved from a direct attack against a high-value server or asset ("shock and awe") to a patient, multistep process that blends exploits, malware, stealth, and evasion in a coordinated network attack ("low and slow"). The cyberattack lifecycle (see following figure) illustrates the sequence of events that an attacker goes through to infiltrate a network and exfiltrate (or steal) valuable data. Blocking of just one step breaks the chain and can effectively defend an organization's network and data against an attack.



1. **Reconnaissance**: Like common criminals, attackers meticulously plan their cyberattacks. They research, identify, and select targets, often extracting public information from targeted employees' social media profiles or from corporate websites, which can be useful for social engineering and phishing schemes. Attackers also will scan for network vulnerabilities, services, and applications that they can exploit by using tools such as:
    - **Network analyzers** (also known as packet analyzers, protocol analyzers, or packet sniffers) are used to monitor and capture raw network traffic (packets). Examples include tcpdump and Wireshark (formerly Ethereal).
    - **Network vulnerability scanners** typically consist of a suite of tools including password crackers, port scanners, and vulnerability scanners and are used to probe a network for vulnerabilities (including configuration errors) that can be exploited. Examples include Nessus and SAINT.
    - **Password crackers** are used to perform brute-force dictionary attacks against password hashes. Examples include John the Ripper and THC Hydra.
    - **Port scanners** are used to probe for open TCP or UDP (including ICMP) ports on an endpoint. Examples include Nmap ("network mapper") and Nessus.
    - **Web application vulnerability scanners** are used to scan web applications for vulnerabilities such as cross-site scripting, SQL injection, and directory traversal. Examples include Burp Suite and OWASP Zed Attack Proxy (ZAP).
    - **Wi-Fi vulnerability scanners** are used to scan wireless networks for vulnerabilities (including open and misconfigured access points) to capture wireless network traffic and to crack wireless passwords. Examples include Aircrack-ng and Wifite.

    Breaking the cyberattack lifecycle at this phase of an attack begins with proactive and effective end-user security awareness training that focuses on topics such as social engineering techniques (for example, phishing, piggybacking, and shoulder surfing), social media (for example, safety and privacy issues), and organizational security policies (for example, password requirements, remote access, and physical security). Another important countermeasure is continuous monitoring and inspection of network traffic flows to detect and prevent unauthorized port and vulnerability scans, host sweeps, and other suspicious activity.

Key Idea

- Effective change and configuration management processes help to ensure that newly deployed applications and endpoints are properly configured (for example, disabling unneeded ports and services) and maintained.

2. **Weaponization**: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message. Or, for highly targeted attacks, attackers may customize deliverables to match the specific interests of an individual within the target organization. Breaking the cyberattack lifecycle at this phase of an attack is challenging because weaponization typically occurs within the attacker's network. However, analysis of artifacts (both malware and weaponizer) can provide important threat intelligence to enable effective zero-day protection when delivery (the next step) is attempted.
3. **Delivery**: Attackers next attempt to deliver their weaponized payload to a target endpoint, for example, via email, instant messaging (IM), drive-by download (an end user's web browser is redirected to a webpage that automatically downloads malware to the endpoint in the background), or infected file share. Breaking the cyberattack lifecycle at this phase of an attack requires visibility into all network traffic (including remote and mobile devices) to effectively block malicious or risky websites, applications, and IP addresses, and preventing known and unknown malware and exploits.
4. **Exploitation**: After a weaponized payload is delivered to a target endpoint, it must be triggered. An end user may unwittingly trigger an exploit, for example, by clicking a malicious link or opening an infected attachment in an email, or an attacker may remotely trigger an exploit against a known server vulnerability on the target network. Breaking the cyberattack lifecycle at this phase of an attack, as during the Reconnaissance phase, begins with proactive and effective end-user security awareness training that focuses on topics such as malware prevention and email security. Other important security countermeasures include vulnerability and patch management; malware detection and prevention; threat intelligence (including known and unknown threats); blocking risky, unauthorized, or unneeded applications and services; managing file or directory permissions and root or administrator privileges; and logging and monitoring network activity.
5. **Installation**: Next, an attacker will escalate privileges on the compromised endpoint, for example, by establishing remote shell access and installing root kits or other malware. With remote shell access, the attacker has control of the endpoint and can execute commands in privileged mode from a command line interface (CLI) as if physically sitting in front of the endpoint. The attacker then will move laterally across the target's network, executing attack code, identifying other targets of opportunity, and compromising additional endpoints to establish persistence. The way to break the cyberattack lifecycle at this phase of an attack is to limit or restrict the attackers' lateral movement within the network. Use network segmentation and a Zero Trust model that monitors and inspects all traffic between zones or segments, and granular control of applications that are allowed on the network.
6. **Command and Control**: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

7. **Actions on the Objective**: Attackers often have multiple, different attack objectives including data theft; destruction or modification of critical systems, networks, and data; and denial-of-service (DoS). This last stage of the cyberattack lifecycle also can be used by an attacker to advance the early stages of the cyberattack lifecycle against another target. The 2018 Verizon Data Breach Investigations Report (DBIR) describes this strategy as a secondary motive in which "[web applications] are compromised to aid and abet in the attack of another victim." For example, an attacker may compromise a company's extranet to breach a business partner that is the primary target. The attacker pivots the attack against the initial victim network to a different victim network, thus making the initial victim an unwitting accomplice.

1.10.1 Describe the purpose of command and control (C2)

Communication is essential to an attack because it enables the attacker to remotely direct the attack and execute the attack objectives. C2 traffic must therefore be resilient and stealthy for an attack to succeed. Attack communication traffic is usually hidden with various techniques and tools, including:

- Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption
- Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic.
- Port evasion using network anonymizers or port hopping to traverse over any available open ports
- Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult
- DNS tunneling is used for C2 communications and data infiltration (for example, sending malicious code, commands, or binary files to a victim) and data exfiltration.

Breaking the cyberattack lifecycle at this phase of an attack requires inspection of all network traffic (including encrypted communications), blocking of outbound C2 communications with anti-C2 signatures (along with file and data pattern uploads), blocking all outbound communications to known malicious URLs and IP addresses, blocking novel attack techniques that employ port evasion methods, prevention of the use of anonymizers and proxies on the network, monitoring DNS for malicious domains and countering with DNS sinkholing or DNS poisoning, and redirecting malicious outbound communications to honeypots to identify or block compromised endpoints and analyze attack traffic.

1.10.2 References

- "2018 Data Breach Investigations Report, 11th Edition." Verizon Enterprise Solutions. 2018, https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

1.11 Identify the characteristics, capabilities, and appropriate actions for different types of malware and ransomware

Malware is malicious software or code that typically takes control of, collects information from, or damages an infected endpoint. Malware broadly includes:

- **Viruses**: A virus is malware that is self-replicating but must first infect a host program and be executed by a user or process.
- **Worms**: A worm is malware that typically targets a computer network by replicating itself to spread rapidly. Unlike viruses, worms do not need to infect other programs and do not need to be executed by a user or process.
- **Trojan horses**: A trojan horse is malware that is disguised as a harmless program but actually gives an attacker full control and elevated privileges of an endpoint when installed. Unlike other types of malware, trojan horses typically are not self-replicating.
- **Ransomware**: Ransomware is malware that locks a computer or device (Locker ransomware) or encrypts data (Crypto ransomware) on an infected endpoint with an encryption key that only the attacker knows, thereby making the data unusable until the victim pays a ransom (usually in cryptocurrency, such as Bitcoin). Reveton and LockeR are two examples of Locker ransomware. Locky, TeslaCrypt/EccKrypt, Cryptolocker, and Cryptowall are examples of Crypto ransomware.
- **Anti-AV**: Anti-AV is malware that disables legitimately installed antivirus software on the compromised endpoint, thereby preventing automatic detection and removal of other malware.
- **Logic bombs**: A logic bomb is malware triggered by a specified condition, such as a given date or a particular user account being disabled.
- **Back doors**: A back door is malware that allows an attacker to bypass authentication to gain access to a compromised system.
- **Root kits**: A root kit is malware that provides privileged (root-level) access to a computer. Root kits are installed in the BIOS of a machine, which means operating system-level security tools cannot detect them.
- **Boot kits**: A boot kit is malware that is a kernel-mode variant of a root kit, commonly used to attack computers that are protected by full-disk encryption.
- **Spyware and adware**: Spyware and adware are types of malware that collect information, such as internet surfing behavior, login credentials, and financial account information on an infected endpoint. Spyware often changes browser and other software settings, and slows computer and internet speeds on an infected endpoint. Adware is spyware that displays annoying advertisements on an infected endpoint, often as popup banners.

Early malware typically consisted of viruses that displayed annoying but relatively benign errors, messages, or graphics.

Key Idea

- The first computer virus was Elk Cloner, written in 1982 by a ninth-grade high school student near Pittsburgh, Pennsylvania. Elk Cloner was a relatively benign boot sector virus that displayed a poem on the fiftieth time that an infected floppy disk was inserted into an Apple II computer.
- The first PC virus was a boot sector virus, written in 1986, called Brain. Brain also was relatively benign and displayed a message with the actual contact information for the creators of the virus. Brain was written by two Pakistani brothers who created the virus so that they could track piracy of their medical software.

Key Terms

- A **boot sector virus** targets the boot sector or master boot record (MBR) of an endpoint's storage drive or other removable storage media.
- A **boot sector** contains machine code that is loaded into an endpoint's memory by firmware during the startup process, before the operating system is loaded.
- A **master boot record (MBR)** contains information about how the logical partitions (or file systems) are organized on the storage media and an executable boot loader that starts up the installed operating system.
- A **floppy disk** is a removable magnetic storage medium commonly used from the mid-1970s until about 2007, when it was largely replaced by compact discs and removable USB storage devices. Floppy disks typically were available in 8-inch, 5¼-inch, and 3½-inch sizes with capacities from 90 kilobytes to 200 megabytes.

One of the first computer worms to gain widespread notoriety was the Morris worm, written by a Harvard and Cornell University graduate student, Robert Tappan Morris, in 1988. The worm exploited weak passwords and known vulnerabilities in several Unix programs and spread rapidly across the early internet (the worm infected up to an estimated 10 percent of all Unix machines connected to the internet at that time, or about 6,000 computers), sometimes infecting a computer numerous times to the point that it was rendered useless – an example of an early DoS attack. The U.S. Government Accountability Office (GAO) estimated the damage caused by the Morris worm between US$100,000 and US$10 million.

Unfortunately, in the more than 35 years since these early examples of malware, modern malware has evolved and is used for far more sinister purposes. Examples of modern malware include:

- **WannaCry**: In a period of just 24 hours in May 2017, the WannaCry ransomware attack infected more than 230,000 vulnerable Windows computers in more than 150 countries worldwide. Although the attack was quickly halted after the discovery of a "kill switch," the total economic damage is estimated between hundreds of millions of U.S. dollars to as much as US$4 billion, despite the perpetrators collecting only 327 ransom payments totaling about US$130,000.
- **HenBox**: HenBox typically masquerades as legitimate Android system and VPN apps, and sometimes drops and installs legitimate versions of other apps as a decoy. The primary goal of the HenBox apps appears to be to spy on those who install them. By using traits similar to legitimate apps, for example, copycat iconography and app or package names, HenBox lures victims into downloading and installing the malicious apps from third-party, non-Google Play app stores that often have fewer security and vetting procedures for the apps they host. As is the case with other Android malware, some apps also may be available on forums or file-sharing sites, or even may be sent to victims as email attachments.
- **TeleRAT**: Telegram Bots are special accounts that do not require an additional phone number to set up and generally are used to enrich Telegram chats with content from external services or to get customized notifications and news. TeleRAT abuses Telegram's Bot API for C2 and data exfiltration.

- **Rarog**: Rarog is a cryptocurrency-mining trojan that has been sold on various underground forums since June 2017 and has been used by countless criminals since then. Rarog has been primarily used to mine the Monero cryptocurrency. However, it can mine others. It comes equipped with several features, including providing mining statistics to users, configuring various processor loads for the running miner, the ability to infect USB devices, and the ability to load additional dynamic link libraries (DLLs) on the victim device. Rarog provides an affordable way for new criminals to gain entry using this particular type of malware. Other examples of cryptocurrency miners include Coinhive, JSE-Coin, Crypto-Loot, and CoinImp.

Key Terms

- A **dynamic link library (DLL)** is a type of file used in Microsoft operating systems that enables multiple programs to simultaneously share programming instructions contained in a single file to perform specific functions.

Modern malware typically is stealthy and evasive, and now plays a central role in a coordinated attack against a target.

Advanced malware leverages networks to gain power and resilience, and can be updated, just like any other software application, so that an attacker can change course and dig deeper into the network or make changes and enact countermeasures.

This advanced malware is a fundamental shift compared to earlier types of malware, which generally were independent agents that simply infected and replicated themselves. Advanced malware increasingly has become a centrally coordinated, networked application. In much the same way that the internet changed what was possible in personal computing, ubiquitous network access is changing what is possible in the world of malware. Now all malware of the same type can work together toward a common goal, with each infected endpoint expanding the attack foothold and increasing the potential damage to the organization.

Important characteristics and capabilities of advanced malware include:

- **Distributed, fault-tolerant architecture**: Advanced malware takes full advantage of the resiliency built into the internet itself. Advanced malware can have multiple control servers distributed all over the world with multiple fallback options, and also can leverage other infected endpoints as communication channels, thus providing a near infinite number of communication paths to adapt to changing conditions or update code as needed.
- **Multifunctionality**: Updates from C2 servers also can completely change the functionality of advanced malware. This multifunctional capability enables an attacker to use various endpoints strategically to accomplish specific desired tasks, such as stealing credit card numbers, sending spam containing other malware payloads (such as spyware), or installing ransomware for the purpose of extortion.
- **Polymorphism and metamorphism**: Some advanced malware have entire sections of code that serve no purpose other than to change the signature of the malware, thus producing an infinite number of unique signature hashes for even the smallest of malware programs. Techniques such as polymorphism and metamorphism are used to avoid detection by traditional signature-based anti-malware tools and software. For example, a change of just a single character or bit of the file or source code completely changes the hash signature of the malware.

- **Obfuscation**: Advanced malware often uses common obfuscation techniques to hide certain binary strings that are characteristically used in malware and therefore are easily detected by anti-malware signatures, or to hide an entire malware program.

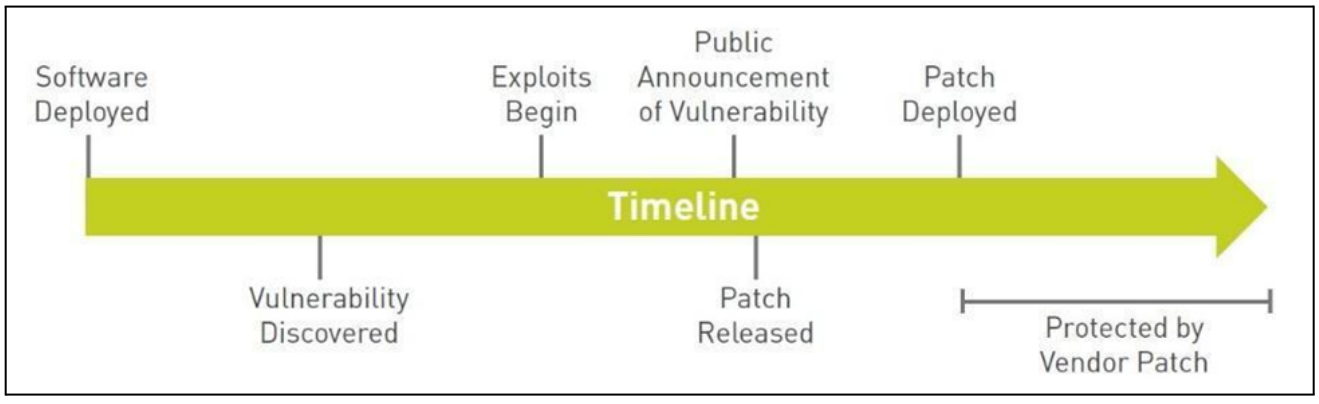
Key Terms

- **Polymorphism** alters part of the malware code with every iteration, such as the encryption key or decryption routine, but the malware payload remains unchanged.
- **Metamorphism** uses more advanced techniques than polymorphism to alter malware code with each iteration. Although the malware payload changes with each iteration (for example, by using a different code structure or sequence or by inserting unnecessary code to change the file size), the fundamental behavior of the malware payload remains unchanged.
- A **hash signature** is a cryptographic representation of an entire file or program's source code.
- **Obfuscation** is a programming technique used to render code unreadable. It can be implemented by using a simple substitution cipher, such as an exclusive or XOR operation, in which the output is true only when the inputs are different (for example, TRUE and TRUE equals FALSE, but TRUE and FALSE equals TRUE), or by using more sophisticated encryption algorithms, such as the Advanced Encryption Standard (AES). A packer also can be used to compress a malware program for delivery and then decompress it in memory at runtime.

1.12 Differentiate between vulnerabilities and exploits

An exploit is a type of malware that takes advantage of a vulnerability in installed endpoint or server software such as a web browser, Adobe Flash, Java, or Microsoft Office. An attacker crafts an exploit that targets a software vulnerability, causing the software to perform functions or execute code on behalf of the attacker.

Vulnerabilities routinely are discovered in software at an alarming rate. Vulnerabilities may exist in software when the software is initially developed and released, or vulnerabilities may be inadvertently created, or even re-introduced, when subsequent version updates or security patches are installed. Security patches are developed by software vendors as quickly as possible after a vulnerability has been discovered in their software. However, an attacker may learn of a vulnerability and begin exploiting it before the software vendor is aware of the vulnerability or has an opportunity to develop a patch. This delay between the discovery of a vulnerability and development and release of a patch is known as a zero-day threat (or exploit). It may be months or years before a vulnerability is announced publicly. After a security patch becomes available, time inevitably is required for organizations to properly test and deploy the patch on all affected systems. During this time, a system running the vulnerable software is at risk of being exploited by an attacker (see figure below).



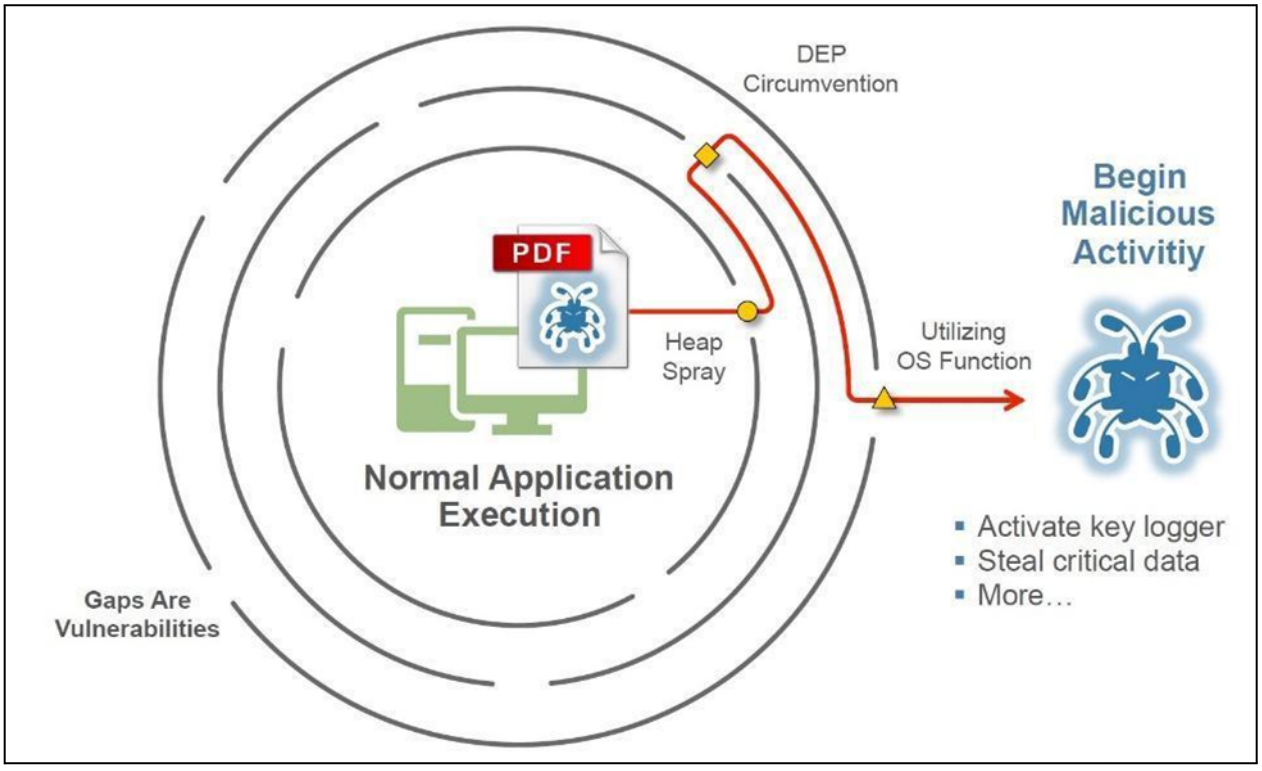
Exploits can be embedded in seemingly innocuous data files (such as Microsoft Word documents, PDF files, and webpages), or they can target vulnerable network services. Exploits are particularly dangerous because they often are packaged in legitimate files that do not trigger anti-malware (or antivirus) software and therefore are not easily detected.

Creation of an exploit data file is a two-step process. The first step is to embed a small piece of malicious code within the data file. However, the attacker still must trick the application into running the malicious code. Thus, the second part of the exploit typically involves memory corruption techniques that allow the attacker's code to be inserted into the execution flow of the vulnerable software. After that happens, a legitimate application, such as a document viewer or web browser, will perform actions on behalf of the attacker, such as establishing communication and providing the ability to upload additional malware to the target endpoint. Because the application being exploited is a legitimate application, traditional signature-based antivirus and allow-list software has virtually no effectiveness against these attacks.

Although there are many thousands of exploits, they all rely on a small set of core techniques that change infrequently. For example, a heap spray is an attempt to insert the attacker's code into multiple locations within the memory heap in the hope that one of those locations will be called by the process and executed. Three to five core techniques typically must be used to exploit an application.

Key Idea

- Regardless of the attack or its complexity, for the attack to be successful the attacker must execute a series of these core exploit techniques in sequence, like navigating a maze to reach its objective.



Key Terms

- **Heap spray** is a technique used to facilitate arbitrary code execution by injecting a certain sequence of bytes into the memory of a target process.

1.12.1 Differentiate between various business email compromise attacks

BEC (business email compromise) is a form of e-mail email scam where the attacker directs the organization to defraud. Business email marketing is a major and growing issue affecting businesses of all sizes and industries around the world. Organizations have been exposed to billions of dollars in potential losses as a result of BEC programs.

BEC programs are divided into five categories by the FBI:

CEO fraud: In this type of fraud, the attacker pretends to be the CEO of a company or an official and then sends an email to someone in the finance department requesting that the money be transferred to an account controlled by the attacker.

Compromise Account: The hacker gains access to the employee's email account, which is then used to claim payments from merchants. Payments are then sent to the attacker's phony accounts.

False Invoice System: This is a common strategy used by attackers to target overseas providers. The scam disguises itself as a provider and demands that funds be transferred to fake accounts.

Pretending to be a lawyer: This is when the attacker pretends to be a lawyer or an attorney.

Data Theft: These attacks often target HR employees in an attempt to obtain personal or sensitive information about company executives, such as CEOs and CFOs. This information can be used in subsequent attacks, such as CEO fraud.

1.12.2 Identify different methodologies for social engineering

The term “social engineering” means the use of various manipulation techniques to cause human error that allows attackers access into a system. The most common type of social engineering attack is phishing. The hacker sends an email that appears to come from a legitimate source. This email can include a link to a site that asks for user credentials, an attachment that installs malware on the user’s computer, etc.

1.12.3 Identify the chain of events that result from social engineering

The basic requirement for social engineering to work is to ensure that the user does not realize that something is wrong. Typically, a successful social engineering attack is accomplished either through a routine the user regularly goes through (for example, logging in to a Twitter account) or by arousing the user’s emotions so that they override normal rational thought. For example, a hacker might call the help desk, pretend to be a vice president of the company, and immediately demand their password or the help desk representative will be fired. The following are examples of the chain of events that have occurred in attacks initiated with social engineering.

- In April 2013, the Twitter account of the Associated Press (AP) was compromised and posted tweets that clearly were false. An employee had clicked on a link to a page that requested the login details of the AP Twitter account, and logged in.
- In 2013, Target lost customer data. By the end of 2015, the company announced a loss of $162 million due to this data breach, which happened because Target provided an HVAC vendor remote access to its internal network. An employee of that vendor opened an attachment, which then installed malware that allowed the hacker to gain access to Target's internal network and take over some Point of Sale (POS) devices.
- In 2016, emails belonging to the Democratic National Committee (DNC) were published publicly. The hacker sent an email to DNC employees, supposedly from Google, telling people their accounts had been compromised and asking them to reset their passwords. Unfortunately, the email included a link to a form provided by the hacker that asked for information (for "verification") and then reset the password. This action allowed the hacker to learn the correct passwords and use them to access the emails.

1.12.4 References

- "Internet Security Threat Report, Volume 23." Symantec. 2018, https://www.symantec.com/security-center/threat-report

1.13 Identify what chain of events follows an attack

Malicious network attacks have been on the rise in the last decade. One of the most damaging attacks, often executed over DNS, is accomplished through command and control, also called C2 or C&C.

The attacker starts by infecting a computer, which may sit behind a firewall. This can be done in a variety of ways:

- Via a phishing email that tricks the user into following a link to a malicious website or opening an attachment that executes malicious code.
- Through security holes in browser plugins.
- Via other infected software.

Once communication is established, the infected machine sends a signal to the attacker's server looking for its next instruction. The infected computer will carry out the commands from the attacker's C2 server and may install additional software, at which point the attacker will complete control of the victim's computer and can execute any code. The malicious code will typically spread to more computers, creating a botnet – a network of infected machines. In this way, an attacker who is not authorized to access a company's network can obtain full control of that network.

What Can Hackers Accomplish?

- **Data theft**. Sensitive company data, such as financial documents, can be copied or transferred to an attacker's server.
- **Shutdown**. An attacker can shut down one or several machines, or even bring down a company's network.
- **Reboot**. Infected computers may suddenly and repeatedly shutdown and reboot, which can disrupt normal business operations.

- **Distributed denial of service**. DDoS attacks overwhelm servers or networks by flooding them with internet traffic. Once a botnet is established, an attacker can instruct each bot to send a request to the targeted IP address, creating a jam of requests for the targeted server. The result resembles traffic clogging a highway – legitimate traffic to the attacked IP address is denied access. This type of attack can be used to take a website down.

1.13.1 References

- Command and Control Explained. https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained

1.14 Differentiate between the functional aspects of bots and botnets

Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyberattack strategy. Spamming and phishing are commonly employed techniques to deliver malware and exploits to an endpoint via an email executable or a web link to a malicious website. After an endpoint is compromised, an attacker typically installs back doors, remote access trojans, and other malware to ensure persistence. An attacker often uses compromised endpoints ("bots") to perpetrate much larger-scale attacks against other organizations or networks as part of a botnet.

Key Terms

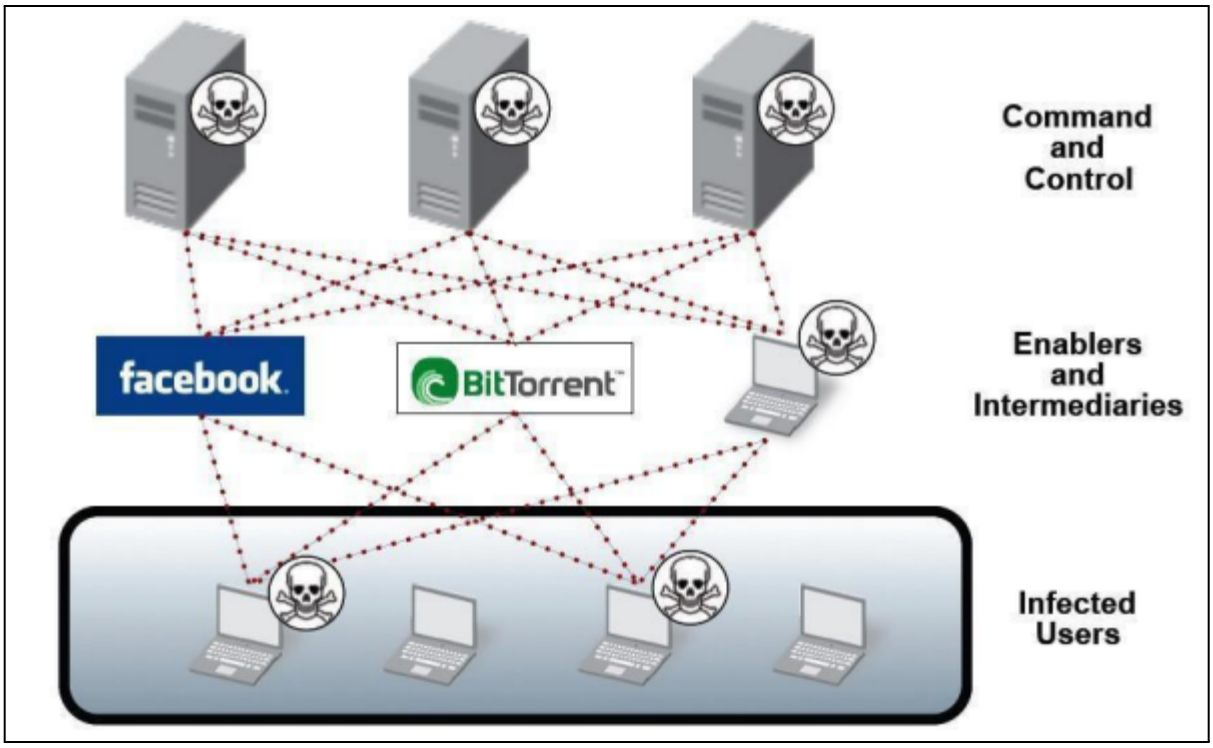
- **Bots (or zombies)** are individual endpoints infected with advanced malware that enables an attacker to take control of the compromised endpoint.
- A **botnet** is a network of bots (often tens of thousands or more) working together under the control of attackers using numerous servers.

Bots and botnets are notoriously difficult for organizations to detect and defend against using traditional anti-malware solutions.

1.14.1 Describe the type of IoT devices that are part of a botnet attack

In a botnet, advanced malware works together toward a common objective, with each bot increasing the power and destructiveness of the overall botnet. The botnet can evolve to pursue new goals or adapt as different security countermeasures are deployed. Communication between the individual bots and the larger botnet through C2 servers provides resiliency in the botnet.

The flexibility and ability of botnets to evade defenses presents a significant threat to organizations. The ultimate impact of a botnet is largely left up to the attacker, from sending spam one day to stealing credit card data the next and far beyond, because many cyberattacks go undetected for months or even years.



Botnets themselves are dubious sources of income for cybercriminals. Botnets are created by cybercriminals to harvest computing resources (bots). Control of botnets (through C2 servers) then can be sold or rented out to other cybercriminals.

The key to “taking down” or “decapitating” a botnet is to separate the bots (infected endpoints) from their brains (C2 servers). If the bots cannot get to their servers, they cannot get new instructions, upload stolen data, or do any of the things that make botnets so unique and dangerous.

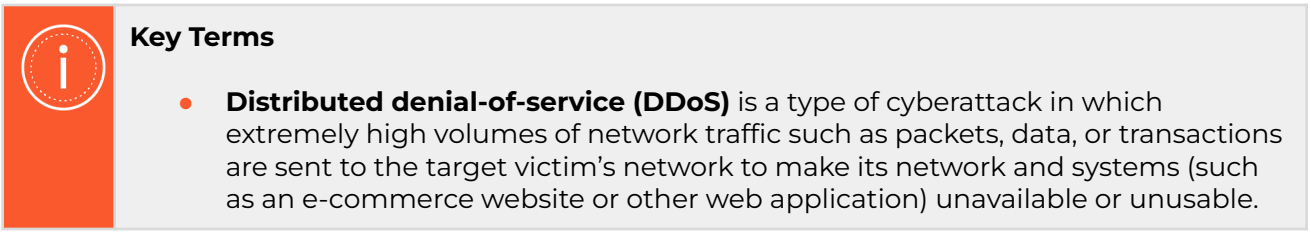
Although this approach may seem straightforward, extensive resources typically are required to map the distributed C2 infrastructure of a botnet, and this approach almost always requires an enormous amount of investigation, expertise, and coordination between numerous industry, security, and law enforcement organizations worldwide.

Disabling of C2 servers often requires both physically seizing the servers and taking ownership of the domain and/or IP address range associated with the servers. Technical teams, legal teams, and law enforcement must coordinate closely to disable the C2 infrastructure of a botnet. Many botnets have C2 servers all over the world and will specifically function in countries that have little or no law enforcement for internet crimes.

Further complicating takedown efforts is the fact that a botnet almost never relies on a single C2 server but rather uses multiple C2 servers for redundancy purposes. Each server also typically is insulated by a variety of intermediaries to hide the true location of the server. These intermediaries include P2P networks, blogs, and social networking sites, and even communications that proxy through other infected bots. These evasion techniques make even finding C2 servers a considerable challenge.

Most botnets also are designed to withstand the loss of a C2 server, which means that the entire botnet C2 infrastructure must be disabled almost simultaneously. If any C2 server is accessible or any of the fallback options survives, the bots will be able to get updates and rapidly populate a completely new set of C2 servers, and the botnet will quickly recover. Thus, even a single C2 server remaining functional for even a small amount of time can give an attacker the window needed to update the bots and recover the entire botnet.

According to a 2019 botnet threat report, Spamhaus Malware Labs identified and issued Spamhaus Block List (SBL) listings for 17,602 botnet C2 servers on 1,210 different networks.



Key Terms

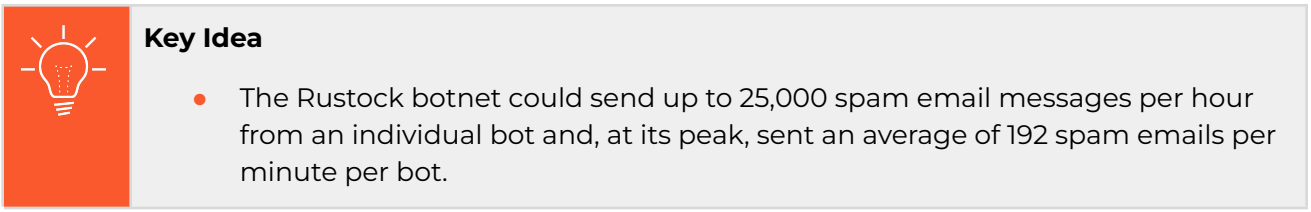
- **Distributed denial-of-service (DDoS)** is a type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make its network and systems (such as an e-commerce website or other web application) unavailable or unusable.

Botnet C2 servers are used to control infected endpoints (bots) and to exfiltrate personal and/or valuable data from bots. Botnets can be easily scaled up to send massive volumes of spam, spread ransomware, launch distributed denial-of-service (DDoS) attacks, commit click-fraud campaigns, and/or mine cryptocurrency (such as Bitcoin).

Spamming botnets

The largest botnets often are dedicated to sending spam. The premise is straightforward: The attacker attempts to infect as many endpoints as possible, and the endpoints then can be used to send out spam email messages without the end users' knowledge. The relative impact of this type of bot on an organization may seem low initially, but an infected endpoint sending spam could consume additional bandwidth and ultimately reduce the productivity of the users and even the network itself. Perhaps more consequential is the fact that the organization's email domain and IP addresses also could easily become listed by various real-time blackhole lists (RBLs), thus causing legitimate emails to be labeled as spam and blocked by other organizations, and damaging the reputation of the organization.

The Rustock botnet is an example of a spamming botnet.



Key Idea

- The Rustock botnet could send up to 25,000 spam email messages per hour from an individual bot and, at its peak, sent an average of 192 spam emails per minute per bot.

Rustock is estimated to have infected more than 2.4 million computers worldwide. In March 2011, the U.S. Federal Bureau of Investigation (FBI), working with Microsoft and others, took down the Rustock botnet, which had operated for more than five years and at the time was responsible for sending up to 60 percent of the world's spam.

Distributed denial-of-service botnets

A DDoS attack is a type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make their network and systems (such as an e-commerce website or other web application) unavailable or unusable. A DDoS botnet uses bots as part of a DDoS attack, overwhelming a target server or network with traffic from a large number of bots. In such attacks, the bots themselves are not the target of the attack. Instead, the bots are used to flood some other remote target with traffic. The attacker leverages the massive scale of the botnet to generate traffic that overwhelms the network and server resources of the target.

Unlike other types of cyberattacks, a DDoS attack does not typically employ a prolonged, stealthy approach. Instead, a DDoS attack usually is a highly visible brute-force attack that is intended to rapidly cause damage to the victim's network and systems infrastructure and to its business and reputation.

DDoS attacks often target specific organizations for personal or political reasons, or to extort a ransom payment in exchange for stopping the DDoS attack. DDoS attacks often are used by hacktivists to promote or protest a particular political agenda or social cause. DDoS attacks also may be used for criminal extortion purposes to extract a ransom payment in exchange for ending the attack.

DDoS botnets represent a dual risk for organizations: The organization itself can be the target of a DDoS attack. And even if the organization isn't the ultimate target, any infected endpoints participating in the attack will consume valuable network resources and facilitate a criminal act, albeit unwittingly.

A DDoS attack also can be used as part of a targeted strategy for a later attack. While the victim organization is busy defending against the DDoS attack and restoring the network and systems, the attacker can deliver an exploit to the victim network (for example, by causing a buffer overflow in an SQL database) that will enable a malware infection and establish a foothold in the network. The attacker then can return later to expand the (stealthy) attack and extract stolen data.

Examples of recent DDoS attacks include attacks against World of Warcraft Classic and Wikipedia in September 2019.

Financial botnets

Financial botnets, such as ZeuS and SpyEye, are responsible for the direct theft of funds from all types of enterprises. These types of botnets typically are not as large as spamming or DDoS botnets, which grow as large as possible for a single attacker. Instead, financial botnets often are sold as kits that allow attackers to license the code and build their own botnets. The impact of a financial breach can be enormous, including the breach of sensitive consumer and financial information, thus leading to significant financial, legal, and brand damage.

As reported by Tech Republic: *"A Mirai botnet variant was used in attacks against at least one financial sector company in January 2018 – possibly the first time an IoT botnet has been observed in use in a DDoS attack since the Mirai botnet took down multiple websites in 2017, according to a Thursday report from Recorded Future."*

1.14.2 References

- "Spamhaus Botnet Threat Report 2019." Spamhaus Malware Labs. January 2020, https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
- Oleg Kuprev, Ekaterina Badovskaya, and Alexander Gutnikov. "DDoS attacks in Q3 2019." Kaspersky. November 11, 2019, https://securelist.com/ddos-report-q3- 2019/94958/
- Rayome, Alison DeNisco. "Mirai variant botnet launches IoT DDoS attacks on financial sector." Tech Republic. April 5, 2018, https://www.techrepublic.com/article/miraivariant-botnet-launches-iot-ddos-attacks-on-financial-sector/

1.15 Differentiate the TCP/IP roles in DDoS attacks

1.15.1 Differentiate between DoS and DDoS

DoS

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

SYN flood – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to. Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system so that it can't be accessed or used.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

- The attacker can leverage the greater volume of machines to execute a seriously disruptive attack.
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide).
- It is more difficult to shut down multiple machines than one.
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

DDoS

A Distributed Denial of Service (DDoS) attack is a variant of a DoS attack that employs very large numbers of attacking computers to overwhelm the target with bogus traffic. To achieve the necessary scale, DDoS attacks are often performed by botnets, which can co-opt millions of infected machines to unwittingly participate in the attack, even though they are not the target of the attack itself. Instead, the attacker leverages the massive number of infected machines to flood the remote target with traffic and cause a DoS.

Though the DDoS attack is a type of DoS attack, it is significantly more popular in its use due to the features that differentiate and strengthen it from other types of DoS attacks.

- The attacking party can execute an attack of disruptive scale as a result of the large network of infected computers—effectively a “zombie army”—under their command.
- The (often worldwide) distribution of attacking systems makes it very difficult to detect where the actual attacking party is located.
- It is difficult for the target server to recognize the traffic as illegitimate and reject it on entry because of the seemingly random distribution of attacking systems.
- DDoS attacks are much more difficult to shut down than other DoS attacks due to the number of machines that must be shut down, as opposed to shutting down just one machine.

DDoS attacks often target specific organizations (enterprise or public) for personal or political reasons, or to extort payment from the target in return for stopping the DDoS attack. The damages of a DDoS attack are typically in time and money lost from the resulting downtime and lost productivity.

Examples of DDoS attacks are abundant. In January 2012, hacktivist cybergroup Anonymous conducted an attack on multiple major supporters of the Stop Online Piracy Act (SOPA). In dissent of SOPA, Anonymous executed DDoS attacks that disabled the websites of the US Justice Department, the Federal Bureau of Investigations (FBI), the White House, the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), Universal Music Group, and Broadcast Music, Inc (BMI). To facilitate the attack, Anonymous built its botnet using an unconventional model that allowed users wishing to support the organization to offer their computers as a bot for the attacks.

Users who wanted to volunteer support could join the Anonymous botnet by clicking links that the organization posted in various locations online, such as Twitter.

The DDoS attack is also leveraged as a weapon of cyber warfare. For example, in 2008 during the South Ossetia war, Georgian government websites were crippled by what is believed to have been Russian criminal gangs under the auspices of the Russian security services. The attack was made just prior to Russia's initial attacks on Georgian soil.

There are a number of DDoS mitigation techniques that organizations can implement to minimize the possibility of an attack. Network security infrastructure should include DDoS detection tools that can identify and block both exploits and tools that attackers use to launch an attack. Additionally, network administrators can create profiles to observe and control specific floods of traffic (i.e. SYN floods, UDP, and ICMP floods). Through looking at all traffic in aggregate, thresholds can be set to monitor and cut behaviors that indicate a possible DDoS attack.

1.15.2 References

- Denial of service attack (DoS), https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
- Distributed Denial of Service Attack (DDoS), https://www.paloaltonetworks.com/cyberpedia/what-is-a-ddos-attack

1.16 Describe advanced persistent threats

Advanced persistent threats (APTs) are a class of threats that are far more deliberate and potentially devastating than other types of cyberattacks. As its name implies, an APT has three defining characteristics. An APT is:

- **Advanced**: Attackers use advanced malware and exploits and typically also have the skills and resources necessary to develop additional cyberattack tools and techniques, and may have access to sophisticated electronic surveillance equipment, satellite imagery, and even human intelligence assets.
- **Persistent**: An APT may take place over a period of several years. The attackers pursue specific objectives and use a "low-and-slow" approach to avoid detection. The attackers are well organized and typically have access to substantial financial backing, such as from a nation-state or organized criminal organization, to fund their activities.
- **Threat**: An APT is deliberate and focused, rather than opportunistic. APTs are designed to cause real damage, including significant financial loss, destruction of systems and infrastructure, and physical harm and loss of life.

Recent APT threat actors include:

- **Lazarus** (also known as APT38, Gods Apostles, Gods Disciples, Guardians of Peace, ZINC, Whois Team, and Hidden Cobra). The Lazarus APT group is a threat actor linked to North Korea and believed to be behind attacks against more than 16 organizations in at least 11 countries, including the Bangladesh cyber heist (US$81 million was surreptitiously transferred from the New York Federal Reserve Bank account of Bangladesh in February 2016), the Troy Operation (attacks against South Korean infrastructure in 2013), the DarkSeoul Operation (malware-based

attacks that wiped tens of thousands of hard drives belonging to South Korean television networks and banks in March 2013), and the Sony Picture hack (employees' emails and personal information including salaries, addresses, and Social Security numbers revealed, unreleased movies posted on file sharing sites, and internal computer systems shut down in 2014).

- **Fancy Bear** (also known as APT28, Sofacy, Sednit, and Tsar Team). Fancy Bear is a Russia-based APT threat actor that has been operating since 2010. Recent targets and attacks have included the German Think Tank Attacks (2019), German elections (2017), World Anti-Doping Agency attack (2016), U.S. Democratic National Committee breach (2016), and Operation "Pawn Storm" (2014).
- **MONSOON** (also known as Patchwork, APT -C-09, Chinastrats, Dropping Elephant, and Quilted Tiger). MONSOON is an APT threat actor that appears to have begun in 2014 in India. According to Forcepoint Security Labs, "The overarching campaign appears to target both Chinese nationals within different industries and government agencies in Southern Asia … The malware components used in MONSOON typically are distributed through [weaponized] documents sent through email to specifically chosen targets. Themes of these documents are usually political in nature and taken from recent publications on topical current affairs. Several malware components have been used in this operation including Unknown Logger Public, TINYTYPHON, BADNEWS, and an AutoIt backdoor."

1.16.1 References

- "Top 25 Threat Actors – 2019 Edition." SBS CyberSecurity. December 12, 2019, https://sbscyber.com/resources/top-25-threat-actors-2019-edition
- Paganini, Pierluigi. "US blames North Korea for the $81 million Bangladesh cyber heist." Security Affairs. March 24, 2017, http://securityaffairs.co/wordpress/57396/cyber-crime/bangladesh-cyber-heist.html
- Paganini, Pierluigi. "Hackers hit South Korea also spread spyware to steal military secrets." Security Affairs. July 9, 2013, http://securityaffairs.co/wordpress/16014/hacking/hackers-hit-south-korea-spyware-steal-military-secrets.html
- Weisman, Aly. "A Timeline of the Crazy Events in the Sony Hacking Scandal." Business Insider. December 9, 2014, http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12
- "Top 25 Threat Actors – 2019 Edition." SBS CyberSecurity. December 12, 2019, https://sbscyber.com/resources/top-25-threat-actors-2019-edition
- "Advanced Persistent Threat Groups." FireEye. 2020, https://www.fireeye.com/current-threats/apt-groups.html
- "Top 25 Threat Actors – 2019 Edition." SBS CyberSecurity. December 12, 2019, https://sbscyber.com/resources/top-25-threat-actors-2019-edition
- Settle, Andy, Nicholas Griffin, and Abel Toro. "Monsoon – Analysis of an APT Campaign: Espionage and Data Loss Under the Cover of Current Affairs." Forcepoint Security Labs. 2016, https://www.forcepoint.com/sites/default/files/resources/files/forcepoint-security-labs-monsoon-analysis-report.pdf

1.17 Describe risks with Wi-Fi networks

With the explosive growth in the number of mobile devices over the past decade, wireless (Wi-Fi) networks now are everywhere. Of course, as a security professional, your first concern when trying to get connected is, “How secure is this Wi-Fi network?” But for the average user, the unfortunate reality is that Wi-Fi connectivity is more about convenience than security.

Thus, the challenge is not only to secure your Wi-Fi networks but also to protect the mobile devices that your organization’s employees use to perform work and access potentially sensitive data, regardless of where they are or whose network they’re on.Wi-Fi security begins and ends with authentication. If you can’t control who has access to your wireless network, then you can’t protect your network.

1.17.1 Differentiate between common types of Wi-Fi attacks

Wired Equivalent Privacy
The Wired Equivalent Privacy (WEP) protocol was the wireless industry’s first attempt at security. As its name falsely implies, WEP was intended to provide data confidentiality equivalent to the security of a wired network. However, WEP had many well-known and well-publicized weaknesses, such as its weak random value, or initialization vector (IV), and key-generation algorithm, and wasn’t effective for establishing a secure wireless network.

Wi-Fi Protected Access (WPA/WPA2/WPA3)
To learn more about this, please refer to section 1.17.2.

Evil Twin

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with “free Wi-Fi access.”

The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can’t easily target a specific victim, because the attack depends on the victim initiating the connection.

A slight variation on this approach is to use a more specific name that mimics a real access point normally found at a particular location, the Evil Twin. For example, if your local airport provides Wi-Fi service and calls it “Airport Wi-Fi,” the attacker might create an access point with the same name using an access point that has two radios. Average users cannot easily discern when they are connected to the real access point or a fake one, so this approach would catch a greater number of users than a method that tries to attract victims at random. Still, the user must select the network, so a bit of chance is involved in trying to reach a particular target.

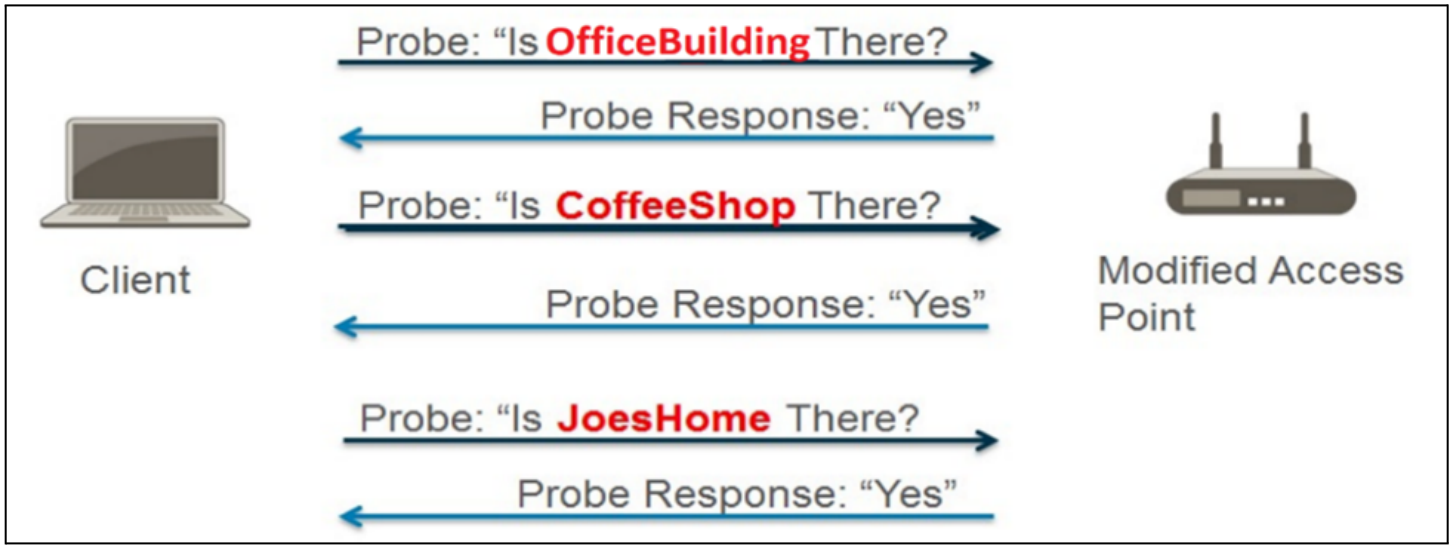
The main limitation of the Evil Twin attack is that the attacker can’t choose the victim. In a crowded location, the attacker will be able to get many people connecting to the wireless network to unknowingly expose their account names and passwords. However, it’s not an effective approach if the goal is to target employees in a specific organization.

Jasager

If you want to understand a more targeted approach than the Evil Twin attack, think about what happens when you bring your wireless device back to a location that you've previously visited. For example, when you bring your laptop home, you don't have to choose which access point to use, because your device remembers the details of wireless networks to which it has previously connected. The same practice applies when you visit the office or your favorite coffee shop.

Your mobile device detects when it's in proximity to a previously known wireless network by sending a beacon out to discover if a preferred network is within range. Under normal conditions, when a wireless device sends out a beacon, the non-matching access points ignore it. The beacon goes unanswered, except when it comes within the proximity of the preferred network.

The Jasager attack takes a more active approach toward beacon requests. Jasager (German for "the yes-man") responds to all beacon requests, thus taking a very permissive approach toward who can connect. The user doesn't have to manually choose the attacker's access point. Instead, the attacker pretends to be whichever access point the user normally connects to. Instead of trying to get victims to connect at random, now the attacker simply needs to be within proximity of the target.



This process intercepts the communication from laptops, mobile phones, and tablets. Many, if not most, 3G/4G/LTE mobile devices automatically switch to Wi-Fi when they recognize that they are near a network that they know.

An attacker can use the same method to capture WPA2 handshake packets to disconnect users from a Wi-Fi network by using forged deauthentication packets. Users that reconnect unwittingly will connect to the modified access point. Unlike the Evil Twin attack, the attacker doesn't have to just wait for a victim to connect to the modified access point; with this approach, everyone in the vicinity will automatically connect and become a potential victim.

Jasager runs on any number of devices, but perhaps one of the most effective ways to employ it is with the Pineapple access point. The Pineapple is simply an access point with modified firmware that embeds several tools for wireless "penetration" testing. It also has several accessories such as support for cellular USB cards to provide network connectivity when it is otherwise unavailable at the target

location, and battery packs to operate as a standalone unit. It's also easily concealed because it can be disguised within any number of housings typically found plugged in at the office.

After the victim connects to a malicious access point, the man-in-the-middle attack can proceed, and the attacker not only can observe and capture network traffic, but also modify it.

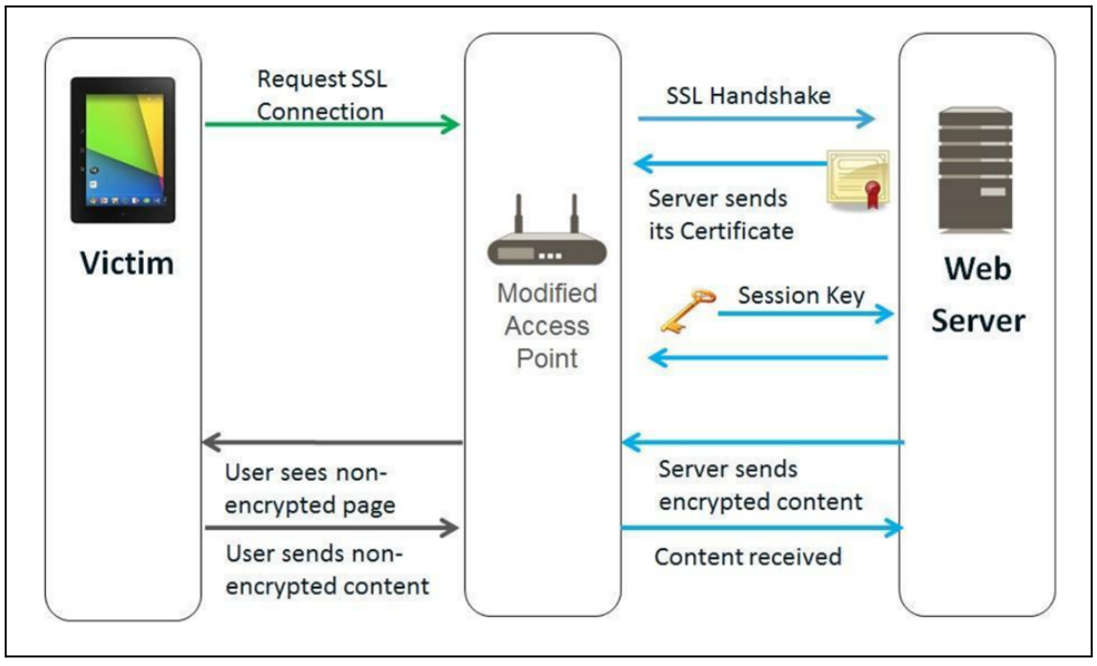
SSLstrip

After a user connects to a compromised Wi-Fi network or to an attacker's Wi-Fi network masquerading as a legitimate network, the attacker can control the content that the victim sees. The attacker simply intercepts the victim's web traffic, redirects the victim's browser to a web server that it controls, and serves whatever content the attacker desires.

A man-in-the middle attack can be used to steal a victim's online banking or corporate email account credentials. Normally, this type of traffic would be considered safe because the webpage typically uses Secure Sockets Layer (SSL) encryption. However, while the average user thinks a padlock icon appearing somewhere in their browser's address bar means that their browser is secure, that is not correct.

Additionally, the padlock appears differently, and in different locations, in different browsers. How does the padlock appear in Internet Explorer? What about Mozilla Firefox, Google Chrome, and Apple Safari? And it appears differently on different smartphones and tablets, too. It's no wonder that typical end users and even many security professionals can be easily tricked.

SSLstrip strips SSL encryption from a "secure" session. When a user connecting to a compromised Wi-Fi network attempts to initiate an SSL session, the modified access point intercepts the SSL request (see Figure 1-6). The modified access point then completes the SSL session on behalf of the victim's device. Then the SSL tunnel between the victim's device and the legitimate secure web server is terminated and decrypted on the modified access point, thus allowing the attacker to see the victim's credentials and other sensitive information in cleartext.



With SSLstrip, the modified access point displays a fake padlock in the victim's web browser. Webpages can display a small icon called a favicon next to a website address in the browser's address bar. SSLstrip replaces the favicon with a padlock that looks like SSL to an unsuspecting user.

Key Terms

- A **favicon** ("favorite icon") is a small file containing one or more small icons associated with a particular website or webpage.

Emotet

Emotet is a trojan, first identified in 2014, that has long been used in spam botnets and ransomware attacks. Emotet variants use Wi-Fi spreader modules to scan Wi-Fi networks and look for vulnerable devices to infect. The Wi-Fi spreader module scans nearby Wi-Fi networks on an infected device and then attempts to connect to vulnerable Wi-Fi networks via a brute-force attack. After Emotet successfully connects to a Wi-Fi network, it scans for non-hidden shares and attempts another brute-force attack to guess usernames and passwords on other devices connected to the network. It then installs its malware payload and establishes C2 communications on newly infected devices.

1.17.2 Describe how to monitor your Wi-Fi network

Wi-Fi Protected Access (WPA/WPA2/WPA3)

WPA was published as an interim standard in 2003, quickly followed by WPA2 in 2004. WPA/WPA2 contains improvements to protect against the inherent flaws in WEP. These improvements include changes to the encryption to avoid many of the problems that plagued WEP.

WPA2 can be implemented in different ways. WPA2-Enterprise, also known as WPA2-802.1x mode, uses the Extensible Authentication Protocol (EAP) and Remote Authentication Dial-In User Service (RADIUS) for authentication. Numerous EAP types also are available for use in WPA2-Enterprise.

However, a pre-shared key (PSK) by far is the most common use, particularly in homes, small businesses, and guest Wi-Fi networks. WPA2-PSK can be implemented with just the AP and the client; neither a third-party 802.1x authentication server nor individual user accounts are required.

Key Terms

- The **Extensible Authentication Protocol (EAP)** is a widely used authentication framework that includes about 40 different authentication methods.
- **Remote Authentication Dial-In User Service (RADIUS)** is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize access to a system or service.
- A **pre-shared key (PSK)** is a shared secret, used in symmetric key cryptography, that has been exchanged between two parties communicating over an encrypted channel.

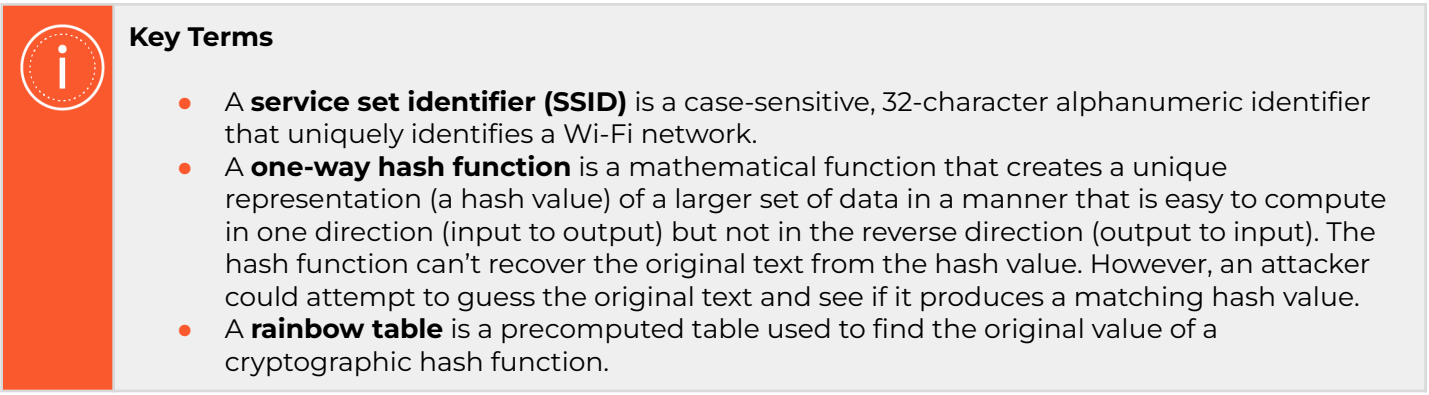
WPA2-PSK supports 256-bit keys, which require 64 hexadecimal characters. Because requiring users to enter a 64-hexadecimal character key is impractical, WPA2 includes a function that generates a 256-bit key based on a much shorter passphrase created by the administrator of the Wi-Fi network and the service set identifier (SSID) of the AP, used as a salt for the one-way hash function.

In WPA2, the name of the SSID is used for the salt. An easy way to make your Wi-Fi security stronger (and make rainbow table attacks impractical) is to change your SSID to something that isn't common or easily guessed.

To execute an attack on a WPA2 passphrase, an attacker needs to be able to test a large number of passphrase candidates. So, although WPA2 remains cryptographically secure (the key isn't recoverable by simple observation of the traffic, as with WEP), methods do exist to test passphrases offline by gathering the handshake packets between the AP and a legitimate user.

To collect the necessary packets to crack a WPA2 passphrase, an attacker could passively gather traffic when a legitimate user joins the network. This method requires time, however, because the attacker does not know when someone will join the network.

For an impatient attacker, the solution is to employ an active attack. If a legitimate user is already online, the attacker can force the user's client device to disconnect from the AP with forged deauthentication packets. After the client device is disconnected, it will automatically attempt to reconnect, thus providing the attacker with the handshake packets needed for offline passphrase analysis. Therefore, unlike with WEP, attacks on WPA2 do not require attackers to spend a significant amount of time in the proximity of the target network after the handshake packets have been captured.



Key Terms

- A **service set identifier (SSID)** is a case-sensitive, 32-character alphanumeric identifier that uniquely identifies a Wi-Fi network.
- A **one-way hash function** is a mathematical function that creates a unique representation (a hash value) of a larger set of data in a manner that is easy to compute in one direction (input to output) but not in the reverse direction (output to input). The hash function can't recover the original text from the hash value. However, an attacker could attempt to guess the original text and see if it produces a matching hash value.
- A **rainbow table** is a precomputed table used to find the original value of a cryptographic hash function.

Next, the attacker must recover (or find) the passphrase itself, which requires the following:

- **A test to check millions of potential passphrases until it finds the correct passphrase**. To avoid detection, an attacker can't use the actual target, because the victim could see this attack activity. The alternative is to use an offline method of testing that uses the handshake packets.
- **A methodology to guess passphrases**. The worst-case scenario is to "brute force" the passphrase, trying every possible combination of numbers and characters until a correct value is found. This effort can produce a correct result given enough time and computing power. However, a much faster method is to take educated guesses without having to resort to brute force. An attacker that uses educated guesses on possible passphrase candidates can attempt a much shorter list.

This basic process for recovering Wi-Fi passphrases is similar to cracking user passwords. In the early days of password cracking, an attacker might have knowledge of a target system's one-way hash function and a list of the system's user password hash values. However, the attacker could not decrypt the password, because the original text isn't recoverable from a hash. But by encrypting a list of words with the same one-way hash function (a dictionary attack), an attacker then can compare the resulting hash values with the hash values stored for the various user accounts on the system. So, although the password itself isn't decrypted, a given input that produces a given result, such as a password match, can be found. With the addition of more computing power, an attacker could try longer word lists and a greater number of variations of each word. The process for attacking WPA2 passphrases is similar.

WPA3 was published in 2018 and introduces security enhancements such as more robust brute-force attack protection, improved hot spot and guest access security, simpler integration with devices that have limited or no user interface (such as IoT devices), and a 192-bit security suite. Newer Wi-Fi routers and client devices likely will support both WPA2 and WPA3 to ensure backward compatibility in mixed environments.

According to the Wi-Fi Alliance, WPA3 features include improved security for IoT devices such as smart bulbs, wireless appliances, smart speakers, and other screen-free gadgets that make everyday tasks easier. The Wi-Fi Alliance is expected to support a one-touch setup system that will make devices without screens (such as IoT devices and smart speakers such as Google Home and Amazon Echo) easier to connect. It will be similar to the existing Wi-Fi Protected Setup protocol, which involves pushing a button on the router to connect a device.

According to a recent VentureBeat article, WPA3 also "supports a much stronger encryption algorithm than WPA2 … intended for industrial, defense, and government applications rather than homes and offices. Specifically, it includes a 192-bit security suite that's aligned with the Commercial National Security Algorithm (CNSA) Suite, a feature requested by the Committee on National Security Systems (CNSS), a part of the U.S. National Security Agency [NSA]."

WPA3 provides protection against brute-force dictionary attacks by implementing "a robust handshake [called the Dragonfly protocol, also referred to as Simultaneous Authentication of Equals] that isn't vulnerable to wireless exploits like KRACK, and it hardens security at the time when the network key is exchanged between a device and the access point." WPA3 also reduces the efficacy of common dictionary attacks by limiting the number of network password attempts on a per-user basis.

An attacker can trick victims into connecting to a wireless network that the attacker controls instead of breaking into a wireless network. These techniques are part of a larger set of attacks known as man-in-the-middle attacks. With a man-in-the-middle exploit in place on a Wi-Fi network, an attacker can produce or display practically any content, for example:

- If a user attempts to download a legitimate file, the attacker can send mobile malware instead.
- When a user attempts to visit a legitimate webpage, the attacker can alter the content to exploit a vulnerability that exists in the device's browser, thus allowing the attacker to further escalate an attack.
- Email addresses and financial account information can be harvested from the connected endpoint, thus enabling an attacker to create a very targeted and convincing phishing attack to trick even more users on a network into disclosing sensitive information.

1.17.3 References

- Wiggers, Kyle. “What is WPA3, why does it matter, and when can you expect it?” VentureBeat. May 19, 2018, https://venturebeat.com/2018/05/19/what-is-wpa3-why-does-it-matter-and-when-can-you-expect-it/
- Quinn, James. “Emotet Evolves With New Wi-Fi Spreader.” Binary Defense. February 7, 2020, https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/
- Quinn, James. “Emotet Evolves With New Wi-Fi Spreader.” Binary Defense. February 7, 2020, https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

1.18 Describe perimeter-based network security

1.18.1 Identify the types of devices used in perimeter defense

Perimeter-based network security models date to the early mainframe era (circa late 1950s), when large mainframe computers were located in physically secure “machine rooms” that could be accessed by only a relatively limited number of remote job entry (RJE) “dumb” terminals that were directly connected to the mainframe and also located in physically secure areas. Today’s data centers are the modern equivalent of machine rooms, but perimeter-based physical security Is no longer sufficient for several obvious but important reasons:

- Mainframe computers predate the internet. In fact, mainframe computers predate ARPANET, which predates the internet. Today, an attacker uses the internet to remotely gain access instead of physically breaching the data center perimeter.
- Data centers today are remotely accessed by millions of remote endpoint devices from anywhere and at any time. Unlike the RJEs of the mainframe era, modern endpoints (including mobile devices) are far more powerful than many of the early mainframe computers and are themselves targets.

The primary value of the mainframe computer was its processing power. The relatively limited data that was produced was typically stored on near-line media, such as tape. Today, data is the target. Data is stored online in data centers and in the cloud, and it is a high-value target for any attacker. The primary issue with a perimeter-based network security strategy in which countermeasures are deployed at a handful of well-defined ingress and egress points to the network is that the strategy relies on the assumption that everything on the internal network can be trusted. However, this assumption no longer is safe to make, given modern business conditions and computing environments where:

- Remote employees, mobile users, and cloud computing solutions blur the distinction between “internal” and “external.”
- Wireless technologies, the proliferation of partner connections, and the need to support guest users introduce countless additional pathways into the network branch offices that may be located in untrusted countries or regions.
- Insiders, whether intentionally malicious or just careless, may present a very real security threat.

- Perimeter-based approach strategies fail to account for:
    - The potential for sophisticated cyberthreats to penetrate perimeter defenses, in which case they would then have free passage on the internal network
    - Scenarios where malicious users can gain access to the internal network and sensitive resources by using the stolen credentials of trusted users
    - The reality that internal networks are rarely homogeneous but instead include pockets of users and resources with inherently different levels of trust or sensitivity that should ideally be separated in any event (for example, research and development and financial systems versus print or file servers)

A broken trust model is not the only issue with perimeter-centric approaches to network security. Another contributing factor is that traditional security devices and technologies (such as port based firewalls) commonly used to build network perimeters allow too much unwanted traffic through. Typical shortcomings in this regard include the inability to:

- Definitively distinguish good applications from bad ones, which leads to overly permissive access control settings
- Adequately account for encrypted application traffic
- Accurately identify and control users (regardless of where they're located or which devices they're using)
- Filter allowed traffic not only for known application-borne threats but also for unknown ones

The net result is that re-architecting defenses in a way that creates pervasive internal trust boundaries is, by itself, insufficient. You also must ensure that the devices and technologies used to implement these boundaries actually provide the visibility, control, and threat inspection capabilities needed to securely enable essential business applications while still thwarting modern malware, targeted attacks, and the unauthorized exfiltration of sensitive data.

1.19 Describe the Demilitarized Zone (DMZ)

The DMZ network is a perimeter network that protects and adds an extra layer of security to the organization's internal network from unreliable traffic. A typical DMZ is a sub-network that resides between a public network and a private network.

DMZ's ultimate goal is to allow the organization to access unreliable networks, such as the Internet, while ensuring that its private or LAN network remains secure. Organizations often store external services and resources, including Domain Name Program (DNS) servers, File Transfer Protocol (FTP), email, proxy, Voice over Internet (VoIP) Protocol, and web servers, on DMZ.

These servers and resources are segregated and are given limited access to the LAN to ensure they can be accessed over the Internet but the internal LAN cannot. As a result, the DMZ method makes it very difficult for a hacker to gain direct access to organizational data and internal servers via the Internet.

1.20 Describe the transition from a trusted network to an untrusted network

A firewall is a hardware and/or software platform that controls the flow of traffic between a trusted network (such as a corporate LAN) and an untrusted network (such as the internet).

Packet filtering firewalls

First-generation packet filtering (also known as port-based) firewalls have the following characteristics:

- They operate up to Layer 4 (Transport layer) of the OSI model and inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, ICMP), and port number.
- They match source and destination IP address, protocol, and port number information contained within each packet header to a corresponding rule on the firewall that designates whether the packet should be allowed, blocked, or dropped.
- They inspect and handle each packet individually, with no information about context or session.

Stateful packet inspection firewalls

Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics:

- They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks.
- They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules.
- After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session.
- This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren't inspected after the connection is established.

Application firewalls

Third-generation application (also known as Application layer gateways, proxy-based, and reverse-proxy) firewalls have the following characteristics:

- They operate up to Layer 7 (Application layer) of the OSI model and control access to specific applications and services on the network.
- They proxy network traffic rather than permit direct communication between hosts. Requests are sent from the originating host to a proxy server, which analyzes the contents of the data packets and, if permitted, sends a copy of the original data packets to the destination host.

They inspect Application layer traffic and thus can identify and block specified content, malware, exploits, websites, and applications or services that use hiding techniques such as encryption and non-standard ports.

Key Idea

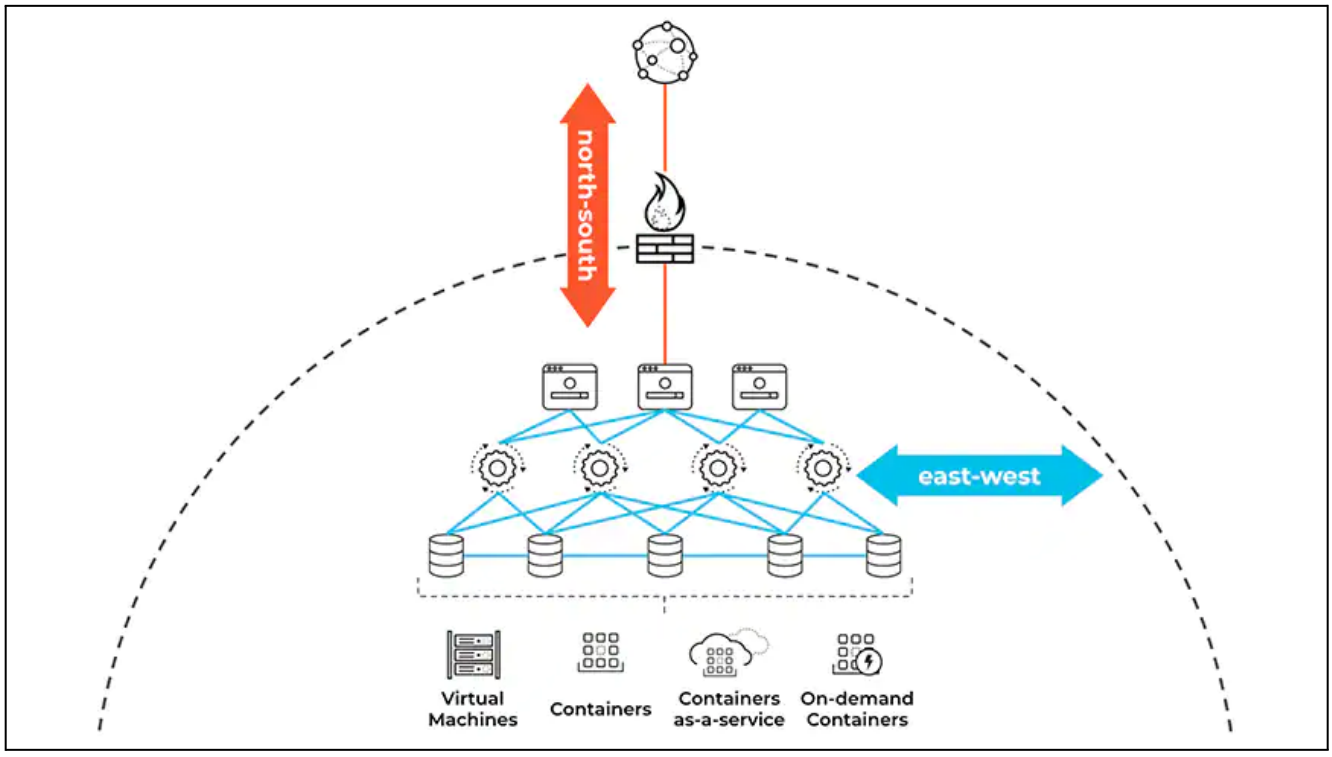
- Proxy servers also can be used to implement strong user authentication and web application filtering and to mask the internal network from untrusted networks. However, proxy servers have a significant negative impact on the overall performance of the network.

1.20.1 Differentiate between North-South and East-West zones

North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls. The edge firewall usually is a high-throughput appliance working in high availability active/passive (or active/active) mode to increase resiliency. It controls all the traffic reaching into the data center and authorizes only allowed and "clean" packets to flow into the virtualized environment.

East-west refers to data packets moving between virtual workloads entirely within the private cloud. East-west traffic is protected by a local, virtualized firewall instantiated on each hypervisor. East-west firewalls are inserted transparently into the application infrastructure and do not necessitate a redesign of the logical topology.

Perimeter security makes up a significant part of most organizations' network security controls. Network security devices such as network firewalls inspect "north-south" (client to server) traffic that crosses the security perimeter and stop bad traffic. Assets within the perimeter are implicitly trusted, thus "east-west" (workload to workload) traffic may go without inspection.



For most organizations, east-west communications make up the majority of data center and cloud traffic patterns, and perimeter-focused defenses do not have visibility into east-west traffic. Given these factors, malicious actors use this as an opportunity to move laterally across workloads.

1.20.2 References

- Firewall, https://www.paloaltonetworks.com/cyberpedia/firewall
- What is Microsegmentation? https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation

1.21 Describe Zero Trust

The Zero Trust security model was introduced by Forrester Research. It addresses some of the limitations of perimeter-based network security strategies by removing the assumption of trust. With Zero Trust, essential security capabilities are deployed in a way that provides policy enforcement and protection for all users, devices, applications, and data resources, and the communications traffic between them, regardless of location.

In particular, with Zero Trust there is no default trust for any entity – including users, devices, applications, and packets – regardless of what it is and its location on or relative to the enterprise network. Verification that authorized entities are always doing only what they're allowed to do becomes mandatory in a Zero Trust model.

These changes imply the following needs:

- The need to establish trust boundaries that effectively compartmentalize the various segments of the internal computing environment. The general idea is to move security functionality closer to the pockets of resources that require protection. In this way, security can always be enforced regardless of the point of origin of associated communications traffic.
- The need for trust boundaries to do more than just initial authorization and access control enforcement. To "always verify" also requires ongoing monitoring and inspection of associated communications traffic for subversive activities (such as threats).

1.21.1 Identify the benefits of the Zero Trust model

Benefits of implementing a Zero Trust network include:

- Clearly improved effectiveness in mitigating data loss with visibility and safe enablement of applications, and detection and prevention of cyberthreats
- Greater efficiency for achieving and maintaining compliance with security and privacy mandates, using trust boundaries to segment sensitive applications, systems, and data
- Improved ability to securely enable transformative IT initiatives, such as user mobility, bring your own device (BYOD) and bring your own access (BYOA), infrastructure virtualization, and cloud computing
- Lower total cost of ownership (TCO) with a consolidated and fully integrated product platform, rather than a disparate array of siloed, purpose-built security point products

1.21.2 Identify the design principles for Zero Trust

The core Zero Trust principles that define the operational objectives of a Zero Trust implementation include:

- **Ensure that all resources are accessed securely, regardless of location**. This principle suggests not only the need for multiple trust boundaries but also increased use of secure access for communication to or from resources, even when sessions are confined to the "internal" network. It also means ensuring that the only devices allowed access to the network have the correct status and settings, have an approved VPN client and proper passcodes, and are not running malware.
- **Adopt a least privilege strategy and strictly enforce access control**. The goal is to minimize allowed access to resources as a means to reduce the pathways available for malware and attackers to gain unauthorized access and subsequently to spread laterally and/or infiltrate sensitive data.
- **Inspect and log all traffic**. This principle reiterates the need to "always verify" while also reinforcing that adequate protection requires more than just strict enforcement of access control. Close and continuous attention also must be given to exactly what "allowed" applications are actually doing, and the only way to accomplish these goals is to inspect the content for threats.

1.21.3 Describe a microperimeter

In Zero Trust, you identify a protect surface. The protect surface is made up of the network's most critical and valuable data, assets, applications, and services (DAAS). Protect surfaces are unique to each organization. Because the protect surface contains only what's most critical to an organization's operations, it is orders of magnitude smaller than the attack surface and is always knowable. With the protect surface identified, you can identify how traffic moves across the organization in relation to it.

The only way to determine and enforce policy that ensures secure access to your data is to understand who the users are, which applications they are using, and how they are connecting. With an understanding of the interdependencies between the DAAS, infrastructure, services, and users, you should put controls in place as close to the protect surface as possible, thus creating a micro-perimeter around it. This micro-perimeter moves with the protect surface wherever it goes.

Key Terms

- The principle of **least privilege** in network security requires that only the permission or access rights necessary to perform an authorized task are granted.
- A **protect surface** consists of the most critical and valuable data, assets, applications, and services (DAAS) on a network.

1.21.4 Differentiate between Trust and Untrust zones

Forrester Research refers to a trust zone as a micro core and perimeter (MCAP). A trust zone is a distinct pocket of infrastructure where the member resources not only operate at the same trust level but also share similar functionality. Functionality such as protocols and types of transactions must be shared in order to minimize the number of allowed pathways into and out of a given zone and, in turn, minimize

the potential for malicious insiders and other types of threats to gain unauthorized access to sensitive resources. Examples of trust zones are the user (or campus) zone, a wireless zone for guest access, a cardholder data zone, database and application zones for multi tier services, and a zone for public-facing web applications.

Remember that a trust zone is not intended to be a “pocket of trust” where systems (and therefore threats) within the zone can communicate freely and directly with each other. For a full Zero Trust implementation, the network would be configured to ensure that all communications traffic, including traffic between devices in the same zone, is intermediated by the corresponding Zero Trust Segmentation Platform.

1.21.5 References

- What is a Zero Trust Architecture? https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture#:~:text=Rooted%20in%20the%20principle%20of,%2C%20and%20simplifying%20granular%2C%20%E2%80%9Cleast

1.22 Describe the integration of services for network, endpoint, and cloud

With network security, no single solution will protect against the variety of threats that organizations face. For more comprehensive protection, a combination of hardware and software provides multiple layers of security to defend the network against various threats. The time, cost and manpower required to carefully select, implement and maintain these tools is a huge investment for any organization. However, those within the network environment will not always be inside the perimeter, and the network protection capabilities will not always apply to them. If endpoints are not protected with the right security solution products, these individuals could bypass the perimeter security and introduce outside threats into the environment. The wrong endpoint security product can undo all of the work that has been done to secure the network.
Below are the five things your endpoint should do to prevent a negative impact on your network security posture:

- **Integrate threat intelligence natively**.

  According to a 2016 Ponemon study, 39 percent of respondents agree that all attacks can be blocked if the organization is engaged in the sharing of threat intelligence. Employing global threat intelligence expands protection capabilities beyond the knowledge of one solution to the shared intelligence of a global community. When other members of the community encounter new attacks, that information is shared so all members can automatically detect known threats and quickly identify unknown threats.

  Both the network and the endpoint should participate in threat intelligence sharing, continuously applying growing threat intelligence across the devices in their own environments. They should also exchange intelligence with each other so that what is identified and prevented on the endpoint can also be identified and prevented on the network.

Threat intelligence alone is not enough, however. Most organizations that subscribe to intelligence feeds are drowning in data they can't correlate or translate into actionable intelligence. Without the ability to automatically translate threat intelligence into new protections, organizations are just buying more data. The problem gets worse when there is no native integration between the components in an environment to produce and share that threat intelligence. Intelligence that is not natively integrated and cannot be automatically translated into new protections is of little use unless you throw more manpower at it. The end result would merely be a more people-intensive process of data analysis.

- **Protect against known and unknown threats.**

  Most traditional security products are designed to detect known threats before they enter an organization. In many cases, by the time an unknown threat has been detected, critical assets have already been compromised and detection is too little, too late. Additionally, while attackers often reuse existing malware and exploit techniques, they will also modify existing attacks or create entirely new ones to evade detection. This leaves a whole gamut of threats undetectable by most security products.

  Detection and remediation on the network or endpoint are invariably time-consuming, people-intensive and inefficient. This problem can be avoided if both the network and the endpoint can prevent known and unknown threats. Ideally, your endpoint security solution's prevention capabilities should not rely on signatures nor prior knowledge of an attack or vulnerability, and should incorporate various analysis and prevention methods to maximize effectiveness.

- **Be automated.**

  Attackers have automation, scalability and specialized tools at their disposal. In Ponemon's 2016 Economics of a Breach survey, 68 percent of respondents said automated hacking tools make it easier for attackers to execute successful attacks. An entire economy and marketplace exists to drive the proliferation of these tools at affordable prices.

  To defend against increasingly sophisticated attacks, organizations employ point solutions that are often complex and people-intensive, yet seemingly insufficient. To outpace attackers, an organization must make successful attacks more challenging and less profitable. Respondents in the aforementioned survey claim 60 percent of attacks can be deterred if an attack requires an additional 40 hours to conduct. The only way to achieve this in a scalable and sustainable fashion is with automated prevention.

  Detection on either the network or endpoint is not scalable if a security analyst must be dispatched to investigate alerts. Automation makes an organization a more difficult target by delaying the success of an attack and thus the payout, and causing the attacker to move on to their next potential victim.

- **Deliver persistent protection.**

  Users are increasingly becoming more mobile, connecting to internal resources from points around the globe that are outside the organizational network perimeter. There should be the same level of protection on all endpoints, regardless of their connectivity: online or offline, on- or

off-premise. Lack of persistence in these protections will lead to a compromised endpoint and, quite possibly, a compromised network, regardless of network protections already in place. Endpoint security must extend beyond the traditional network perimeter, where many cyberattacks target end users and endpoints, and where the network does not have complete visibility.

- **Provide full visibility into activity on the network, endpoint and cloud.**

  Modern attacks go through multiple steps to achieve their objectives. To successfully prevent an attack, organizations must have full visibility of all users, devices and data across their network, endpoint and the cloud. This visibility is necessary to understand the context of an attack, enforce security policy across the network and endpoint, and correlate security events to improve the organization's security posture. When natively integrated threat intelligence is combined with the automated prevention of known and unknown threats to deliver persistent protection, regardless of connectivity or location, the synergistic effect can dramatically improve an organization's security posture. This will make the organization less appealing to opportunistic attackers as well as minimize the likelihood of a successful targeted attack.

  Choosing the wrong endpoint security solution can leave your endpoints vulnerable to threats and impede, or undo, the significant work that has gone into securing the network. Your endpoint security solution should secure all endpoints continuously, as well as bring additional capabilities to other parts of the organization and bolster your overall network security posture overall.

1.22.1 References

- 5 Ways Endpoint Security and Network Security Should Work Together. https://www.paloaltonetworks.com/cyberpedia/5-ways-endpoint-security-and-network-security-should-work-together

1.23 Identify the capabilities of an effective Security Operating Platform

Cybercrime and the types of security threats continue to evolve, thus challenging organizations to stay current as network boundaries and attack surfaces expand. Security breaches and intellectual property loss can have a huge impact on organizations. Current approaches to security, which focus mainly on detection and remediation, are inadequate to sufficiently address the rise in volume and sophistication of attacks.

Cybercriminals leverage automation and big data analytics to execute massively scalable and increasingly effective attacks against their targets. Cybercriminals are not the only threat: Employees often may unknowingly violate corporate compliance and expose critical data in locations such as the public cloud.

To enable the prevention of successful cyberattacks, the security operating portfolio platform delivers four key capabilities:

- Provide full visibility: For network administrators and security practitioners to understand the full context of an attack, visibility of all users and devices is provided across the organization's network, endpoint, cloud, and SaaS applications.
- Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility.
- Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats.
- Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and delivery of near-real-time protections against new threats to the various security solutions in the organization's environments enable dynamic policy updates. These updates are designed to allow enterprises to scale defenses with technology, rather than people.

Security should not be a barrier to the adoption of new mobility, SaaS, public, or private cloud technologies that enable productivity. Organizations that have a natively integrated, prevention-first security platform in place can securely adopt innovative, productivity-enhancing applications and technologies, all while maintaining a comprehensive and consistent prevention oriented enterprise security posture.

1.23.1 Describe the components of the Security Operating Platform

Because of the rapid evolution of applications moving to the cloud, decentralization of IT infrastructure, and the increased threat landscape, organizations have lost visibility and control. Devices are proliferating and the network perimeter has all but disappeared, leaving enterprise security teams struggling to safely enable and protect their businesses, customers, and users. Because of new threats growing in number and sophistication, organizations are finding that traditional security products and approaches are less and less capable of protecting their networks against advanced cyberattacks.

Application development and IT operations teams also are accelerating the delivery of new applications to drive business growth by adopting DevOps tools and methodologies, cloud and container technologies, big data analytics, and automation and orchestration. Meanwhile, applications are increasingly accessible. The result is an incredibly complex network that introduces significant business risk. Organizations must minimize this risk without slowing down the business. A different approach to security, therefore, is needed. Defenders need to replace siloed point products with security innovations that are tightly integrated. Security requires simplicity. The Palo Alto Networks product portfolio consists of a tightly integrated system of components and services, including a partner ecosystem, that delivers consistent security across the network, endpoints, and cloud. The product portfolio is a fully integrated system that simplifies security by leveraging consolidated threat intelligence information, automation, machine learning, and data analytics.

The product portfolio is designed so that security teams can operate simply and efficiently to protect their organizations. The platform prevents successful attacks and stops attacks in progress while providing consistent protection to secure the enterprise, the cloud, and the future. The product portfolio is based on prevention and is designed and purpose-built to counter attacks before they can breach an organization's environment.

The product portfolio's prevention architecture allows organizations to reduce threat exposure by first enabling applications for all users or devices in any location and then preventing threats within application flows, associating application use to user identities across physical, cloud based, and software-as-a-service (SaaS) environments.

1.23.2 References

- SECURITY OPERATING PLATFORM. https://www.paloaltonetworks.co.uk/products/security-operating-platform

1.24 Summary of key ideas

- The use of Web 2.0 apps in the enterprise is sometimes referred to as Enterprise 2.0, although not all Web 2.0 apps are considered Enterprise 2.0 applications.
- For proof of detection in each category, MITRE requires that the proof be provided to them, but they may not include all detection details in public results, particularly when those details are sensitive.
- You can click each individual CVE to view in-depth details about it on a panel that appears on the right.
- Effective change and configuration management processes help to ensure that newly deployed applications and endpoints are properly configured (for example, disabling unneeded ports and services) and maintained.

- The first computer virus was Elk Cloner, written in 1982 by a ninth-grade high school student near Pittsburgh, Pennsylvania. Elk Cloner was a relatively benign boot sector virus that displayed a poem on the fiftieth time that an infected floppy disk was inserted into an Apple II computer.
- The first PC virus was a boot sector virus, written in 1986, called Brain. Brain also was relatively benign and displayed a message with the actual contact information for the creators of the virus. Brain was written by two Pakistani brothers who created the virus so that they could track piracy of their medical software.
- Regardless of the attack or its complexity, for the attack to be successful the attacker must execute a series of these core exploit techniques in sequence, like navigating a maze to reach its objective.
- The Rustock botnet could send up to 25,000 spam email messages per hour from an individual bot and, at its peak, sent an average of 192 spam emails per minute per bot.
- Proxy servers also can be used to implement strong user authentication and web application filtering and to mask the internal network from untrusted networks. However, proxy servers have a significant negative impact on the overall performance of the network.

Domain 2 Network Security Components

2.1 Differentiate between hubs, switches, and routers

In the 1960s, the U.S. Defense Advanced Research Project Agency (DARPA) created ARPANET, the precursor to the modern internet. ARPANET was the first packet-switched network. A packet-switched network breaks data into small blocks (packets), transmits each individual packet from node to node toward its destination, and then reassembles the individual packets in the correct order at the destination. The following are several types of equipment that move information from one location to another.

Routers are physical or virtual devices that send data packets to destination networks along a network path using logical addresses (discussed under task 2.6). Routers use various routing protocols to determine the best path to a destination, based on variables such as bandwidth, cost, delay, and distance. A wireless router combines the functionality of a router and a wireless access point (AP) to provide routing between a wired and wireless network. An AP is a network device that connects to a router or wired network and transmits a Wi-Fi signal so that wireless devices can connect to a wireless (or Wi-Fi) network. A wireless repeater rebroadcasts the wireless signal from a wireless router or AP to extend the range of a Wi-Fi network.

A hub (or concentrator) is a network device that connects multiple devices such as desktop computers, laptop docking stations, and printers on a LAN. Network traffic that is sent to a hub is broadcast out of all ports on the hub, which can create network congestion and introduces potential security risks (because broadcast data can be intercepted).

A switch is essentially an intelligent hub that uses physical addresses to forward data packets to devices on a network. Unlike a hub, a switch is designed to forward data packets only to the port that corresponds to the destination device. This transmission method (referred to as micro-segmentation) creates separate network segments and effectively increases the data transmission rates available on the individual network segments. Also, a switch can be used to implement virtual LANs (VLANs), which logically segregate a network and limit broadcast domains and collision domains.

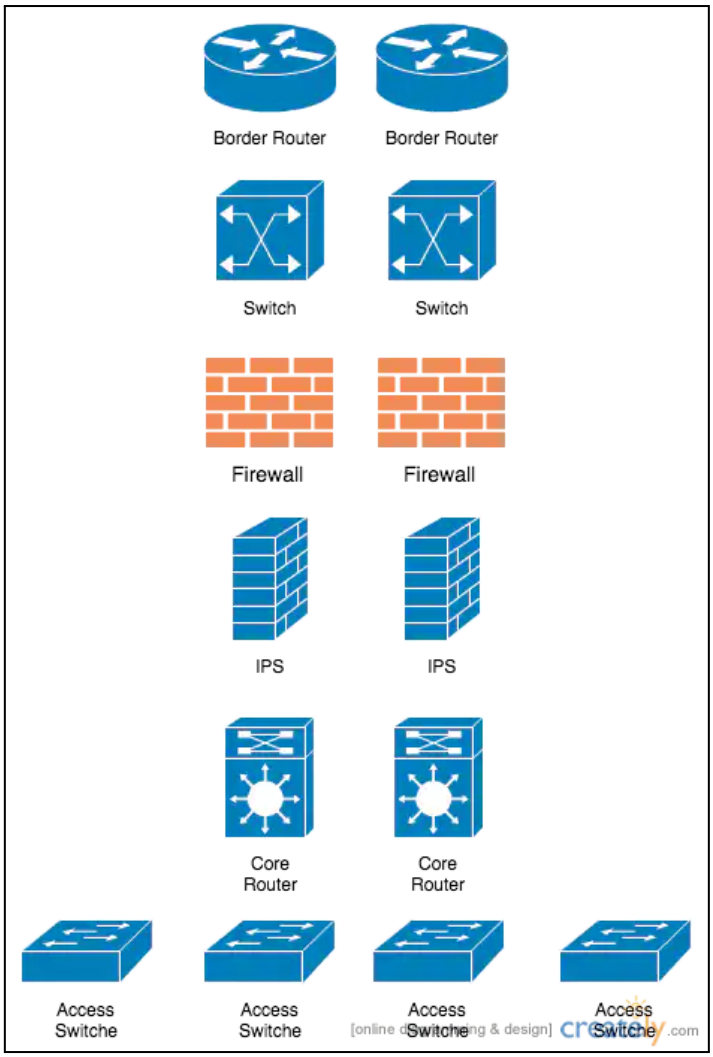
Key Idea

- ARPANET was the first packet-switched network created by the U.S. Defense Advanced Research Project Agency (DARPA).

Key Terms

- A **router** is a network device that sends data packets to a destination network along a network path.
- A **wireless repeater** rebroadcasts the wireless signal from a wireless router or AP to extend the range of a Wi-Fi network.
- A **hub** (or **concentrator**) is a device used to connect multiple networked devices on a local-area network (LAN).
- A **switch** is an intelligent hub that forwards data packets only to the port associated with the destination device on a network.
- A **virtual LAN** (VLAN) is a logical network that is created within a physical LAN.
- A **broadcast domain** is the portion of a network that receives broadcast packets sent from a node in the domain.
- A **collision** domain is a network segment on which data packets may collide with each other during transmission.

2.1.1 Given a network diagram, identify the icons for hubs, switches, and routers



The architecture above contains:

- **Border Routers** that connect to the Internet and are the first hop for the IPs provided by the ISP
- **Core Routers** or Switches that handle routing between internal networks
- **Distribution Routers or Switches** that aggregate Access Switches. They will either pass traffic between locally connected access switches or forward traffic to the core to be routed
- **Access Switches** that provide physical Ethernet connectivity for endpoints (clients and servers)
- **Security Gateways** that may include multiple layers of firewalls, Network IPS, Web Gateways, and Email Gateways

2.1.2 References

- "Ericsson Mobility Report, November 2019." Ericsson. November 2019, https://www.ericsson.com/en/mobility-report.
- Networking, https://www.paloaltonetworks.com/blog/2015/04/when-it-comes-to-networking-keep-it-simple/

2.2 Describe the use of VLANs

A VLAN is a set of devices or network nodes that communicate with each other as if they were building a single LAN, when in fact they are present in one or more LAN sections. Virtual local-area networks (VLANs) segment broadcast domains in a LAN, typically into logical groups (such as business departments). VLANs are created on network switches.

2.3 Differentiate between routed and routing protocols

Routed protocols, such as Internet Protocol (IP), address packets with routing information that enables those packets to be transported across networks using routing protocols.

Key Terms

- An **Internet Protocol (IP)** address is a 32-bit or 128-bit identifier assigned to a networked device for communications at the Network layer of the OSI model or the Internet layer of the TCP/IP model.

Routing protocols are defined at the Network layer of the OSI model and specify how routers communicate with one another on a network. Routing protocols can either be static or dynamic.

2.4 Differentiate between static and dynamic routing protocols

A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

A dynamic routing protocol can automatically learn new (or alternate) routes and determine the best route to a destination. The routing table is updated periodically with current routing information. Dynamic routing protocols are further classified as:

- **Distance-vector:** A distance-vector protocol makes routing decisions based on two factors: the distance (hop count or other metric) and vector (the egress router interface). It periodically informs its peers and/or neighbors of topology changes. Convergence is the time required for all routers in a network to update their routing tables with the most current information (such as link status changes), and it can be a significant problem for distance-vector protocols. Without convergence, some routers in a network may be unaware of topology changes, which causes the router to send traffic to an invalid destination. During convergence, routing information is exchanged between routers, and the network slows down considerably. Convergence can take several minutes in networks that use distance-vector protocols.

Routing Information Protocol (RIP) is an example of a distance-vector routing protocol that uses hop count as its routing metric. To prevent routing loops, in which packets effectively get stuck bouncing between various router nodes, RIP implements a hop limit of 15, which limits the size of networks that RIP can support. After a data packet crosses 15 router nodes (hops) between a source and a destination, the destination is considered unreachable. In addition to hop limits, RIP employs four other mechanisms to prevent routing loops:

- **Split horizon:** Prevents a router from advertising a route back out through the same interface from which the route was learned.
- **Triggered updates:** When a change is detected, the update is sent immediately instead of after the 30-second time delay normally required to send a RIP update.
- **Route poisoning:** Sets the hop count on a bad route to 16, which effectively advertises the route as unreachable.
- **Holddown timers:** Cause a router to start a timer when the router first receives information that a destination is unreachable. Subsequent updates about that destination will not be accepted until the timer expires. This timer also helps avoid problems associated with flapping. Flapping occurs when a route (or interface) repeatedly changes state (up, down, up, down) over a short period of time.

2.4.1 Differentiate between link state and distance vector

Link state: A link-state protocol requires every router to calculate and maintain a complete map, or routing table, of the entire network. Routers that use a link-state protocol periodically transmit updates that contain information about adjacent connections, or link states, to all other routers in the network. Link-state protocols are compute-intensive, but they can calculate the most efficient route to a destination. They consider numerous factors, such as link speed, delay, load, reliability, and cost (an arbitrarily assigned weight or metric). Convergence occurs very rapidly (within seconds) with link-state protocols.

Open Shortest Path First (OSPF) is an example of a link-state routing protocol that often is used in large enterprise networks. OSPF routes network traffic within a single autonomous system (AS). OSPF networks are divided into areas identified by 32-bit area identifiers. Area identifiers can (but don't need to) correspond to network IP addresses and can duplicate IP addresses without conflicts.

Path vector: A path-vector protocol is similar to a distance-vector protocol but without the scalability issues associated with limited hop counts in distance-vector protocols. Each routing table entry in a path-vector protocol contains path information that gets dynamically updated.

Border Gateway Protocol (BGP) is an example of a path-vector protocol used between separate autonomous systems. BGP is the core protocol used by internet service providers (ISPs) and network service providers (NSPs), and on very large private IP networks.

Key Idea

- Open Shortest Path First (OSPF) is an example of a link-state routing protocol that often is used in large enterprise networks.
- Border Gateway Protocol (BGP) is an example of a path-vector protocol used between separate autonomous systems.

Key Terms

- **Convergence** is the time required for all routers in a network to update their routing tables with the most current routing information about the network.
- **Hop count** generally refers to the number of router nodes that a packet must pass through to reach its destination.
- An **autonomous system (AS)** is a group of contiguous IP address ranges under the control of a single internet entity. Individual autonomous systems are assigned a 16-bit or 32-bit AS number (ASN) that uniquely identifies the network on the internet. ASNs are assigned by the Internet Assigned Numbers Authority (IANA).

2.5 Identify the borders of collision and broadcast domains

A **broadcast domain** is the portion of a network that receives broadcast packets sent from a node in the domain.

A **collision domain** is a network segment on which data packets may collide with each other during transmission.

2.6 Differentiate between different types of area networks

2.6.1 WAN

A wide-area network (WAN) is a computer network that connects multiple LANs or other WANs across a relatively large geographic area such as a small city, a region or country, or a global enterprise network.

A WAN connects networks using telecommunications circuits and technologies such as multiprotocol label switching (MPLS), broadband cable, digital subscriber line (DSL), fiber optic, optical carrier (for example, OC-3), and T-carrier (for example, T-1) at various speeds, typically ranging from 256Kbps to several hundred megabits per second. Examples of networking equipment commonly used in WANs include access servers, channel service units (CSUs) and data service units (DSUs), firewalls, modems, routers, virtual private network (VPN) gateways, and WAN switches.

2.6.2 LAN

A local-area network (LAN) is a computer network that connects end-user devices such as laptop and desktop computers, servers, printers, and other devices so that applications, databases, files, file storage, and other networked resources can be shared among authorized users on the LAN. A LAN operates across a relatively small geographic area (such as a floor, a building, or a group of buildings), typically at speeds of up to 10Mbps (Ethernet), 100Mbps (Fast Ethernet), 1,000Mbps (or 1Gbps – Gigabit Ethernet) on wired networks and 11Mbps (802.11b), 54Mbps (802.11a and g), 450Mbps (802.11n), 1.3Gbps (802.11ac), and 14Gbps (802.11ax – theoretical) on wireless networks. A LAN can be wired, wireless, or a combination of wired and wireless. Examples of networking equipment commonly used in LANs include bridges, hubs, repeaters, switches, and wireless access points (APs).

Two basic network topologies (with many variations) are commonly used in LANs:

- **Star:** Each node on the network is directly connected to a switch, hub, or concentrator, and all data communications must pass through the switch, hub, or concentrator. The switch, hub, or concentrator thus can become a performance bottleneck or single point of failure in the network. A star topology is ideal for practically any size environment and is the most commonly used basic LAN topology.
- **Mesh:** All nodes are interconnected to provide multiple paths to all other resources. A mesh topology may be used throughout the network or only for the most critical network components, such as routers, switches, and servers, to eliminate performance bottlenecks and single points of failure.

Key Idea

- Two basic network topologies which are commonly used in LANs are star and mesh.

Key Terms

- A **local-area network (LAN)** is a computer network that connects laptop and desktop computers, servers, printers, and other devices so that applications, databases, files and file storage, and other networked resources can be shared across a relatively small geographic area, such as a floor, a building, or a group of buildings.
- A **bridge** is a wired or wireless network device that extends a network or joins separate network segments.
- A **repeater** is a network device that boosts or retransmits a signal to physically extend the range of a wired or wireless network.
- In a **ring topology**, all nodes are connected in a closed loop that forms a continuous ring and all communication travels in a single direction around the ring. Ring topologies were common in token ring networks.
- In a **bus (or linear bus)** topology, all nodes are connected to a single cable (the backbone) that is terminated on both ends. In the past, bus networks were commonly used for very small networks because they were inexpensive and relatively easy to install.

Other once-popular network topologies, such as ring and bus, are rarely found in modern networks.

2.7 Describe the advantages of SD-WAN

A software-defined wide-area network (SD-WAN) separates the control and management processes from the underlying networking hardware, thus making them available as software that can be easily configured and deployed. A centralized control console means network administrators can write new rules and policies, and then configure and deploy them across an entire network at once.

SD-WAN makes management and direction of traffic across a network easier. With traditional networking approaches such as MPLS, traffic created in the branch is returned, or “backhauled,” to a centralized internet security point in a headquarters data center. Backhauling of traffic can lower application performance, which results in reduced productivity and poor user experience. Because MPLS networks are private networks built for one given organization, they are considered reliable and secure, but they are expensive. Moreover, MPLS is not designed to handle the high volumes of WAN traffic that result from software-as-a-service (SaaS) applications and cloud adoption.

Compared to traditional WANs, SD-WANs can manage multiple types of connections, including MPLS, broadband, Long-Term Evolution (LTE), and others, and support applications hosted in data centers, public and private clouds, and SaaS services. SD-WAN can route application traffic over the best path in real time. In the case of cloud, SD-WAN can forward internet-bound and cloud-bound traffic directly from the branch without backhauling.

SD-WAN offers many benefits to geographically distributed organizations, including:

- **Simplicity:** Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. Also, when SD-WAN is combined with zero-touch provisioning, a feature that helps automate the deployment and configuration processes, organizations can further reduce the complexity, resources, and operating expenses required to spin up new sites.
- **Improved performance:** By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.
- **Reduced costs:** Network administrators can supplement or substitute expensive MPLS with broadband and other connectivity options.

Key Terms

- A **software-defined wide-area network (SD-WAN)** separates the network control and management processes from the underlying hardware in a wide-area network and makes them available as software.
- **Long-Term Evolution (LTE)** is a type of 4G cellular connection that provides fast connectivity primarily for mobile internet use.

2.8 Describe the purpose of the Domain Name System (DNS)

2.8.1 Describe how DNS record types are used

The basic DNS record types are as follows:

- A **(IPv4)** or **AAAA (IPv6)** (Address): Maps a domain or subdomain to an IP address or multiple IP addresses
- **CNAME** (Canonical Name): Maps a domain or subdomain to another hostname
- **MX** (Mail Exchanger): Specifies the hostname or hostnames of email servers for a domain
- **PTR** (Pointer): Points to a CNAME; commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain
- **SOA** (Start of Authority): Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number
- **NS** (Name Server): The NS record specifies an authoritative name server for a given host.
- **TXT** (Text): Stores text-based information

Key Terms

- An **intranet** is a private network that provides information and resources such as a company directory, human resources policies and forms, department or team files, and other internal information to an organization's users. Like the internet, an intranet uses the HTTP and/or HTTPS protocols, but access to an intranet typically is restricted to an organization's internal users. Microsoft SharePoint is a popular example of intranet software.
- **Hypertext Transfer Protocol (HTTP)** is an application protocol used to transfer data between web servers and web browsers.
- **Hypertext Transfer Protocol Secure (HTTPS)** is a secure version of HTTP that uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption.
- A **recursive** DNS query is performed (if the DNS server allows recursive queries) when a DNS server is not authoritative for a destination domain. The non-authoritative DNS server obtains the IP address of the authoritative DNS server for the destination domain and sends the original DNS request to that server to be resolved.
- **DNS over HTTPS (DOH)** uses the HTTPS protocol to encrypt DNS traffic.

2.8.2 Identify a fully qualified domain name (FQDN)

The Domain Name System (DNS) is a distributed, hierarchical internet database that maps fully qualified domain names (FQDNs) for computers, services, and other resources such as a website address (also known as a uniform resource locator, or URL) to IP addresses, similar to how a contact list on a smartphone maps the names of businesses and individuals to phone numbers. If you want to create a new domain name that will be accessible via the internet, you must register your unique domain name with a domain name registrar, such as GoDaddy or Network Solutions. This registration is similar to listing a new phone number in a phone directory. DNS is critical to the operation of the internet.

Key Terms

- A **fully qualified domain name (FQDN)** is the complete domain name for a specific computer, service, or resource connected to the internet or a private network.
- A **domain name registrar** is an organization that is accredited by a top-level domain (TLD) registry to manage domain name registrations.
- A **top-level domain (TLD)** is the highest-level domain in DNS, represented by the last part of an FQDN (for example, .com and .edu). The most commonly used TLDs are generic top-level domains (gTLDs) (such as .com, edu, .net, and .org) and country-code top-level domains (ccTLDs) (such as .ca and .us).
- An **authoritative** DNS server is the system of record for a given domain.

2.8.3 Describe the DNS hierarchy

There are several components that are used to provide DNS and they have a hierarchy in terms of authority.

A root name server is the authoritative name server for a DNS root zone. Worldwide, 13 root name servers (actually, 13 networks comprising hundreds of root name servers) are configured. They are named a.root-servers.net through m.root-servers.net. DNS servers typically are configured with a root hints file that contains the names and IP addresses of the root servers.

A host (such as a web browser on a desktop computer) on a network that needs to connect to another host (such as a web server on the internet) must first translate the name of the destination host from its URL to an IP address. The connecting host (the DNS client) sends a DNS request to the IP address of the DNS server that is specified in the network configuration of the DNS client. If the DNS server is authoritative for the destination domain, the DNS server resolves the IP address of the destination host and answers the DNS request from the DNS client. Imagine, for example, you are attempting to connect to an intranet server on your internal network from the desktop computer in your office. If the DNS server address that is configured on your computer is an internal DNS server that is authoritative for your intranet domain, the DNS server resolves the IP address of the intranet server. Your computer then encapsulates the resolved destination IP address in the Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) request packets that are sent to the intranet server.

If a DNS server is not authoritative for the destination domain (for example, an internet website address), then the DNS server performs a recursive query (if it is configured to perform recursive queries) to obtain the IP address of the authoritative DNS server and then sends the original DNS request to the authoritative DNS server. This process is a top-down procedure in which the DNS server first consults its root hints file and queries a root name server to identify the authoritative DNS server for the top-level domain (TLD; for example, .com) associated with the DNS query. The DNS server then queries the TLD server to identify the authoritative server for the specific domain that is being queried (for example, paloaltonetworks.com). This process continues until the authoritative server for the FQDN is identified and queried. The recursive DNS server then answers the original DNS client's request with the DNS information from the authoritative DNS server.

DNS over HTTPS (DoH) is a more secure implementation of the DNS protocol that uses HTTPS to encrypt data between the DNS client and the DNS resolver.

2.9 Differentiate between categories of IoT devices

In 2019, there were nearly 27 billion active internet of things (IoT) devices worldwide, including machine-to-machine (M2M), wide-area IoT, short-range IoT, massive-and-critical IoT, and multi-access edge computing (MEC) devices (source: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020).

Key Terms

- **Machine-to-machine (M2M)** devices are networked devices that exchange data and can perform actions without manual human interaction.
- **Multi-access edge computing (MEC)** is defined by the European Telecommunications Standards Institute (ETSI) as an environment "characterized by ultra-low latency and high bandwidth as well as real-time access to radio network information that can be leveraged by applications."

IoT connectivity technologies are broadly categorized as follows:

- **Cellular:**
  - **2G/2.5G:** 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications.
  - **3G:** IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to achieve data transfer rates of 384Kbps to 168Mbps.
  - **4G/Long-Term Evolution (LTE):** 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.
  - **5G:** 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.
- **Satellite:**
  - **C-band:** C-band satellite operates in the 4 to 8 gigahertz (GHz) range. It is used in some Wi-Fi devices and cordless phones, and in surveillance and weather radar systems.
  - **L-band:** L-band satellite operates in the 1 to 2GHz range. It commonly is used for radar, global positioning systems (GPSs), radio, and telecommunications applications.
- **Short-range wireless:**
  - **Adaptive Network Technology + (ANT+):** ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors.
  - **Bluetooth/Bluetooth Low-Energy (BLE):** Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.

- **Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN):** 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters.
- **Wi-Fi/802.11:** The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include:
  - 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps
  - 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps
  - 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps
- **Z-Wave:** Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors.
- **Zigbee/802.14:** Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

- **Low-power WAN (LP-WAN) and other wireless WAN (WWAN):**
  - **Narrowband IoT (NB-IoT):** NB-IoT provides low cost, long battery life, and high connection density for indoor applications. It uses a subset of the LTE standard in the 200 kilohertz (kHz) range.
  - **LoRa:** The LoRa Alliance is driving the Long-Range Wide-Area Network (LoRaWAN) protocol as the open global standard for secure, carrier-grade IoT low-power wide-area (LPWA) connectivity, primarily for large-scale public networks with a single operator.
  - **Sigfox:** Sigfox provides subscription-based global cellular LPWA connectivity for IoT devices. The Sigfox network relies on Ultra Narrowband (UNB) modulation and operates in unlicensed sub-GHz frequency bands.
  - **Worldwide Interoperability for Microwave Access (WiMAX):** WiMAX is a family of wireless broadband communications standards based on the IEEE 802.16 standards. WiMAX applications include portable mobile broadband connectivity, smart grids and metering, and internet failover for business continuity.

2.9.1 Identify the known security risks and solutions associated with IoT

Identity of Things (IDoT) refers to Identity and Access Management (IAM) solutions for the IoT. These solutions must be able to manage human-to-device, device-to-device, and/or device-to-service/system IAM by:

- Establishing a naming system for IoT devices
- Determining an identity lifecycle for IoT devices, ensuring that it can be modified to meet the projected lifetime of IoT devices
- Creating a well-defined process for registering IoT devices. The type of data that the device will be transmitting and receiving should shape the registration process.
- Defining security safeguards for data streams from IoT devices
- Outlining well-defined authentication and authorization processes for admin local access to connected devices
- Creating safeguards for protecting different types of data, making sure to create privacy safeguards for personally identifiable information (PII)

Though the IoT presents innovative new approaches and services in all industries, it also presents new cybersecurity risks. According to research conducted by the Palo Alto Networks Unit 42 threat intelligence team, the general security posture of IoT devices is declining, thus leaving organizations vulnerable to new IoT-targeted malware and older attack techniques that IT teams have long forgotten. Key findings include:

- **IoT devices are unencrypted and unsecured:** Ninety-eight percent of all IoT device traffic is unencrypted, thus exposing personal and confidential data on the network. Attackers that have successfully bypassed the first line of defense (most frequently via phishing attacks) and established C2 can listen to unencrypted network traffic, collect personal or confidential information, and then exploit that data for profit on the dark web.

  Fifty-seven percent of IoT devices are vulnerable to medium-severity or high-severity attacks, thus making IoT the “low-hanging fruit” for attackers. Because of the generally low patch level of IoT assets, the most frequent attacks are exploits via long-known vulnerabilities and password attacks using default device passwords.
- **Internet of Medical Things (IoMT) devices are running outdated software:** In 2019, 83 percent of medical imaging devices run on unsupported operating systems, which is a 56 percent jump from 2018, as a result of the Windows 7 operating system reaching its end of life. This general decline in security posture presents opportunities for new attacks, such as cryptojacking (which increased from 0 percent in 2017 to 5 percent in 2019) and brings back long-forgotten attacks such as Conficker, which IT environments had previously been immune to for a long time.

  The IoMT devices with the most security issues are imaging systems, which represent a critical part of the clinical workflow. For healthcare organizations, 51 percent of threats involve imaging devices, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on these devices.
- **Healthcare organizations are displaying poor network security hygiene:** Seventy-two percent of healthcare VLANs mix IoT and IT assets, allowing malware to spread from users’ computers to vulnerable IoT devices on the same network. There is a 41 percent rate of attacks exploiting device vulnerabilities, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses. We’re seeing a shift from IoT botnets conducting denial-of-service attacks to more sophisticated attacks targeting patient identities, corporate data, and monetary profit via ransomware.

- **IoT-focused cyberattacks are targeting legacy protocols:** There is an evolution of threats targeting IoT devices using new techniques, such as peer-to-peer C2 communications and wormlike features for self-propagation. Attackers recognize the vulnerability of decades-old legacy operational technology (OT) protocols, such as Digital Imaging and Communications in Medicine (DICOM), and can disrupt critical business functions in the organization.

Zingbox IoT Guardian is a Palo Alto Networks IoT security offering that automates the orchestration of the IoT lifecycle to provide security, management, and optimization of all assets. Zingbox IoT Guardian uses a unique, IoT personality-based approach to secure and manage IoT devices with integrated IoT security based on machine learning throughout their entire lifecycles, from discovery through retirement. It allows customers to automate threat detection and response for their IT and IoT infrastructures from a single system.

2.9.1 References

- Mayan, Gilad David. "The IoT Rundown for 2020: Stats, Risks, and Solutions." Security Today. January 13, 2020, https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.

2.10 Identify IoT connectivity technologies

Cellular:

- **2G/2.5G:** 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications.
- **3G:** IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to achieve data transfer rates of 384Kbps to 168Mbps.
- **4G/Long-Term Evolution (LTE):** 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.
- **5G:** 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

Satellite:

- **C-band:** C-band satellite operates in the 4 to 8 gigahertz (GHz) range. It is used in some Wi-Fi devices and cordless phones, and in surveillance and weather radar systems.
- **L-band:** L-band satellite operates in the 1 to 2GHz range. It commonly is used for radar, global positioning systems (GPSs), radio, and telecommunications applications.

Short-range wireless:

- **Adaptive Network Technology+ (ANT+):** ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors.
- **Bluetooth/Bluetooth Low-Energy (BLE):** Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.
- **Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN):** 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters.
- **Wi-Fi/802.11:** The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include:
  – 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps
  – 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps
  – 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps
- **Z-Wave:** Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors.
- **Zigbee/802.14:** Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

Low-power WAN (LP-WAN) and other wireless WAN (WWAN):

- **Narrowband IoT (NB-IoT):** NB-IoT provides low cost, long battery life, and high connection density for indoor applications. It uses a subset of the LTE standard in the 200 kilohertz (kHz) range.
- **LoRa:** The LoRa Alliance is driving the Long-Range Wide-Area Network (LoRaWAN) protocol as the open global standard for secure, carrier-grade IoT low-power wide-area (LPWA) connectivity, primarily for large-scale public networks with a single operator.
- **Sigfox:** Sigfox provides subscription-based global cellular LPWA connectivity for IoT devices. The Sigfox network relies on Ultra Narrowband (UNB) modulation and operates in unlicensed sub-GHz frequency bands.
- **Worldwide Interoperability for Microwave Access (WiMAX):** WiMAX is a family of wireless broadband communications standards based on the IEEE 802.16 standards. WiMAX applications include portable mobile broadband connectivity, smart grids and metering, and internet failover for business continuity.

2.11 Differentiate between IPv4 and IPv6 addresses

2.11.1 Describe binary-to-decimal conversion

A binary (base2) numbering system comprises only two digits: 1 (“on”) and 0 (“off”). Binary numbering is used in computers and networking because they use electrical transistors (rather than fingers) to count. The basic function of a transistor is a gate: When electrical current is present, the gate is closed (“1” or “on”). When no electrical current is present, the gate is open (“0” or “off”). With only two digits, a binary numbering system increments to the next position more frequently than a decimal numbering system. For example, the decimal number one is represented in binary as “1,” number two is represented as “10,” number three is represented as “11,” and number four is represented as “100.”

2.11.2 Describe IPv4 CIDR notation

Unlike subnetting, which divides an IPv4 address along an arbitrary (default) classful 8-bit boundary (8 bits for a Class A network, 16 bits for a Class B network, 24 bits for a Class C network), classless inter-domain routing (CIDR) allocates address space on any address bit boundary (known as variable-length subnet masking, or VLSM). For example, using CIDR, a Class A network could be assigned a 24-bit mask (255.255.255.0, instead of the default 8-bit 255.0.0.0 mask) to limit the subnet to only 254 addresses, or a 23-bit mask (255.255.254.0) to limit the subnet to 512 addresses.

CIDR is used to reduce the size of routing tables on internet routers by aggregating multiple contiguous network prefixes (known as supernetting).

Key Idea

- An IP address can be represented with its subnet mask value, using “netbit” or CIDR notation.

Key Terms

- **Classless inter-domain routing (CIDR)** is a method for allocating IP addresses and IP routing that replaces classful IP addressing (for example, Class A, B, and C networks) with classless IP addressing.
- **Variable-length subnet masking (VLSM)** is a technique that enables IP address spaces to be divided into different sizes.
- **Supernetting** aggregates multiple contiguous smaller networks into a larger network to enable more efficient internet routing.

2.11.3 Describe IPv4 classful subnetting

For a Class C IPv4 address, there are 254 possible node (or host) addresses. This includes 28 or 256 potential addresses, but you lose two addresses for each network: one for the base network address and the other for the broadcast address. A typical Class C network uses a default 24-bit subnet mask (255.255.255.0). This subnet mask value identifies the network portion of an IPv4 address, with the first three octets being all ones (11111111 in binary notation, 255 in decimal notation). The mask displays

the last octet as zero (00000000 in binary notation). For a Class C IPv4 address with the default subnet mask, the last octet is where the node-specific values of the IPv4 address are assigned.

For example, in a network with an IPv4 address of 192.168.1.0 and a mask value of 255.255.255.0, the network portion of the address is 192.168.1, and 254 node addresses (192.168.1.1 through 192.168.1.254) are available. Remember, the first address (192.168.1.0) is the base network, and the last address (192.168.1.255) is the broadcast address.

Class A and Class B IPv4 addresses use smaller mask values and support larger numbers of nodes than Class C IPv4 addresses for their default address assignments. Class A networks use a default 8-bit (255.0.0.0) subnet mask, which provides a total of more than 16 million (256 x 256 x 256) available IPv4 node addresses. Class B networks use a default 16-bit (255.255.0.0) subnet mask, which provides a total of 65,534 (256 x 256, minus the network address and the broadcast address) available IPv4 node addresses.

2.11.4 Given a scenario, identify the proper subnet mask

An IP address can be represented with its subnet mask value, using “netbit” or CIDR notation. A netbit value represents the number of ones in the subnet mask and is displayed after an IP address, separated by a forward slash.

For example, 192.168.1.0/24 represents a subnet mask consisting of 24 ones:

- 11111111.11111111.11111111.00000000 (in binary notation)
  or
- 255.255.255.0 (in decimal notation)

2.11.5 Describe the purpose of subnetting

Subnetting is a technique used to divide a large network into smaller, multiple subnetworks by segmenting an IP address into two parts: the network and the host. Subnetting can be used to limit network traffic or limit the number of devices that are visible to, or can connect to, each other. Routers examine IP addresses and subnet values (called masks) and determine whether to forward packets between networks. With IP addressing, the subnet mask is a required element.

Key Terms

- **Subnetting** is a technique used to divide a large network into smaller subnetworks.

2.11.6 Describe the structure of IPv4 and IPv6

Physical, logical, and virtual addressing in computer networks requires a basic understanding of decimal (base10), binary (base2), and hexadecimal (base16) numbering (see Table).

The decimal (base10) numbering system comprises the numerals 0 through 9. Humans use the decimal numbering system because we have ten fingers, so a base10 numbering system is easiest for humans to understand.

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Table: Decimal, hexadecimal, and binary notation

A hexadecimal (base16) numbering system comprises 16 digits (0 through 9, and A through F). Hexadecimal numbering is used because it is more convenient to represent a byte (which consists of 8 bits) of data as two digits in hexadecimal, rather than eight digits in binary. The decimal numbers 0 through 9 are represented as in hexadecimal “0” through “9,” respectively. However, the decimal number 10 is represented in hexadecimal as “A,” the number 11 is represented as “B,” the number 12 is represented as “C,” the number 13 is represented as “D,” the number 14 is represented as “E,” and

the number 15 is represented as “F.” The number 16 then increments to the next numeric position, represented as “10.”

The physical address of a network device, known as a media access control (MAC) address (also referred to as a burned-in address [BIA] or hardware address), is used to forward traffic on a local network segment. The MAC address is a unique 48-bit identifier assigned to the network adapter of a device. If a device has multiple NICs, each NIC must have a unique MAC address. The MAC address is usually assigned by the device manufacturer and is stored in the device read-only memory (ROM) or firmware. MAC addresses typically are expressed in hexadecimal format with a colon or hyphen separating each 8-bit section.

An example of a 48-bit MAC address is:

- 00:40:96:9d:68:16

The logical address of a network device, such as an IP address, is used to route traffic from one network to another. An IP address is a unique 32-bit or 128-bit (IPv4 and IPv6, respectively) address assigned to the NIC of a device. If a device has multiple NICs, each NIC may be assigned a unique IP address, or multiple NICs may be assigned a virtual IP address to enable bandwidth aggregation or failover capabilities. IP addresses are assigned statically or dynamically (most commonly using Dynamic Host Configuration Protocol, or DHCP), typically by a network administrator or network service provider (NSP). IPv4 addresses usually are expressed in dotted decimal notation with a dot separating each decimal section (known as an octet).

An example of an IPv4 address is:

- 192.168.0.1

IPv6 addresses typically are expressed in hexadecimal format (32 hexadecimal numbers grouped into eight blocks) with a colon separating each block of four hexadecimal digits (known as a hextet).

An example of an IPv6 address is:

- 2001:0db8:0000:0000:0008:0800:200c:417a

2.11.7 Describe the purpose of IPv4 and IPv6 addressing

IPv4 and IPv6 addressing is explained further below.

Address Resolution Protocol (ARP) translates a logical address, such as an IP address, to a physical MAC address. Reverse Address Resolution Protocol (RARP) translates a physical MAC address to a logical address.

Key Terms

- A **media access control (MAC)** address is a unique 48-bit or 64-bit identifier assigned to a network interface card (NIC) for communications at the Data Link layer of the OSI model.
- **Dynamic Host Configuration Protocol (DHCP)** is a network management protocol that dynamically assigns (leases) IP addresses and other network configuration parameters (such as default gateway and DNS information) to devices on a network.
- A **default gateway** is a network device, such as a router or switch, to which an endpoint sends network traffic when a specific destination IP address is not specified by an application or service, or when the endpoint does not know how to reach a specified destination.
- An **octet** is a group of 8 bits in a 32-bit IPv4 address.
- A **hextet** is a group of four 4-bit hexadecimal digits in a 128-bit IPv6 address.
- **Address Resolution Protocol (ARP)** translates a logical address, such as an IP address, to a physical MAC address. Reverse Address Resolution Protocol (RARP) translates a physical MAC address to a logical address.

DHCP is a network management protocol used to dynamically assign IP addresses to devices that do not have a statically assigned (manually configured) IP address on a TCP/IP network. Bootstrap Protocol (BOOTP) is a similar network management protocol that is commonly used on Unix and Linux TCP/IP networks. When a network-connected device that does not have a statically assigned IP address is powered on, the DHCP client software on the device broadcasts a DHCPDISCOVER message on UDP port 67. When a DHCP server on the same subnet (or a different subnet if a DHCP Helper or DHCP Relay Agent is configured) as the client receives the DHCPDISCOVER message, it reserves an IP address for the client and sends a DHCPOFFER message to the client on UDP port 68. The DHCPOFFER message contains the MAC address of the client, the IP address that is being offered, the subnet mask, the lease duration, and the IP address of the DHCP server that made the offer. When the client receives the DHCPOFFER, it broadcasts a DHCPREQUEST message on UDP port 67, requesting the IP address that was offered. A client may receive DHCPOFFER messages from multiple DHCP servers on a subnet but can accept only one offer. When the DHCPREQUEST message is broadcast, the other DHCP servers that sent an offer that was not requested (in effect, accepted) in the DHCPREQUEST message will withdraw their offers. Finally, when the correct DHCP server receives the DHCPREQUEST message, it sends a DHCPACK (acknowledgment) message on UDP port 68, and the IP configuration process is completed.

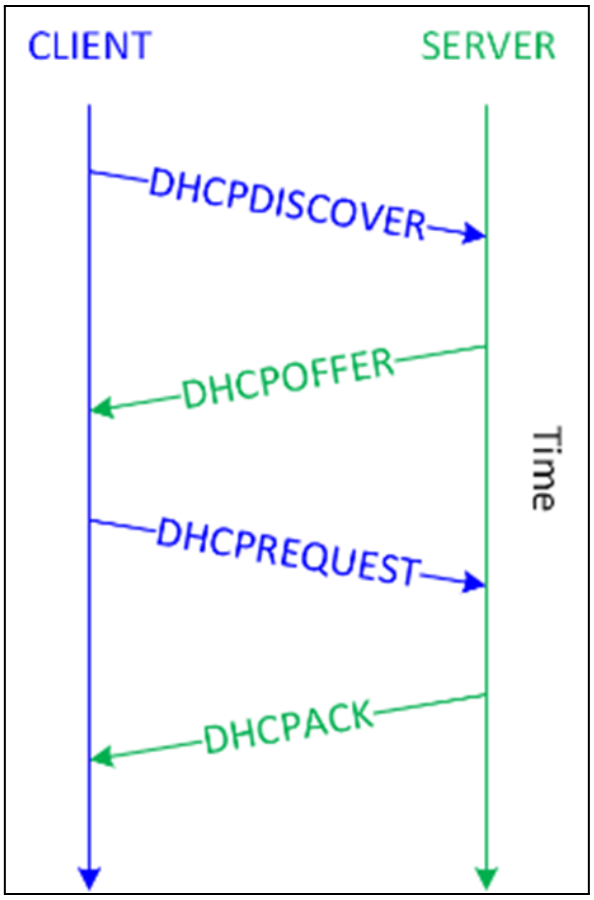


Figure: DHCP operation

Network address translation (NAT) virtualizes IP addresses by mapping private, non-routable IP addresses that are assigned to internal network devices to public IP addresses when communication across the internet is required. NAT commonly is implemented on firewalls and routers to conserve public IP addresses.

Data packets are routed over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using IP addressing information. IPv4, which is the most widely deployed version of IP, consists of a 32-bit logical IP address. The first four bits in an octet are known as the high-order bits; the first bit in the octet is referred to as the most significant bit. The last four bits in an octet are known as the low-order bits; the last bit in the octet is referred to as the least significant bit.

Key Idea

- IPv4 is the most widely deployed version of IP consisting of a 32-bit logical IP address.

Key Terms

- **Network address translation (NAT)** virtualizes IP addresses by mapping private, non-routable IP addresses assigned to internal network devices to public IP addresses.
- The first four bits in a 32-bit IPv4 address octet are referred to as the **high-order** bits.
- The last four bits in a 32-bit IPv4 address octet are referred to as the **low-order** bits.
- The first bit in a 32-bit IPv4 address octet is referred to as the **most significant** bit.
- The last bit in a 32-bit IPv4 address octet is referred to as the **least significant** bit.

As shown in the following table, each bit position represents its value if the bit is "on" (1); otherwise, the bit's value is zero ("off" or 0).

High-order bits					Low-order bits			
128	64	32	16		8	4	2	1

Table: Bit position values in an IPv4 address

Decimal	Binary		Decimal	Binary		Decimal	Binary
225	1111 1111		172	1010 1100		64	0100 0000
254	1111 1110		170	1010 1010		32	0010 0000
253	1111 1101		160	1010 0000		16	0001 0000
252	1111 1100		150	1001 0110		8	0000 1000
251	1111 1011		140	1000 1100		7	0000 0111
250	1111 1010		130	1000 0010		6	0000 0110
249	1111 1001		128	1000 0000		5	0000 0101
248	1111 1000		120	0111 1000		4	0000 0100
224	1110 0000		110	0110 1110		3	0000 0011
200	1100 1000		100	0110 0100		2	0000 0010
192	1100 0000		96	0110 0000		1	0000 0001
180	1011 0100		90	0101 1010		0	0000 0000

Table: Binary notation of octet values

The five IPv4 address classes (indicated by the high-order bits) are shown in Table.

Class	Purpose	High-Order Bits	Address Range	Max. # of Hosts
A	Large networks	0	1 to 126	16,777,214
B	Medium-size networks	10	128 to 191	65,534
C	Small networks	110	192 to 223	254
D	Multicast	1110	224 to 239	—
E	Experimental	1111	240 to 254	—

Table: IP address classes

The address range 127.0.0.1 to 127.255.255.255 is a loopback network used for testing and troubleshooting. Packets sent to a loopback (or localhost) address such as 127.0.0.1 are immediately routed back to the source device.

A subnet mask is a number that hides the network portion of an IPv4 address, leaving only the host portion of the IP address. The network portion of a subnet mask is represented by contiguous "on" (1) bits beginning with the most significant bit. For example, in the subnet mask 255.255.255.0, the first three octets represent the network portion and the last octet represents the host portion of an IP address. Recall that the decimal number 255 is represented in binary notation as 1111 1111.

Key Terms

- A **subnet mask** is a number that hides the network portion of an IPv4 address, leaving only the host portion of the IP address.

The default (or standard) subnet masks for Class A, B, and C networks are:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Several IPv4 address ranges are reserved for use in private networks and are not routable on the internet, including:

- 10.0.0.0–10.255.255.255 (Class A)
- 172.16.0.0–172.31.255.255 (Class B)
- 192.168.0.0–192.168.255.255 (Class C)

The 32-bit address space of an IPv4 address limits the total number of unique public IP addresses to about 4.3 billion. The widespread use of NAT delayed the inevitable depletion of IPv4 addresses, but, as of 2018, the pool of available IPv4 addresses that can be assigned to organizations is officially depleted. (A small pool of IPv4 addresses has been reserved by each regional internet registry to facilitate the transition to IPv6.) IPv6 addresses, which use a 128-bit hexadecimal address space providing about 3.4 x 1038 (340 hundred undecillion) unique IP addresses, were created to replace IPv4 when the IPv4 address space was exhausted.

IPv6 addresses consist of 32 hexadecimal numbers grouped into eight hextets of four hexadecimal digits, separated by a colon. A hexadecimal digit is represented by 4 bits (see Table 2-1), so each hextet is 16 bits (four 4-bit hexadecimal digits), and eight 16-bit hextets equals 128 bits.

An IPv6 address is further divided into two 64-bit segments: The first (also referred to as the “top” or “upper”) 64 bits represent the network part of the address, and the last (also referred to as the “bottom” or “lower”) 64 bits represent the node or interface part of the address. The network part is further subdivided into a 48-bit global network address and a 16-bit subnet. The node or interface part of the address is based on the MAC address of the node or interface.

The basic format for an IPv6 address is:

- xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
  Where x represents a hexadecimal digit (0–f).

This is an example of an IPv6 address:

- 2001:0db8:0000:0000:0008:0800:200c:417a

The Internet Engineering Task Force (IETF) has defined several rules to simplify an IPv6 address:

- Leading zeros in an individual hextet can be omitted, but each hextet must have at least one hexadecimal digit, except as noted in the next rule. Application of this rule to the previous example yields this result: 2001:db8:0:0:8:800:200c:417a.
- Two colons (::) can be used to represent one or more groups of 16 bits of zeros, and leading or trailing zeroes in an address; the two colons (::) can appear only once in an IPv6 address. Application of this rule to the previous example yields this result: 2001:db8::8:800:200c:417a.
- In mixed IPv4 and IPv6 environments, the form x:x:x:x:x;x:d.d.d.d can be used, in which x represents the six high-order 16-bit hextets of the address and d represents the four low-order 8-bit octets (in standard IPv4 notation) of the address. For example, 0db8:0:0:0:0:FFFF:129.144.52.38 is a valid IPv6 address. Application of the previous two rules to this example yields this result: db8::ffff:129.144.52.38.

IPv6 security features are specified in Request for Comments (RFC) 7112 and include techniques to prevent fragmentation exploits in IPv6 headers and implementation of Internet Protocol Security (IPsec) at the Network layer of the OSI model.

2.12 Describe the purpose of a default gateway

A default gateway is a network device, such as a router or switch, to which an endpoint sends network traffic when a specific destination IP address is not specified by an application or service, or when the endpoint does not know how to reach a specified destination.

2.13 Describe the role of NAT

Network address translation (NAT) virtualizes IP addresses by mapping private, non-routable IP addresses that are assigned to internal network devices to public IP addresses when communication across the internet is required. NAT commonly is implemented on firewalls and routers to conserve public IP addresses. It is also used as a method of obfuscating a host's "true" IP.

2.14 Describe OSI and TCP/IP models

2.14.1 Identify the order of the layers of both OSI and TCP/IP models

The OSI model is defined by the International Organization for Standardization (ISO, not an acronym but the adopted organizational name from the Greek isos, meaning “equal”) and consists of seven layers:

- **Application (Layer 7 or L7):** This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication.
- **Presentation (Layer 6 or L6):** This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system.
- **Session (Layer 5 or L5):** This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release.
- **Transport (Layer 4 or L4):** This layer provides transparent, reliable data transport and end-to-end transmission control.
- **Network (Layer 3 or L3):** This layer provides routing and related functions that enable data to be transported between systems on the same network or on interconnected networks. Routing protocols are defined at this layer. Logical addressing of devices on the network is accomplished at this layer using routed protocols such as Internet Protocol (IP). Routers operate at the Network layer of the OSI model.
- **Data Link (Layer 2):** This layer ensures that messages are delivered to the proper device across a physical network link.
- **Physical (Layer 1 or L1):** This layer sends and receives bits across the network medium (cabling or wireless links) from one device to another. It specifies the electrical, mechanical, and functional requirements of the network, including network topology, cabling and connectors, and interface types, and the process for converting bits to electrical (or light) signals that can be transmitted across the physical medium.

The TCP/IP model was developed by the U.S. Department of Defense (DoD) and actually preceded the OSI model. Whereas the OSI model is a theoretical model used to logically describe networking processes, the TCP/IP model defines actual networking requirements, including, for example, for frame construction. The TCP/IP model consists of four layers:

- **Application (Layer 4 or L4):** This layer consists of network applications and processes.
- **Transport (Layer 3 or L3):** This layer provides end-to-end delivery.
- **Internet (Layer 2 or L2):** This layer defines the IP datagram and routing.
- **Network Access (Layer 1 or L1):** Also referred to as the Link layer, this layer contains routines for accessing physical networks.

2.14.2 Compare the similarities of some OSI and TCP/IP layers

Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model.

Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.

Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.

Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model.

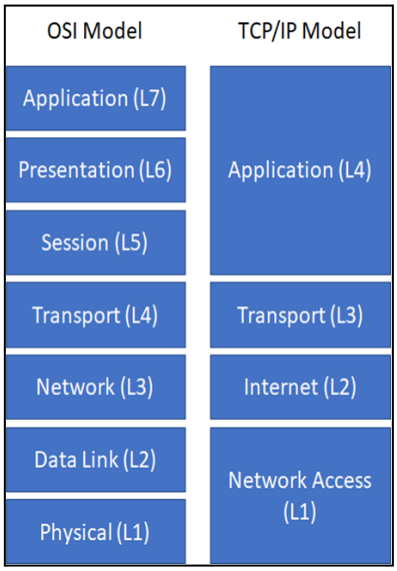


Figure: The OSI model and the TCP/IP model

2.14.3 Identify the protocols and functions of each OSI layer

- **Application (Layer 7 or L7):** This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication. Protocols that function at the Application layer include:
  - **File Transfer Protocol (FTP):** Used to copy files from one system to another on TCP ports 20 (the data port) and 21 (the control port)
  - **Hypertext Transfer Protocol (HTTP):** Used for communication between web servers and web browsers on TCP port 80
  - **Hypertext Transfer Protocol Secure (HTTPS):** Used for SSL/TLS encrypted communications between web servers and web browsers on TCP port 443 (and other ports, such as 8443)
  - **Internet Message Access Protocol (IMAP):** A store-and-forward electronic mail protocol that allows an email client to access, manage, and synchronize email on a remote mail server on TCP and UDP port 143
  - **Post Office Protocol Version 3 (POP3):** An email retrieval protocol that allows an email client to access email on a remote mail server on TCP port 110
  - **Simple Mail Transfer Protocol (SMTP):** Used to send and receive email across the internet on TCP/UDP port 25

    - **Simple Network Management Protocol (SNMP):** Used to collect network information by polling stations and sending traps (or alerts) to a management station on TCP/UDP ports 161 (agent) and 162 (manager)
    - **Telnet:** Provides terminal emulation for remote access to system resources on TCP/UDP port 23
- **Presentation (Layer 6 or L6):** This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system. Protocols that function at the Presentation layer include:
    - **American Standard Code for Information Interchange (ASCII):** A character-encoding scheme based on the English alphabet, consisting of 128 characters
    - **Extended Binary-Coded Decimal Interchange Code (EBCDIC):** An 8-bit character-encoding scheme mainly used on mainframe and midrange computers.
    - **Graphics Interchange Format (GIF):** A bitmap image format that allows up to 256 colors and is suitable for images or logos (but not photographs)
    - **Joint Photographic Experts Group (JPEG):** A photographic compression method used to store and transmit photographs.
    - **Motion Picture Experts Group (MPEG):** An audio and video compression method used to store and transmit audio and video files.
- **Session (Layer 5 or L5):** This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release. Protocols that function at the Session layer include:
    - **Network File System (NFS):** Facilitates transparent user access to remote resources on a Unix-based TCP/IP network
    - **Remote Procedure Call (RPC):** A client-server network redirection protocol
    - **Secure Shell (SSH):** Establishes an encrypted tunnel between a client and a server
    - **Session Initiation Protocol (SIP):** An open signaling protocol standard for establishing, managing, and terminating real-time communications (such as voice, video, and text) over large IP-based networks
- **Transport (Layer 4 or L4):** This layer provides transparent, reliable data transport and end-to-end transmission control. Specific Transport layer functions include:
    - **Flow control:** Manages data transmission between devices by ensuring that the transmitting device doesn't send more data than the receiving device can process
    - **Multiplexing:** Enables data from multiple applications to be simultaneously transmitted over a single physical link
    - **Virtual circuit management:** Establishes, maintains, and terminates virtual circuits
    - **Error checking and recovery:** Detects transmission errors and resolves any errors that occur, such as requesting that data be retransmitted.
    - TCP and UDP port numbers assigned to applications and services are defined at the Transport layer. Protocols that function at the Transport layer include:
    - **Transmission Control Protocol (TCP):** A connection-oriented (a direct connection between network devices is established before data segments are transferred) protocol that provides reliable delivery (received segments are acknowledged, and retransmission of missing or corrupted segments is requested) of data. TCP connections are established via a three-way handshake. The additional overhead associated with connection establishment, acknowledgment, and error correction means that TCP generally is slower than connectionless protocols such as User Datagram Protocol (UDP).

- **User Datagram Protocol (UDP):** A connectionless (a direct connection between network devices is not established before datagrams are transferred) protocol that provides best-effort delivery (received datagrams are not acknowledged and missing or corrupted datagrams are not requested) of data. UDP has no overhead associated with connection establishment, acknowledgment, sequencing, or error-checking and recovery. UDP is ideal for data that requires fast delivery, if that data isn't sensitive to packet loss and doesn't need to be fragmented. Applications that use UDP include Domain Name System (DNS), Simple Network Management Protocol (SNMP), and streaming audio or video.
- **Stream Control Transmission Protocol (SCTP):** A message-oriented protocol (similar to UDP) that ensures reliable, in-sequence transport with congestion control (similar to TCP).

- **Network (Layer 3 or L3):** This layer provides routing and related functions that enable data transportation between systems on the same network or on interconnected networks. Routing protocols are defined at this layer. Logical addressing of devices on the network is accomplished at this layer using routed protocols such as Internet Protocol (IP). Routers operate at the Network layer of the OSI model.
- **Data Link (Layer 2):** This layer ensures that messages are delivered to the proper device across a physical network link. This layer also defines the networking protocol (for example, Ethernet) used to send and receive data between individual devices and formats messages from the layers into frames for transmission, handles point-to-point synchronization and error control, and can perform link encryption. Switches typically operate at Layer 2 of the OSI model (although multilayer switches that operate at different layers also exist). The Data Link layer is further divided into two sublayers:
  - **Logical Link Control (LLC):** The LLC sublayer provides an interface for the MAC sublayer; manages the control, sequencing, and acknowledgment of frames being passed up to the Network layer or down to the Physical layer; and manages timing and flow control.
  - **Media access control (MAC):** The MAC sublayer is responsible for framing and performs error control using a cyclic redundancy check (CRC), identifies MAC addresses, and controls media access.
- **Physical (Layer 1 or L1):** This layer sends and receives bits across the network medium (cabling or wireless links) from one device to another. It specifies the electrical, mechanical, and functional requirements of the network, including network topology, cabling and connectors, and interface types, and the process for converting bits to electrical (or light) signals that can be transmitted across the physical medium.

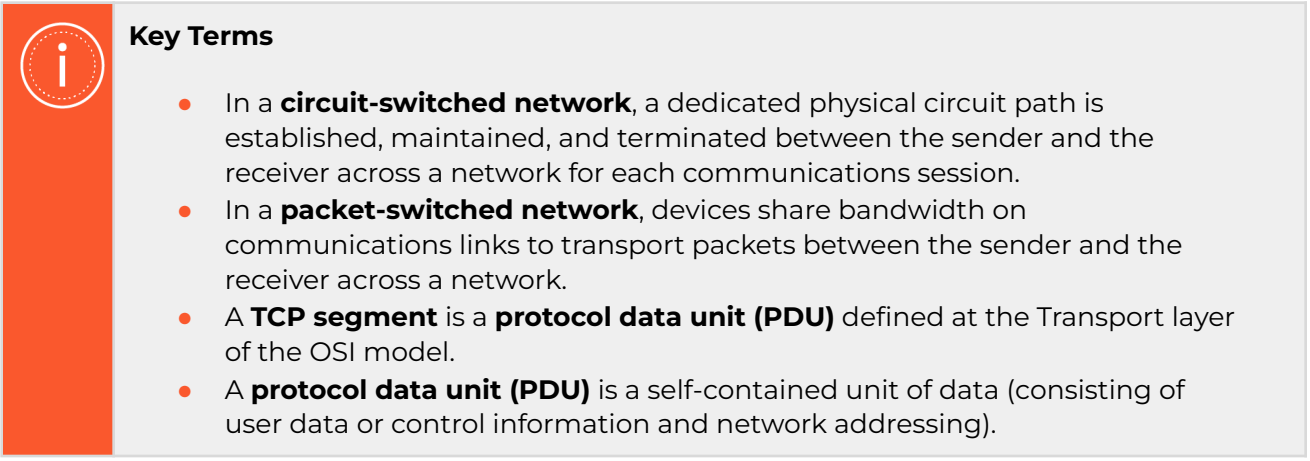
2.15 Describe the data-encapsulation process

2.15.1 Describe the PDU format used at different layers

In a circuit-switched network, a dedicated physical circuit path is established, maintained, and terminated between the sender and receiver across a network for each communications session. Before the development of the internet, most communications networks, such as telephone company networks, were circuit-switched. The internet is a packet-switched network comprising hundreds of millions of routers and billions of servers and user endpoints. In a packet-switched network, devices share bandwidth on communications links to transport packets between a sender and a receiver across a network. This type of network is more resilient to error and congestion than circuit-switched networks.

An application that needs to send data across the network (for example, from a server to a client computer) first creates a block of data and sends it to the TCP stack on the server. The TCP stack places the block of data into an output buffer on the server and determines the maximum segment size (MSS) of individual TCP blocks (segments) permitted by the server operating system. The TCP stack then divides the data blocks into appropriately sized segments (for example, 1,460 bytes), adds a TCP header, and sends the segment to the IP stack on the server. The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network. When the server operating system is ready, the IP packet is sent to the network adapter, which then converts the IP packet to bits and sends the message across the network.

Packets on their way to the destination computer typically traverse several network and security devices (such as switches, routers, and firewalls) before reaching the destination computer, where the encapsulation process described is reversed.



Key Terms

- In a **circuit-switched network**, a dedicated physical circuit path is established, maintained, and terminated between the sender and the receiver across a network for each communications session.
- In a **packet-switched network**, devices share bandwidth on communications links to transport packets between the sender and the receiver across a network.
- A **TCP segment** is a **protocol data unit (PDU)** defined at the Transport layer of the OSI model.
- A **protocol data unit (PDU)** is a self-contained unit of data (consisting of user data or control information and network addressing).

2.16 Identify the characteristics of various types of network firewalls

2.16.1 Traditional firewalls

A traditional firewall is a network security device that typically offers stateful inspection of network traffic at network entry and exit points based on state, port, and protocol. Therefore, the major function of a classical firewall is to control flow. It is capable of using a virtual private network (VPN).

2.16.2 Next-generation firewalls

A next-generation firewall inspects all traffic, including applications, threats, and content, and associates it with the user, regardless of location or device type. The application, content, and user become integral components of the enterprise security policy.

Palo Alto Networks Next-Generation Firewalls are built on a single-pass architecture, which is a unique integration of software and hardware that simplifies management, streamlines processing, and maximizes performance. The single-pass architecture integrates multiple threat prevention disciplines (IPS, anti-malware, URL filtering, etc.) into a single stream-based engine with a uniform signature format. This architecture allows traffic to be fully analyzed in a single pass without the performance degradation seen in multifunction gateways. The software is associated directly to a parallel processing hardware platform that uses function-specific processors for threat prevention, to maximize throughput and minimize latency.

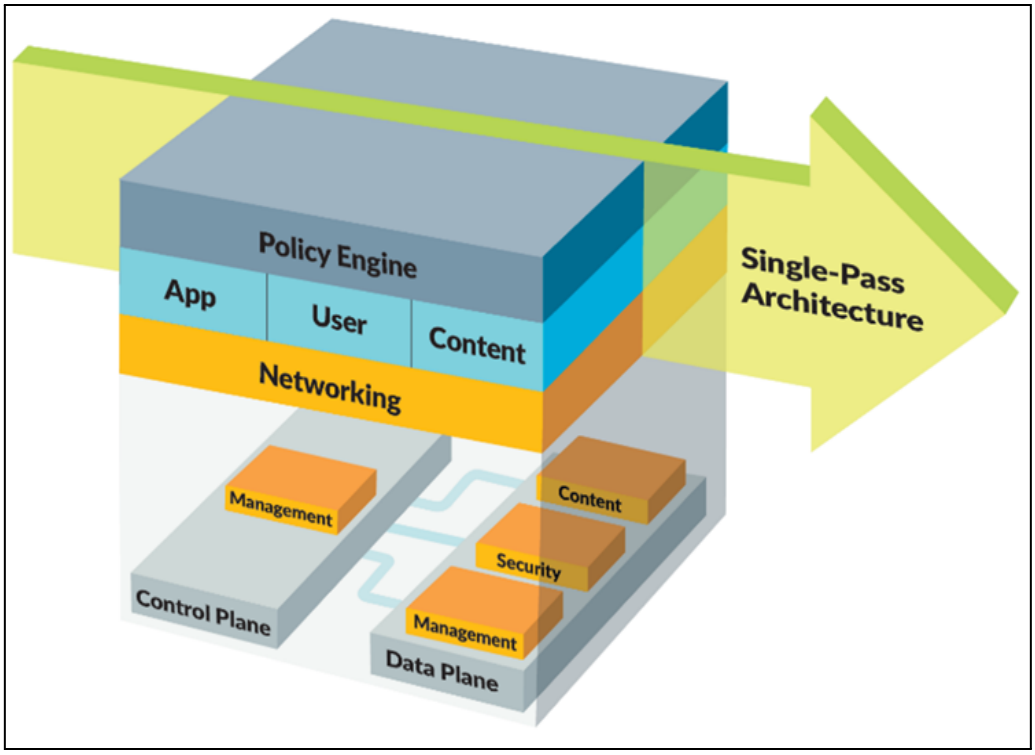


Figure: Palo Alto Networks Next-Generation Firewalls use a single-pass architecture.

The use of one common engine means that two key benefits are realized. First, unlike file proxies that need to download the entire file before they can scan the traffic, a stream-based engine scans traffic in real time, reassembling packets only as needed and only in very small amounts. Second, unlike with traditional approaches, all traffic can be scanned with a single engine, instead of multiple scanning engines.

Organizations deploy next-generation firewalls at the network perimeter and inside the network at logical trust boundaries. All traffic crossing the next-generation firewall undergoes a full-stack, single-pass inspection, providing the complete context of the application, associated content, and user identity. With this level of context, you can align security with your key business initiatives.

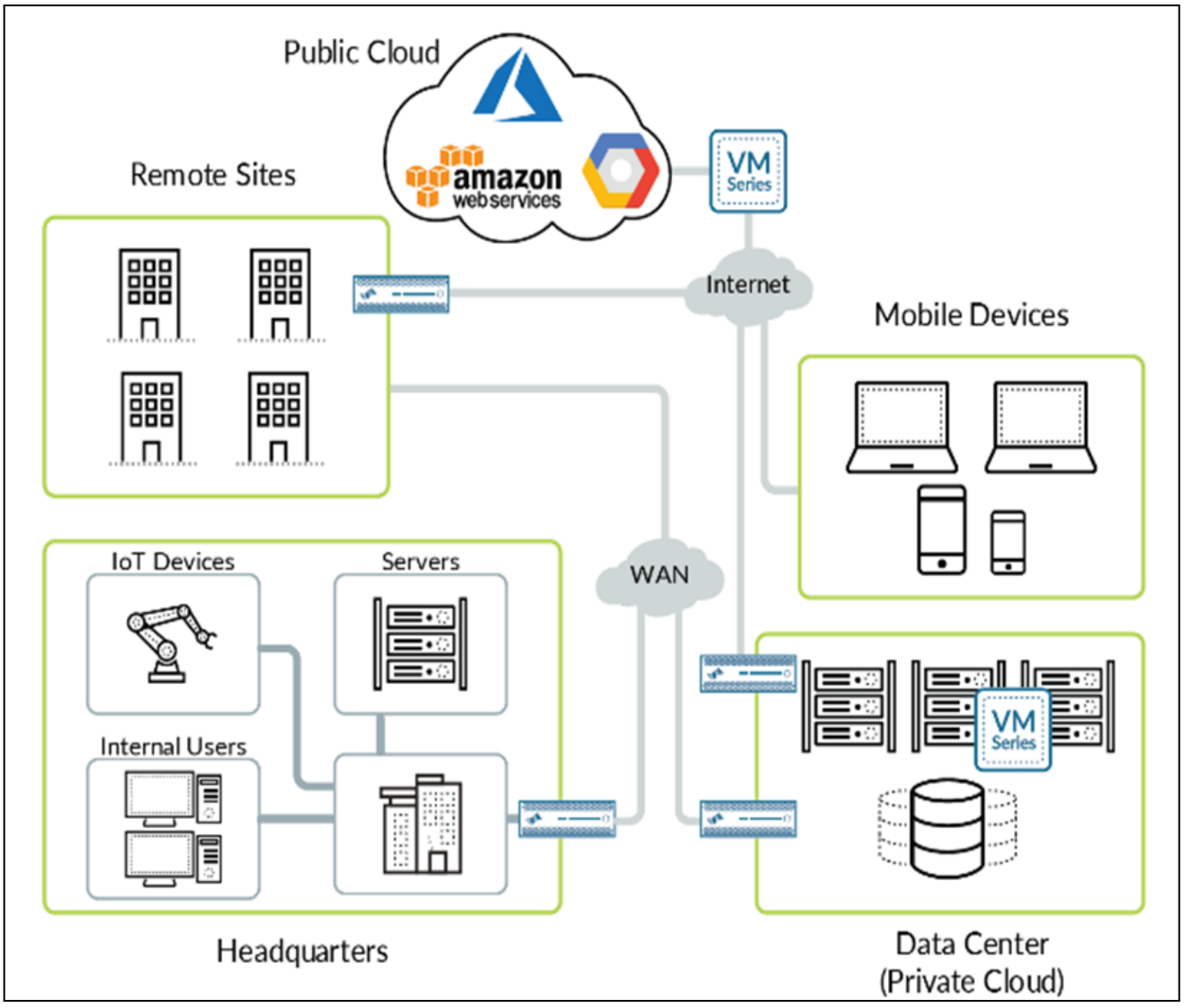


Figure: Next-generation firewall locations in the enterprise network

The next-generation firewall functions as a segmentation gateway in a Zero Trust architecture. By creating a micro-perimeter, the next-generation firewall ensures that only known, allowed traffic or legitimate applications have access to the protect surface.

2.16.3 Differentiate between NGFWs and traditional firewalls

Next-generation firewalls include several key capabilities that enable complete visibility of the application traffic flows, associated content, and user identity and protect them from known, unknown, and advanced persistent threats. The essential functional capabilities in an effective next-generation firewall include:

- Application identification: Accurately identify applications regardless of port, protocol, evasive techniques, or encryption. Provide visibility of applications and granular policy-based control over applications, including individual application functions.
- User identification: Accurately identify users and subsequently use identity information as an attribute for policy control.

- Content identification: Content identification controls traffic based on complete analysis of all allowed traffic, using multiple threat prevention and data loss prevention techniques in a single-pass architecture that fully integrates all security functions.

2.17 Describe the application of NGFW deployment options (i.e., PA-,VM- and CN-Series)

Next-generation firewall deployment options

The Palo Alto Networks family of next-generation firewalls includes physical appliances, virtualized firewalls, and 5G-ready firewalls.

Physical appliances (PA-Series)

The full range of Palo Alto Networks physical next-generation firewalls is easy to deploy into your organization's network. They are purposefully designed for simplicity, automation, and integration. PA-Series firewalls support a variety of data center and remote branch deployment use cases. Available PA Series firewalls include the following:

- **PA-7000 Series**: The PA-7000 Series next-generation firewalls enable enterprise-scale organizations and service providers to deploy security in high-performance environments, such as large data centers and high-bandwidth network perimeters. These systems are designed to handle growing throughput needs for application-, user-, and device-generated data, and they offer performance, prevention capabilities to stop the most advanced cyberattacks, and high-throughput decryption to stop threats hiding under the veil of encryption. The PA-7000 Series is built to maximize security-processing resource use and automatically scale as new computing power becomes available, and it offers simplicity defined by a single-system approach to management and licensing.
- **PA-5200 Series**: The PA-5200 Series next-generation firewalls comprising the PA-5280, PA-5260, PA-5250, and PA-5220 firewalls are ideal for high-speed data center, internet gateway, and service provider deployments. The PA-5200 Series delivers up to 64 Gbps of throughput, using dedicated processing and memory, for the key functional areas of networking, security, threat prevention, and management.
- **PA-3200 Series**: The PA-3200 Series next-generation firewalls comprising the PA-3260, PA-3250, and PA-3220 are targeted at high-speed internet gateway deployments. PA-3200 Series appliances secure all traffic (including encrypted traffic) using dedicated processing and memory for networking, security, threat prevention, and management.
- **PA-800 Series**: The PA-800 Series next-generation firewalls comprising the PA-850 and PA-820 firewalls are designed to provide secure connectivity for organizations' branch offices and for midsize businesses.
- **PA-220**: The PA-220 firewall brings next-generation firewall capabilities to distributed enterprise branch offices, retail locations, and midsize businesses in a small form factor.
- **PA-220R**: The PA-220R firewall is a ruggedized next-generation firewall that secures industrial and defense networks in a range of harsh environments, such as utility substations, power plants, manufacturing plants, oil and gas facilities, building management systems, and healthcare networks.

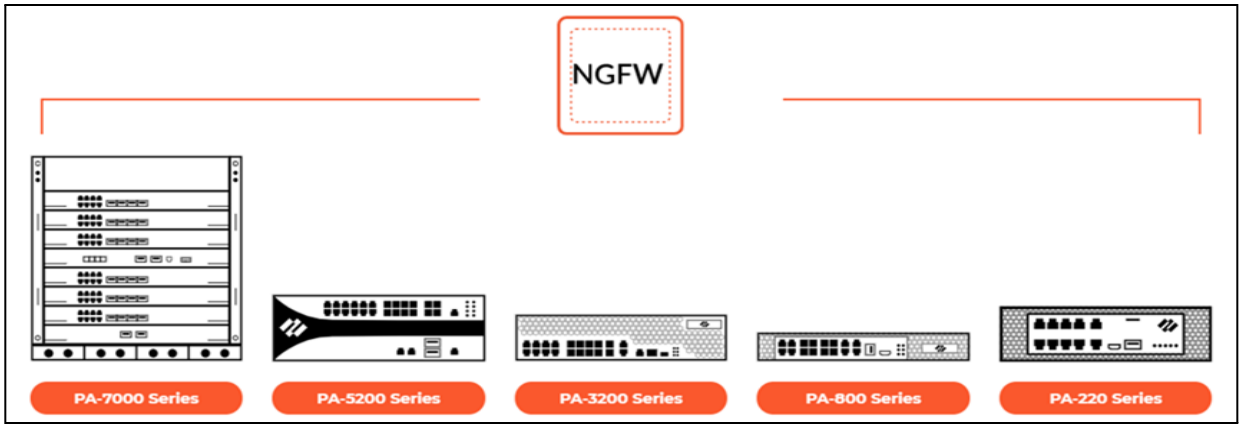


Figure: Strata next-generation firewalls

Virtualized firewalls (VM-Series)

VM-Series virtual firewalls provide all the capabilities of Palo Alto Networks next-generation physical hardware firewalls (PA-Series) in a virtual machine form factor. VM-Series form factors support a variety of deployment use cases, including:

- Micro-segmentation: VM-Series virtual firewalls reduce your environment's attack surface by enabling granular segmentation and micro-segmentation. Threat prevention capabilities ensure that threats that enter the environment are quickly identified and stopped before they can exfiltrate data, deliver malware or ransomware payloads, or cause other damage.
- Multicloud and hybrid cloud: VM-Series virtual firewalls eliminate the need for multiple security tool sets by providing comprehensive visibility and control across multicloud and hybrid cloud environments – including Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and Oracle Cloud – and just as effortlessly in software-defined networks and virtualized environments, all managed from a single console.
- DevOps and CI/CD pipelines: VM-Series virtual firewalls provide on-demand, elastic scalability to ensure security when and where it is needed most. With automated network security, security provisioning can be integrated directly into DevOps workflows and CI/CD pipelines without slowing the pace of business.

CN-Series

CN-Series is the container native version of the ML-powered Next-Generation Firewall (NGFW) that is designed specifically for Kubernetes environments. CN-Series container firewalls help network security teams safeguard developers with deep security integration into Kubernetes orchestration. Deploy the CN-Series to secure traffic between pods in different trust zones and namespaces, for protection against known and zero-day malware, and to block data exfiltration from your containerized environments.

2.18 Differentiate between intrusion detection systems and intrusion prevention systems

An **intrusion prevention system (IPS)** – sometimes referred to as an intrusion detection prevention system (IDPS) – is a network security technology and key part of any enterprise security system that continuously monitors network traffic for suspicious activity and takes steps to prevent it. Largely automated, IPS solutions help filter out this malicious activity before it reaches other security devices or controls, effectively reducing the manual effort of security teams and allowing other security products to perform more efficiently.

IPS solutions are also very effective at detecting and preventing vulnerability exploits. When a vulnerability is discovered, there is typically a window of opportunity for threat actors to exploit it before a security patch can be applied. An intrusion prevention system is used here to quickly block these types of attacks.

An **Intrusion Detection System (IDS)** is a network security technology originally built for detecting vulnerability exploits against a target application or computer. Intrusion Prevention Systems (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. Rather, IDS solutions will often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance).

2.18.1 Differentiate between knowledge-based and behavior-based systems

IDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems:

- A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.
- A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

2.18.2 References

- Intrusion Prevention System, https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
- Intrusion Detection System, https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids

2.19 Describe virtual private networks

A virtual private network (VPN) allows you to safely connect to another network over the internet by encrypting the connection from your device. A VPN makes your internet connection more secure and offers both privacy and anonymity online. Organizations, governments and businesses of all sizes use VPNs to secure remote connections to the internet for protection against malicious actors, malware and other cyberthreats. Personal VPNs have also become widely popular as they keep users' locations private, safely encrypt data and allow users to browse the web anonymously.

How Does VPN Work?

A VPN creates a private connection, known as a "tunnel," to the internet. All information traveling from a device connected to a VPN will get encrypted and go through this tunnel. When connected to a VPN, a device will behave as if it's on the same local network as the VPN. The VPN will forward device traffic to and from the intended website or network through its secure connection. This allows remote users and offices to connect securely to a corporate network or website. It also shields device IP addresses from hackers and prying eyes.

Different Types

There are two types of VPN:

- Site-to-site VPN is used to connect branch offices to a central office over the internet when distance prevents direct network connections.
- Remote access VPN allows individual users to remotely connect to a central network. In this case, the devices are referred to as endpoints.

2.19.1 Describe when to use VPNs

VPN client software typically is installed on mobile endpoints, such as laptop computers and smartphones, to extend a network beyond the physical boundaries of the organization. The VPN client connects to a VPN server, such as a firewall, router, or VPN appliance (or concentrator). After a VPN tunnel is established, a remote user can access network resources such as file servers, printers, and Voice over IP (VoIP) phones in the same way as if they were physically located in the office.

2.20 Differentiate between the different tunneling protocols

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is a basic VPN protocol that uses Transmission Control Protocol (TCP) port 1723 to establish communication with the VPN peer and then creates a Generic Routing Encapsulation (GRE) tunnel that transports encapsulated Point-to-Point Protocol (PPP) packets between the VPN peers. Although PPTP is easy to set up and is considered very fast, it is perhaps the least secure of the various VPN protocols. It commonly is used alongside either the Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Microsoft Challenge-Handshake Authentication Protocol versions 1 and 2 (MS-CHAP v1/v2), all of which have well-known security vulnerabilities, to authenticate tunneled PPP traffic. The Extensible Authentication Protocol Transport Layer Security (EAP-TLS) provides a more secure authentication protocol for PPTP but requires a public key infrastructure (PKI) and is therefore more difficult to set up.

Key Terms

- **Generic Routing Encapsulation (GRE)** is a tunneling protocol developed by Cisco Systems that can encapsulate various Network layer protocols inside virtual point-to-point links.
- **Point-to-Point Protocol (PPP)** is a Layer 2 (Data Link) protocol used to establish a direct connection between two nodes.
- **Password Authentication Protocol (PAP)** is an authentication protocol used by PPP to validate users with an unencrypted password.
- **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)** is used to authenticate Microsoft Windows-based workstations, using a challenge-response mechanism to authenticate PPTP connections without sending passwords.
- **Extensible Authentication Protocol Transport Layer Security (EAP-TLS)** is an Internet Engineering Task Force (IETF) open standard that uses the Transport Layer Security (TLS) protocol in Wi-Fi networks and PPP connections.
- **Public key infrastructure (PKI)** is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is supported by most operating systems (including mobile devices). Although it provides no encryption by itself, it is considered secure when used together with IPsec.

Secure Socket Tunneling Protocol

Secure Socket Tunneling Protocol (SSTP) is a VPN tunnel created by Microsoft to transport PPP or L2TP traffic through an SSL 3.0 channel. SSTP primarily is used for secure remote client VPN access, rather than for site-to-site VPN tunnels.

Microsoft Point-to-Point Encryption

Microsoft Point-to-Point Encryption (MPPE) encrypts data in PPP-based dial-up connections or PPTP VPN connections. MPPE uses the RSA RC4 encryption algorithm to provide data confidentiality and supports 40-bit and 128-bit session keys.

OpenVPN

OpenVPN is a highly secure, open-source VPN implementation that uses SSL/TLS encryption for key exchange. OpenVPN uses up to 256-bit encryption and can run over TCP or UDP. Although it is not natively supported by most major operating systems, it has been ported to most major operating systems, including mobile device operating systems.

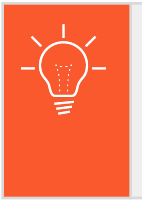
Internet Protocol Security

IPsec is a secure communications protocol that authenticates and encrypts IP packets in a communication session. An IPsec VPN requires compatible VPN client software to be installed on the endpoint device. A group password or key is required for configuration. Client-server IPsec VPNs typically require user action to initiate the connection, such as launching the client software and logging in with a username and password.

A security association (SA) in IPsec defines how two or more entities will securely communicate over the network using IPsec. A single Internet Key Exchange (IKE) SA is established between communicating entities to initiate the IPsec VPN tunnel. Separate IPsec SAs are then established for each communication direction in a VPN session.

An IPsec VPN can be configured to force all of the user's internet traffic back through an organization's firewall, thus providing optimal protection with enterprise-grade security but with some performance loss. Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation.

If split tunneling is used, a personal firewall should be configured and active on the organization's endpoints because a split tunneling configuration can create a "side door" into the organization's network. Attackers essentially can bridge themselves over the internet, through the client endpoint, and into the network over the IPsec tunnel.



Key Idea

- A single Internet Key Exchange (IKE) security association is established between communicating entities to initiate the IPsec VPN tunnel.

Secure Sockets Layer

Secure Sockets Layer (SSL) is an asymmetric encryption protocol used to secure communication sessions. SSL has been superseded by Transport Layer Security (TLS), although SSL still is the more commonly used terminology.

An SSL VPN can be deployed as an agent-based or agentless browser-based connection. An agentless SSL VPN requires users only to launch a web browser, open a VPN portal or webpage using the HTTPS protocol, and log in to the network with their user credentials. An agent-based SSL client is used within the browser session, which persists only while the connection is active and removes itself when the connection is closed. This type of VPN can be particularly useful for remote users that are connecting from an endpoint device they do not own or control, such as a hotel kiosk, where full client VPN software cannot be installed.

SSL VPN technology has become the de facto standard and preferred method of connecting remote endpoint devices back to the enterprise network, and IPsec is most commonly used in site-to-site or device-to-device VPN connections, such as connecting a branch office network to a headquarters location network or data center.

Key Terms

- **Secure Sockets Layer (SSL)** is a cryptographic protocol for managing authentication and encrypted communication between a client and a server to protect the confidentiality and integrity of data exchanged in the session.
- **Transport Layer Security (TLS)** is the successor to SSL (although it still is commonly referred to as SSL).

2.21 Describe the purpose of data loss prevention

Data loss prevention (DLP) is a security strategy that ensures sensitive or confidential information doesn't leak outside of the corporate network in a way that is unsafe or non-compliant.

Today, most enterprises face challenges in implementing effective data security because of:

- A lack of granular visibility into what, how, and where their employees access and use their data, or transfer and share it with others.
- Limited control over data stored in the cloud, which creates security gaps
- Inconsistent data security due to the varying security capabilities of public and private cloud providers, network security, and SaaS.
- The growing number of data breaches and insider threats caused by well-meaning employees, malicious insiders, and cyber criminals.

To successfully overcome these challenges, it's crucial for companies to put a solid DLP strategy in place. An effective data security strategy requires discovering and securing data while it's at rest, in use, and in motion. Monitoring the transmission of data both inside and outside of the organization and proactively detecting and stopping data leakage is another important requirement.

To successfully meet these requirements, companies must:

- Protect their company and data consistently across their in-house network, cloud, and mobile users.
- Centralize their data loss prevention and security management efforts.
- Discover, classify, monitor, and protect their data, as well as authenticate users and control who has access to specific applications and data at any given time.
- Clearly define and enforce role-based data access and usage policies.
- Better oversee and manage third-party vendor security and compliance.
- Ensure their data is being stored, accessed, and used in a way that complies with data protection regulations and data privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the European Union General Data Protection Regulation (GDPR), and others. This is especially important because any violations can result in a hefty fine and/or significant damage to a company's reputation, or even criminal or civil penalties.

This is where an innovative enterprise DLP security solution comes in to fill in the gaps.

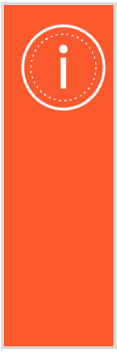
2.21.1 Classify different types of data (e.g., sensitive, inappropriate)

Network data loss prevention (DLP) solutions inspect data that is leaving, or egressing, a network (for example, via email, file transfer, or internet uploads, or by copying to a USB thumb drive) and prevent certain sensitive data as based on defined policies from leaving the network. Sensitive data may include:

- Personally identifiable information (PII) such as names, addresses, birthdates, Social Security numbers, health records (including electronic medical records, or EMRs, and electronic health records, or EHRs), and financial data (such as bank account numbers and credit card numbers)
- Classified materials (such as military or national security information)
- Intellectual property, trade secrets, and other confidential or proprietary company information

A DLP security solution prevents sensitive data from being transmitted outside the network by a user, either inadvertently or maliciously. A robust DLP solution can detect the presence of certain data patterns even if the data is encrypted.

However, these solutions introduce a potential new vulnerability in the network because they have visibility into, and the ability to decrypt, all data on the network. Other methods rely on decryption happening elsewhere, such as on a web security appliance or other man-in-the-middle decryption engine.



Key Terms

- As defined by HealthIT.gov, an **electronic medical record (EMR)** "contains the standard medical and clinical data gathered in one provider's office."
- As defined by HealthIT.gov, an **electronic health record (EHR)** "go[es] beyond the data collected in the provider's office and include[s] a more comprehensive patient history. EHR data can be created, managed, and consulted by authorized providers and staff from across more than one healthcare organization."

2.21.2 References

- Data Loss Prevention – Protecting Your Sensitive Enterprise Data, https://www.paloaltonetworks.com/cyberpedia/data-loss-prevention-protecting-your-sensitive-enterprise-data#:~:text=Data%20loss%20prevention%20(DLP)%20is,is%20unsafe%20or%20non%2Dcompliant.

2.22 Differentiate the various types of security functions from those integrated into UTM devices

Unified threat management (UTM) devices combine numerous security functions into a single appliance, including:

- Anti-malware
- Anti-spam
- Content filtering
- DLP
- Firewall (stateful inspection)
- IDS/IPS
- VPN

UTM devices don't necessarily perform any of these security functions better than their standalone counterparts, but they nonetheless serve a purpose in small to medium-size enterprise networks as a convenient and inexpensive solution that gives an organization an all-in-one security device. Typical disadvantages of UTM include:

- They sometimes have reduced feature sets to make them more affordable.
- All security functions use the same processor and memory resources. Enablement of all the functions of a UTM can result in up to a 97 percent drop in throughput and performance, as compared to top-end throughput without security features enabled.

Despite numerous security functions running on the same platform, the individual engines operate in silos with little or no integration or cooperation between them.

2.23 Describe endpoint security standards

Traditional endpoint security encompasses numerous security tools, such as anti-malware software, anti-spyware software, personal firewalls, host-based intrusion prevention systems (HIPSs), and mobile device management (MDM) software. Endpoint security also requires implementation of effective endpoint security best practices, including patch management and configuration management.

Most organizations deploy several security products to protect their endpoints, including personal firewalls, HIPSs, MDM, mobile application management (MAM), DLP, and antivirus software. Nevertheless, cyber breaches continue to increase in frequency, variety, and sophistication. The numbers and types of endpoints, including mobile and IoT devices, also has grown exponentially and increased the attack surface. New variants of the Gafgyt, Mirai, and Muhstik botnets, among others, specifically target IoT devices, and new search engines such as Shodan (Shodan.io) can automate the search for vulnerable internet-connected endpoints. Traditional endpoint security solutions and antivirus no longer can prevent security breaches on the endpoint in the rapidly changing threat landscape.

2.23.1 Describe the advantages of endpoint security

Endpoint security is an essential element of cybersecurity because the network firewall cannot completely protect hosts from zero-day exploits. Zero-day exploits target unknown vulnerabilities in operating systems and application software on host machines. Network firewalls may not be able to block an attacker's delivery of a zero-day exploit until a new signature identifying the zero-day attack has been developed and delivered to the firewall.

Network firewalls also may be restricted from decrypting all traffic because of regulations and laws. This restriction provides a window of opportunity for attackers to bypass a firewall's protection and exploit a host machine, thus necessitating endpoint security protection. Endpoint security protection is provided by an application that runs on the host machine. Effective endpoint security must be able to stop malware, exploits, and ransomware before they can compromise the host, provide protection while endpoints are online and offline, and detect threats and automate containment to minimize impact.

2.23.2 Describe host-based intrusion detection/prevention systems

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) provide real-time monitoring of network traffic and perform deep-packet inspection and analysis of network activity and data. Unlike traditional packet filtering and stateful packet inspection firewalls that examine only packet header information, an IDS/IPS examines both the packet header and the payload of network traffic. The IDS/IPS attempts to match known-bad, or malicious, patterns (or signatures) found within inspected packets. An IDS/IPS typically is deployed to detect and block exploits of software vulnerabilities on target networks.

The primary difference between an IDS and an IPS is that an IDS is considered to be a passive system, whereas an IPS is an active system. An IDS monitors and analyzes network activity and provides alerts to potential attacks and vulnerabilities on the network, but it doesn't perform any preventive action to stop an attack. An IPS, however, performs all of the same functions as an IDS but also automatically blocks or drops suspicious, pattern-matching activity on the network in real time. However, an IPS has some disadvantages, including:

- It must be placed inline along a network boundary and thus is directly susceptible to attack itself.
- False alarms must be properly identified and filtered to avoid inadvertently blocking authorized users and applications. A false positive occurs when legitimate traffic is improperly identified as malicious traffic. A false negative occurs when malicious traffic is improperly identified as legitimate traffic.
- It may be used to deploy a denial-of-service (DoS) attack by flooding the IPS, thus causing it to block connections until no connection or bandwidth is available.

2.23.3 Differentiate between signature-based and behavioral-based malware protection

Malware protection (more specifically, antivirus software) has been one of the first and most basic tenets of information security since the early 1980s. Unfortunately, all of this hard-earned experience doesn't necessarily mean that malware protection mechanisms are guaranteed to detect all attacks instantly. For example, Trustwave's 2019 Global Security Report found that infection to detection of malware "in the wild" takes an average of 55 days. Interestingly, web-based zero-day attacks, on average, remain "in the wild" up to four times longer than email-based threats because of factors that include user awareness of email-borne threats, availability and use of email security solutions (such as anti-spam and antivirus), and preferred use of the web as a threat vector by malware developers.

This poor "catch rate" is due to several factors. Some malware can mutate or can be updated to avoid detection by traditional anti-malware signatures. Also, advanced malware is increasingly specialized to the point where an attacker can develop customized malware that is targeted against a specific individual or organization.

Traditional anti-malware software uses various approaches to detect and respond to malware threats, including signature-based, container-based, application allow lists , and anomaly-based techniques.

Note: With the proliferation of advanced malware such as remote access trojans (RATs), anti-AV, and root kits/boot kits, security vendors have largely rebranded their antivirus solutions as "anti-malware" and expanded their malware protections to encompass the broader malware classifications.

Signature-based anti-malware software

Signature-based antivirus (or anti-malware) software is the oldest and most commonly used approach for detecting and identifying malware on endpoints. This approach requires security vendors to continuously collect malware samples, create matching signature files for those samples, and distribute those signature files as updates for their endpoint security products to all of their customers.

Deployment of signature-based antivirus software requires installation of an engine that typically has kernel-level access to an endpoint's system resources. Signature-based antivirus software scans an endpoint's hard drive and memory, based on a predefined schedule and in real time when a file is accessed. If a known malware signature is detected, the software performs a predefined action, such as:

- Quarantine: Isolates the infected file so that it cannot infect the endpoint or other files
- Delete: Removes the infected file
- Alert: Notifies the user (and/or system administrator) that malware has been detected

Updated signatures must be regularly and frequently downloaded from the security vendor and installed on the organization's endpoints. Download and processing of signature files in this manner can cause noticeable performance degradations on the networks and endpoints on which they are running.

Although the signature-based approach is very popular, its effectiveness is limited. By design, it is a reactive countermeasure because a signature file for new malware can't be created and delivered until the malware is already "in the wild," during which time networks and endpoints are blind to the threat: the notorious zero-day threat (or attack). The "zero-day" label is misleading, however, because the number of days from release to detection averages 5 to 20 days.

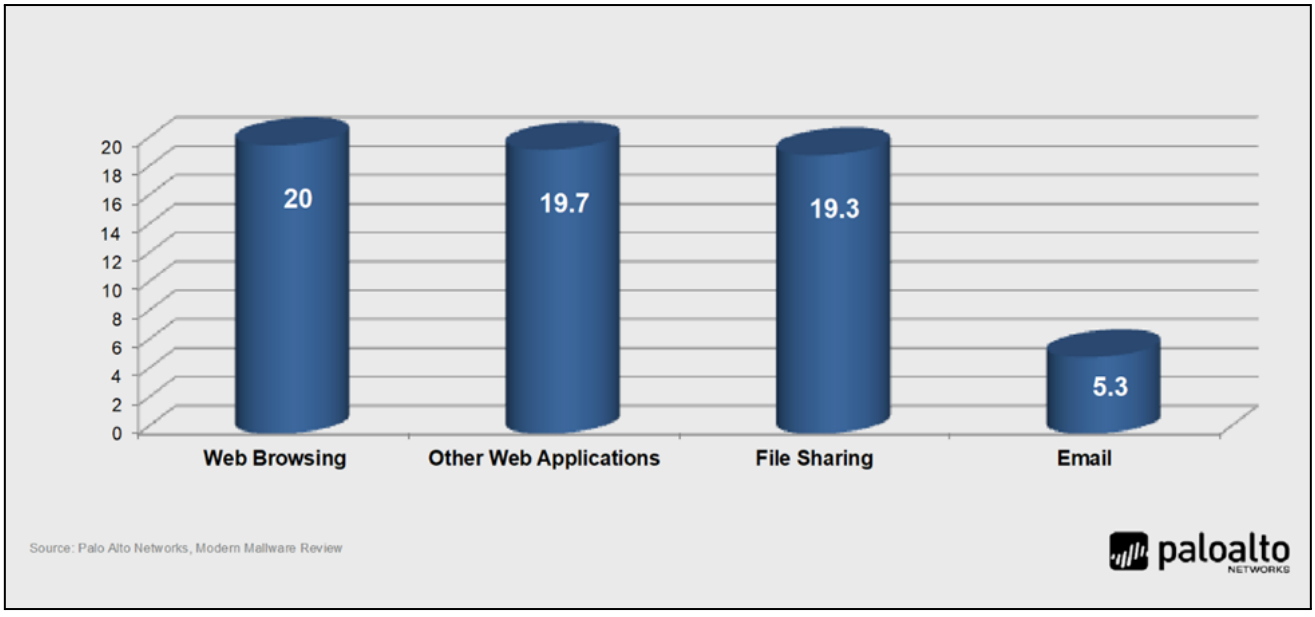


Figure: Average time to detection by application vector

A sample of new or unknown suspicious traffic first must be captured and identified before a detection signature can be created by security vendors. The new signature then must be downloaded and installed on an organization's endpoints to provide protection.

This process means that some users and networks will be successfully breached by new malware until a new detection signature is created, downloaded, and installed. This reactive model creates a window of opportunity for attackers, leaving endpoints vulnerable, sometimes for weeks or even months, until new malware is suspected, collected, analyzed, and identified. During this time, attackers can infect networks and endpoints.

Another challenge for the signature-based approach is that millions of new malware variations are created each year (on average about 20,000 new forms daily), for which unique signatures must be written, tested, and deployed after the new malware variation is discovered and sampled. Despite the fact that 70 percent of these millions of malware variations are based on a relatively limited number of malware "families" numbering just seven in 2005 and increasing to only 20 over the past decade, this reactive approach is not effective for protecting endpoints against modern malware threats.

Also, advanced malware uses techniques such as metamorphism and polymorphism to take advantage of the inherent weaknesses of signature-based detection to avoid being discovered in the wild and to circumvent signatures that have already been created.

2.23.4 Describe application block and allow listing

Application block

Although the overall goal of your security policy is to safely enable applications using application whitelist rules (also known as positive enforcement), the initial best practice rulebase must also include rules to help you find gaps in your policy and identify possible attacks. Because these rules are designed to catch things you didn't know were running on your network, they allow traffic that could also pose security risks on your network. Therefore, before you can create the temporary rules, you must create rules that explicitly blacklist applications designed to evade or bypass security or that are commonly exploited by attackers, such as public DNS and SMTP, encrypted tunnels, remote access, and non-sanctioned file-sharing applications.

Step 1: Block applications that do not have a legitimate use case.

Rule Highlights

- Use the Drop Action to silently drop the traffic without sending a signal to the client or the server.
- Enable logging for traffic matching this rule so that you can investigate misuse of applications and potential threats on your network.
- Because this rule is intended to catch malicious traffic, it matches to traffic from any user running on any port.

			Source			Destination						
Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
Block Bad Apps	Best Practice	universal	Users	any	any	Internet	any	encrypted tunnels file sharing remote access	any	Drop	none	

Step 2: Block public DNS and SMTP applications.
Rule Highlights

- Use the **Reset both client and server** Action to send a TCP reset message to both the client-side and server-side devices.
- Enable logging for traffic matching so that you can investigate a potential threat on your network.

			Source			Destination				
Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	Action
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	Internet	any	dns smtp	any	Reset Both

Application allow lists

Application allow lists are another endpoint protection technique that is commonly used to prevent end users from running unauthorized applications, including malware, on their endpoints.

Application allow lists require a positive control model in which no applications are permitted to run on the endpoint unless explicitly permitted to do so by the allow list policy. In practice, application allow lists require a large administrative effort to establish and maintain a list of approved applications. This approach is based on the premise that if you create a list of applications that are specifically allowed and then prevent any other file from executing, you can protect the endpoint. Although this basic functionality can be useful to reduce the attack surface, it is not a comprehensive approach to endpoint security.

Modern trends such as cloud and mobile computing, consumerization, and bring your own device (BYOD) and bring your own access (BYOA) make application allow lists extremely difficult to enforce in the enterprise. Also, after an application is added to an allow list, it is permitted to run, even if the application has a vulnerability that can be exploited. An attacker then can simply exploit an allowed application and have complete control of the target endpoint regardless of the allow list. After the application has been successfully exploited, the attacker can run malicious code while keeping all of the activity in memory. Because no new files are created and no new executables attempt to run, allow-list software is rendered ineffective against this type of attack.

2.23.5 Describe the concepts of false-positive and false-negative alerts

In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative incorrectly identifies a threat as legitimate traffic.

2.23.6 Describe the purpose of anti-spyware software

Anti-spyware software is very similar to traditional antivirus software because it uses signatures to look for other forms of malware beyond viruses, such as adware, malicious web application components, and other malicious tools, which share user behaviors without their permission.

Key Terms

- In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative incorrectly identifies a threat as legitimate traffic.

2.23.7 Reference

- "2019 Trustwave Global Security Report." Trustwave. 2019, https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/.
- "2019 Trustwave Global Security Report." Trustwave. 2019, https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/.

2.24 Identify differences in managing wireless devices compared to other endpoint devices

There are several challenges that must be addressed when attempting to manage wireless devices:

1. Links

A clear understanding of network topology is required to properly manage a wireless network. This includes not just the access points, connected end-points, and other stations, but also the types of links (active, standby, or backup) being utilized for access to the network.

2. Client tracking

Managing and tracking the clients connected to a wireless access point in a network is another fundamental challenge for managing wireless environments. Clients attached to an access point are typically dynamic. As a result, client connectivity maps give meaningful insights for proper planning. One example of an insight would be the identification of usage patterns for clients as they dynamically switch connectivity between various access points within an environment.

3. Throughput

For wireless connections, throughput depends on the signal strength and interference from other access points. As a result, clients get different throughput at different locations. Problematic areas must be identified so that network administrators might make adjustments to coverage. Topology diagrams are one tool that can help with planning for the potential throughput requirements of an environment.

4. Dynamic discovery

Many wireless networks allow the dynamic addition of new access points, and the discovery and provisioning of new access points is often a requirement for the management of dynamic networks.

5. Inspections

Since wireless networks are highly dynamic, and the network topology of a wireless network can change very often, the tracking and identification of such network changes becomes essential for the administrators to have any chance of maintaining a healthy environment. To achieve this, the status of the wireless devices should be checked frequently. A device's status may be obtained via various methods, including asynchronous notifications from the device (such as SNMP traps and TL1 autonomous messages) and polling.

2.25 Describe the purpose of identity and access management

Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

As an example of an IAM policy, a team could create a rule that grants a specific user the right to list files within an object storage bucket in the cloud. Or, an IAM policy could grant a group of users in a branch office the ability to both read and upload files to a local database.

These are just basic examples. In a large-scale environment, a team might maintain dozens or even hundreds of different IAM policies. The policies can be used to manage access rights for any of the dozens of services that the organization may use, either on-premises or in the cloud.
Identity and access management is important because it allows organizations to share IT resources among multiple users and groups. It helps organizations establish trust for who can be signed in to an account (authentication) while at the same time ensuring that each user or group has only the specific access rights that he or she requires (authorization).

Without IAM, teams would struggle to manage access rights in an efficient way. They would have to rely on alternatives such as creating an entirely separate cloud computing account for each user. That would be inefficient to manage, and would make it difficult to share cloud resources between users.

They could also simply allow every user within their team to have the same level of access to every resource in their environment. But that would be insecure because each individual typically needs to access only certain resources. For example, developers who work for the HR department may need to access databases and virtual machines associated only with their applications, while other developers who build software for the finance department require different permissions. If you were to give all developers access to all resources, you would increase the risk of security oversights and exposures.

With IAM, it's easy to ensure that each user and group has exactly the level of access rights he, she, or they need – no more and no less. Doing so adheres to the principle of least privilege, which states that access rights should be restricted to the minimum necessary for a user to complete his or her work.

2.25.1 Single- and Multi-factor authentication

Authentication is a method for protecting services and applications by verifying the identities of users so that only legitimate users have access. Several firewall and Panorama features require authentication. Administrators authenticate to access the web interface, CLI, or XML API of the firewall and Panorama. End users authenticate through Captive Portal or GlobalProtect to access various services and applications. You can choose from several authentication services to protect your network and to accommodate your existing security infrastructure while ensuring a smooth user experience.

Single-factor Authentication

The firewall and Panorama can use external servers to control administrative access to the web interface and end user access to services or applications through Captive Portal and GlobalProtect. In this context, any authentication service that is not local to the firewall or Panorama is considered external, regardless of whether the service is internal (such as Kerberos) or external (such as a SAML identity provider) relative to your network.

Multi-factor authentication (MFA)

You can Configure Multi-Factor Authentication (MFA) to ensure that each user authenticates using multiple methods (factors) when accessing highly sensitive services and applications. For example, you can force users to enter a login password and then enter a verification code that they receive by phone before allowing access to important financial documents. This approach helps to prevent attackers from accessing every service and application in your network just by stealing passwords. Of course, not every service and application requires the same degree of protection, and MFA might not be necessary for less sensitive services and applications that users access frequently. To accommodate a variety of security needs, you can Configure Authentication Policy rules that trigger MFA or a single authentication factor (such as login credentials or certificates) based on specific services, applications, and end users.

2.25.2 Separation of duties and impact on privileges

Server and system administrators perform a variety of important tasks in a network environment. Typical server and system administration tasks include:

- Account provisioning and deprovisioning
- Managing account permissions
- Installing and maintaining server software
- Maintaining and optimizing servers, applications, databases (may be assigned to a database administrator), network devices (may be assigned to a network administrator), and security devices (may be assigned to a security administrator)
- Installing security patches
- Managing system and data backup and recovery
- Monitoring network communication and server logs
- Troubleshooting and resolving server and system issues

Identity and Access Management (IAM) provides authentication, authorization, and access control functions. IAM tools provide control for the provisioning, maintenance, and operation of user identities and the level of access to network, data center, and cloud resources that different identities are permitted.

Directory services
A directory service is a database that contains information about users, resources, and services in a network. The directory service associates users and network permissions to control who has access to which resources and services on the network. Directory services include:

- Active Directory: A centralized directory service developed by Microsoft for Windows networks to provide authentication and authorization of users and network resources. Active Directory uses Lightweight Directory Access Protocol (LDAP), Kerberos, and the Domain Name System (DNS).
- Lightweight Directory Access Protocol (LDAP): An IP-based client-server protocol that provides access and manages directory information in TCP/IP networks

2.25.3 RBAC, ABAC, DAC, and MAC

Role-based access control (RBAC) is a method for implementing discretionary access controls in which access decisions are based on group membership, according to organizational or functional roles.

Attribute-based access control (ABAC) is a way to provide and manage user access to IT services to support areas that require more contextual awareness than simple user-focused parameters as an assigned role.

DAC stands for Discretionary Access Control. The app owner has complete control over who can access a particular service. An application can be a file, directory, or any other, which can be accessed via the network. Can grant permission to other users to access the app.

Media access control (MAC) address is a unique 48-bit or 64-bit identifier assigned to a network interface card (NIC) for communications at the Data Link layer of the OSI model.

2.25.4 User profiles

User and group information must be directly integrated into the technology platforms that secure modern organizations. Knowing who is using the applications on your network, and who may have transmitted a threat or is transferring files, strengthens security policies and reduces incident response times. User-ID, a standard feature on Palo Alto Networks next-generation firewalls, enables you to leverage user information stored in a wide range of repositories.

- **Visibility into a User's Application Activity**
  Visibility into the application activity at a user level, not just an IP address level, allows you to more effectively monitor and control the applications traversing the network. You can align application usage with business requirements and, if appropriate, inform users that they are in violation of policy, or even block their application usage outright.

- **User-Based Policy Control**
  Policies can be defined to safely enable applications based on users or groups of users in either outbound or inbound directions. For example, user-based policy control can allow only the IT department to use tools such as SSH, telnet, and FTP on standard ports. With User-ID, policy follows the users no matter where they go – headquarters, branch office, or at home – and whatever device they may use.

- **User-Based Analysis, Reporting, and Forensics**
  Informative reports on user activities can be generated using any one of the pre-defined reports or by creating a custom report.

- **Neutralizing Credential Theft**
  User-ID integrates with identity and authentication frameworks, which enables precise access control through policy-based multi-factor authentication. These controls disrupt the use of stolen credentials.

2.25.5 References

- Authentication Types, https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-types

- User-ID, https://www.paloaltonetworks.com/technologies/user-id

2.26 Describe the integration of NGFWs with the cloud, networks, and Endpoints

After creating rulestacks on your Cloud NGFW tenant, you can create associations between them and NGFW resources and NGFW endpoints. Upon creation, a NGFW is associated with the specified VPC. NGFW endpoints are constructs created – manually or automatically – in each availability zone in the VPC that you specify.

The NGFW is a firewall resource, dedicated to the VPC you specify, that provides next-generation firewall capabilities. The NGFW applies your security policy to the traffic received by the NGFW endpoints and enforces that policy. When creating your NGFW, you must specify a VPC and local rulestack. Additionally, you must also specify how and where the associated NGFW endpoints are deployed.

NGFW endpoints are responsible for directing traffic to the NGFW for inspection and enforcement. NGFW endpoints intercept traffic and route it to the NGFW for inspection and policy enforcement. There are two management modes that can be used to create endpoints automatically or manually.

- In a **service-managed mode**, the Cloud NGFW tenant creates an endpoint in each subnet you specify. The NGFW service retrieves a list of subnets in the VPC you specified and you choose the subnets from that list that should have an endpoint.
- In a **customer-managed mode**, you choose existing availability zones that need to be secured in your specified VPC, then manually create the NGFW endpoints in existing subnets in the chosen availability zones. After the NGFW has been created, you must go to the AWS console to complete the NGFW endpoint creation process.

2.27 Describe App-ID, User-ID, and Content-ID

Application identification

Stateful packet inspection technology, which is the basis for most of today's legacy firewalls, was created more than 25 years ago, at a time when applications could be controlled using ports and source/destination IP addresses. The strict adherence to port-based classification and control methodology is the primary policy element; it is hard-coded into the foundation and cannot be turned off. As a result, many of today's applications cannot be identified, much less controlled, by the firewall, and no amount of "after the fact" traffic classification by firewall "helpers" can correct the firewall port-based classification.

Establishment of port and protocol information is a first step in application identification, but it is insufficient by itself. Robust application identification and inspection in a next-generation firewall enables granular control of the flow of sessions through the firewall. Identification is based on the specific applications (such as Skype, Gmail, and WebEx) that are being used, instead of just relying on the underlying set of often indistinguishable network communication services.

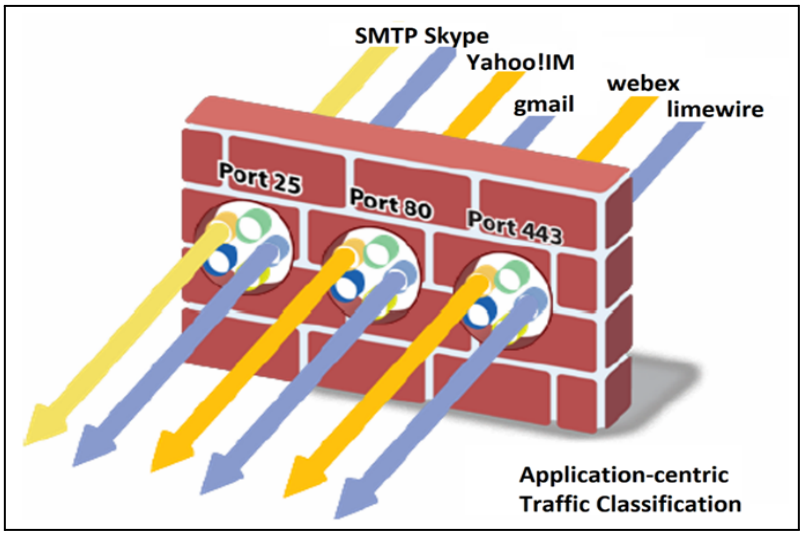


Figure: Application-centric traffic classification identifies specific applications on the network, irrespective of the port and protocol in use.

Application identification provides visibility and control over work-related and non-work-related applications that can evade detection by legacy port-based firewalls, for example, by masquerading as legitimate traffic, hopping ports, or using encryption to slip past the firewall.

Application identification (App-ID) technology in a Palo Alto Networks Next-Generation Firewall does not rely on a single element, such as port or protocol. Instead, App-ID uses multiple mechanisms to first determine what the application is, and the application identity then becomes the basis for the firewall policy that is applied to the session. App-ID is highly extensible, and, as applications continue to evolve, application detection mechanisms can be added or updated as a means of keeping pace with the ever-changing application landscape.

Many organizations are not fully aware of the number of applications in use, how heavily they are used, or by whom. This lack of visibility forces organizations to implement negative (block list) enforcement approaches where they selectively block traffic and destinations known to be a risk to the organization. The next-generation firewall also allows you to implement a positive (allow list)

enforcement policy where you selectively allow the applications required to run your organization. A key to positive enforcement is App-ID. App-ID identifies the applications traversing the firewall, regardless of port or protocol, even if the traffic is tunneled in Generic Routing Encapsulation (GRE) tunnels, uses evasive tactics, or is encrypted. App-ID can determine the difference between base applications and application functions. This level of visibility brings a complete understanding of the applications on your network and their value and risk to your organization.

App-ID traffic classification technology

The first task that a Palo Alto Networks Next-Generation Firewall executes is using App-ID to identify the applications traversing the network. App-ID uses a multifaceted approach to determine the application's identity, irrespective of port, protocol, encryption (SSL and SSH), or other evasive tactics employed. The number and order of identification mechanisms used to identify the application vary depending on the application. The application identification techniques used include:

- **Application signatures**: To identify an application, App-ID first uses signatures to look for unique application properties and related transaction characteristics. The signature also determines whether the application is using its default port or a non-standard port. Context-based signatures look for unique properties and transaction characteristics to correctly identify the application regardless of the port and protocol being used. These signatures include the ability to detect specific functions within applications (such as file transfers within SaaS applications). If the security policy allows the identified application, App-ID further analyzes the traffic to identify more granular applications and scan for threats.

- **TLS/SSL and SSH decryption**: If App-ID determines that TLS/SSL encryption is in use, it can decrypt and re-evaluate the traffic. App-ID uses a similar approach with SSH to determine whether port forwarding is being used to tunnel traffic over SSH.

- **Application and protocol decoding**: For known protocols, decoders apply additional context-based signatures to detect applications tunneling inside the protocols. Decoders validate that traffic conforms to the protocol specification, and they support network address translation (NAT) traversal and opening dynamic pinholes for applications such as Voice over IP (VoIP) or File Transfer Protocol (FTP). Decoders for popular applications also identify the individual functions within the application. In addition to identifying applications, decoders identify files and other content to be scanned for threats or sensitive data.

- **Heuristics**: In certain cases, evasive applications cannot be detected by using advanced signature and protocol decoding. In those cases, App-ID uses heuristic or behavioral analysis to identify applications that use proprietary encryption, such as peer-to-peer (P2P) file sharing. Heuristic analysis, with the other App-ID techniques, provides visibility into applications that might otherwise elude identification. The heuristics are specific to each application and include checks based on information such as the packet length, session rate, and packet source.

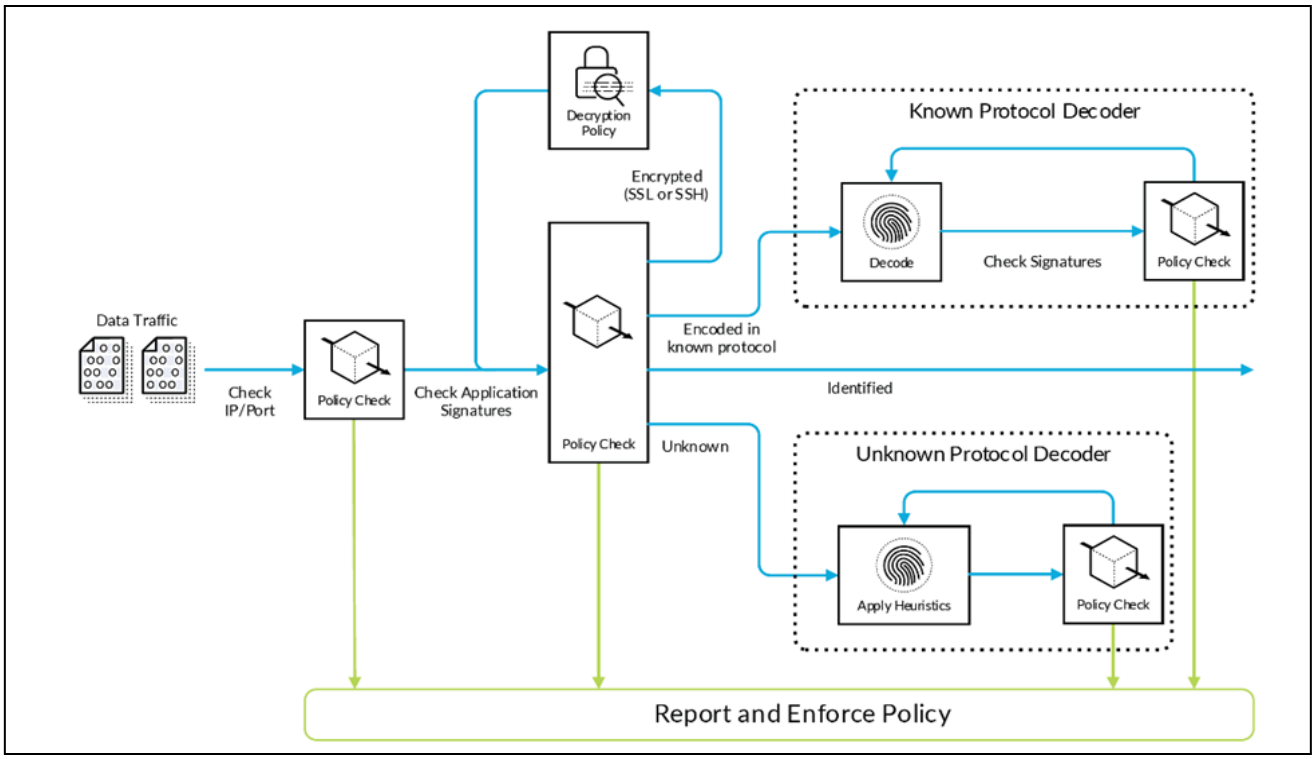


Figure: How Palo Alto Networks App-ID classifies applications

With App-ID as the foundational element for every Palo Alto Networks Next-Generation Firewall, administrators can regain visibility into, and control over, the applications traversing the network.

App-ID: Addressing custom or unknown applications

You can use the Application Command Center (ACC) to see the applications in use across your organization. After you've determined the value of an application to your organization, App-ID controls the security policy for that application. The security policy can include a number of different actions, such as:

- Allowing or denying
- Allowing but scanning the content for exploits, viruses, and other threats
- Allowing based on schedule, users, or groups
- Controlling file or sensitive data transfer
- Allowing or denying a subset of application functions

While you are compiling the list of the applications you want to support, tolerate, or block, App-ID can restrict applications that behave in undesirable ways. You can use application categories, technologies, and risk ratings to define a security policy that will block any applications that match those characteristics.

Safe application enablement often means achieving an appropriate security policy balance between allowing some application functions and denying others. Examples include:

- Allowing Facebook but denying Facebook mail, chat, posting, and apps, effectively allowing users only to browse Facebook
- Allowing the use of SaaS applications such as Dropbox but denying file uploads. This technique grants internal users access to personal file shares but prevents intentional or unintended corporate information leaks.

The list of App-IDs is updated monthly, with new applications added based on input from the Palo Alto Networks community (customers, partners) and market trends. All App-IDs are classified by category, subcategory, technology, and risk rating. The security policy can use these classifications to automatically support new applications as the App-ID list expands. Alternatively, you can specify that you want to review new applications and determine how they are treated before the new list is installed.

Despite regular updates, unknown application traffic inevitably still will be detected on the network, such as:

- Unknown commercial applications: Administrators can use the ACC and the log viewer to quickly determine whether an unknown application is a commercial application. Administrators can use the packet capture (pcap) feature on the Palo Alto Networks Next-Generation Firewall to record the traffic and submit it for App-ID development. The new App-ID is developed, tested with the organization, and then added to the global database for all users.
- Internal or custom applications: Administrators can use the ACC and the log viewer to quickly determine whether an unknown application is an internal or custom application. You can develop a custom App-ID for the application, using the exposed protocol decoders. The protocol decoders that have been exposed include:
    - FTP (File Transfer Protocol)
    - HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure, or HTTP over SSL)
    - IMAP (Internet Message Access Protocol) and SMTP (Simple Mail Transfer Protocol)
    - RTSP (Real Time Streaming Protocol)
    - Telnet
    - Unknown-TCP, unknown-UDP, and file body (for html/pdf/flv/swf/riff/mov)

After the custom App-ID is developed, traffic identified by it is treated in the same manner as the previously classified traffic: It can be enabled via policy, inspected for threats, shaped using quality of service (QoS), etc. Alternatively, users can create and apply an application override, which effectively renames the application. Custom App-ID entries are managed in a separate database on the next-generation firewall to ensure they are not impacted by weekly App-ID updates.

An important point to highlight is that Palo Alto Networks Next-Generation Firewalls use a positive enforcement model, which means that all traffic can be denied except those applications explicitly allowed via policy. This positive enforcement model means that in some cases the unknown traffic can be easily blocked or tightly controlled. Alternative offerings that are based on IPS will allow unknown traffic to pass through without providing any semblance of visibility or control.

App-ID in action: Identifying WebEx

When a user initiates a WebEx session, the initial connection is an SSL-based communication. With App-ID, the device sees the traffic and determines that it is using SSL. If there is a matching decryption policy rule, then the decryption engine and protocol decoders are initiated to decrypt the SSL and detect that it is HTTP traffic. After the decoder has the HTTP stream, App-ID can apply contextual signatures and detect that the application in use is WebEx.

WebEx then is displayed in the ACC and can be controlled via a security policy. If the end user initiates the WebEx Desktop Sharing feature, WebEx undergoes a “mode-shift.” This means the session has been altered from a conferencing application to a remote access application. In this scenario, the characteristics of WebEx have changed, and App-ID detects the WebEx Desktop Sharing feature, which then is displayed in the ACC. At this stage, an administrator has learned more about the application use and can exert policy control over the use of the WebEx Desktop Sharing feature separately from general WebEx use.

Application identification and policy control

Application identification enables administrators to see the applications on the network, learn how they work, and analyze their behavioral characteristics and relative risk. When application identification is used in conjunction with user identification, administrators can see exactly who is using the application based on their identity, rather than just an IP address. With this information, administrators can use granular rules based on a positive security model to block unknown applications, while enabling, inspecting, and shaping those applications that are allowed.

After an application has been identified and a complete picture of its use is gained, organizations can apply policies with a range of responses that are far more granular than the “allow” or “deny” actions available in legacy firewalls. Examples include:

- Allow or deny
- Allow but scan for exploits, viruses, and other threats
- Allow based on schedule, users, or groups
- Decrypt and inspect
- Apply traffic shaping through QoS
- Apply policy-based forwarding
- Allow certain application functions
- Any combination of the preceding examples

Application function control

For many organizations, secure application enablement means achieving an appropriate security policy balance by enabling individual application functionality while blocking other functions within the same application. Examples may include:

- Allowing SharePoint documents but blocking the use of SharePoint administration
- Blocking Facebook mail, chat, posting, and applications but allowing Facebook itself, effectively allowing users to browse only Facebook

App-ID uses an application hierarchy that follows a “container and supporting function” model to help administrators easily choose which applications to allow, while blocking or controlling functions within the application. The figure below shows SharePoint as the container application and the individual functions within it.

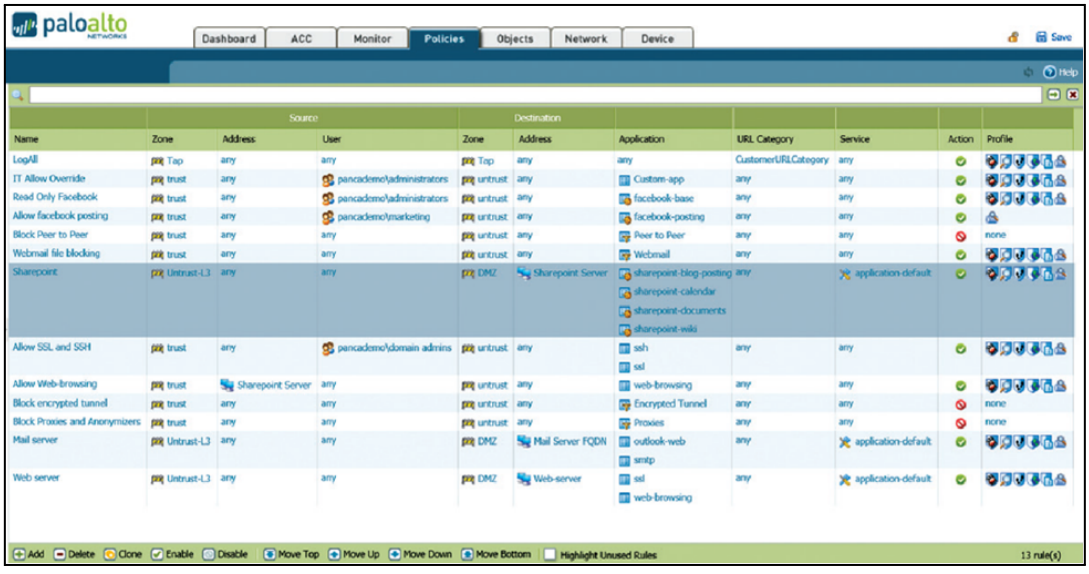


Figure: Application function control maximizes productivity by safely enabling the application itself (Microsoft SharePoint) or individual functions.

User-ID

Creation and management of security policies on a next-generation firewall, based on the application and the identity of the user regardless of device or location, is a more effective means of protecting the network than relying solely on port and IP address information in legacy, port-based firewalls. User-ID enables organizations to leverage user information stored in a wide range of repositories for the following purposes:

- **Visibility:** Improved visibility into application use based on user and group information can help organizations maintain a more accurate view of network activity.
- **Policy control:** Binding user information to the security policy helps organizations to safely enable applications or specific application functions while reducing the administrative effort associated with employee moves, adds, and changes.
- **Logging and reporting:** If a security incident occurs, forensics analysis and reporting can include user information, which provides a more complete view of the incident.

User-ID in action

User-ID seamlessly integrates Palo Alto Networks Next-Generation Firewalls with a wide range of user repositories and terminal services environments. Depending on the network environment, multiple techniques can be configured to accurately map the user identity to an IP address. Events include authentication events, user authentication, terminal services monitoring, client probing, directory services integration, and a powerful XML API.

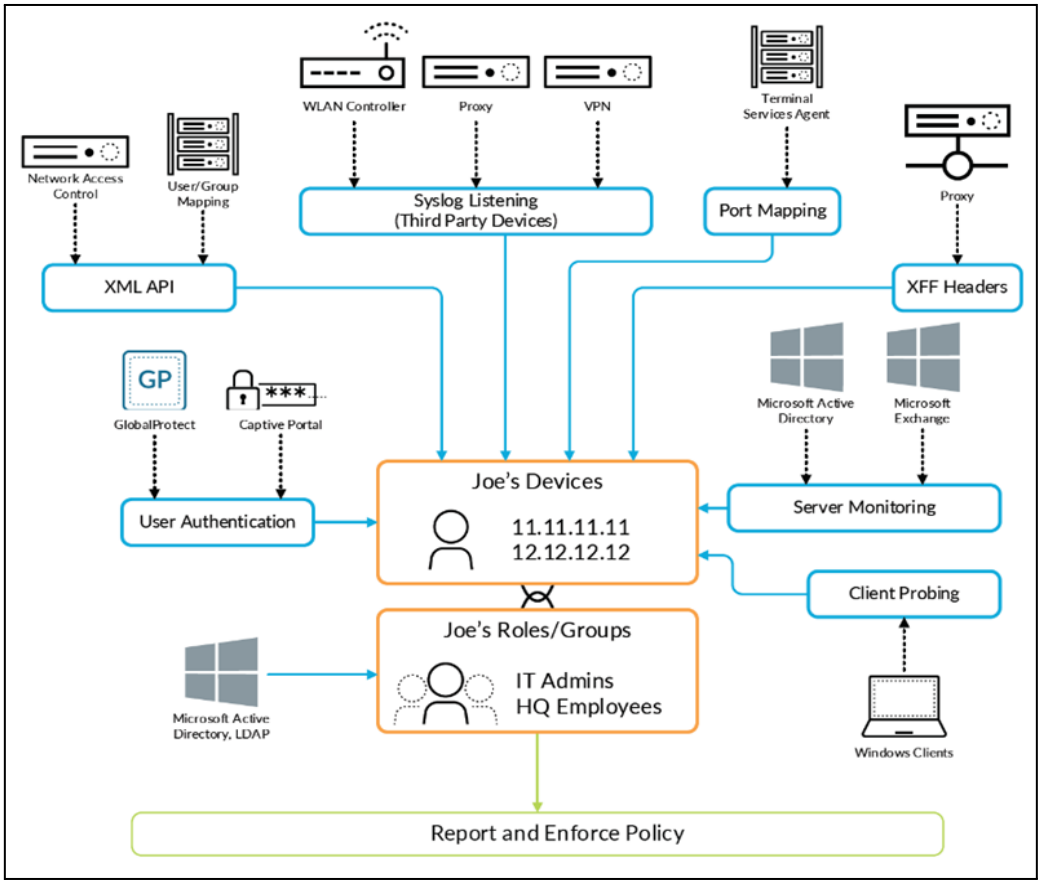


Figure: User-ID integrates enterprise directories for user-based policies, reporting, and forensics.

After the applications and users are identified, full visibility and control within the Application Command Center (ACC), policy editing, and logging and reporting are available. User-ID tools and techniques include:

- **User authentication:** This technique allows organizations to configure a challenge-response authentication sequence to collect user and IP address information, using the following tools:
- **Authentication Portal:** In cases where administrators need to establish rules under which users are required to authenticate to the firewall before accessing the internet, Authentication Portal can be deployed. Authentication Portal is used in cases where the user cannot be identified using other mechanisms. Authentication Portal can be configured to send an NT LAN Manager (NTLM) authentication request to the web browser to make the authentication process transparent to the user.
- **Prisma Access:** Users logging in to the network with Prisma Access provide user and host information to the next-generation firewall, which, in turn, can be used for policy control.
- **Server monitoring:** Monitoring of the authentication events on a network allows User-ID to associate a user with the IP address of the device from which the user logs in to enforce policy on the firewall. User-ID can be configured to monitor authentication events for:
- **Microsoft Active Directory:** User-ID constantly monitors domain controller event logs to identify users when they log in to the domain. When a user logs in to the Windows domain, a new authentication event is recorded on the corresponding Windows domain controller. By remotely monitoring the authentication events on Windows domain controllers, User-ID can recognize authentication events to identify users on the network for creation and enforcement of policy.
- **Microsoft Exchange Server:** User-ID can be configured to constantly monitor Microsoft Exchange login events produced by clients accessing their email. When this monitoring technique is used, even macOS, Apple iOS, and Linux/Unix client systems that don't directly authenticate to Active Directory can be discovered and identified.
- **Novell eDirectory:** User-ID can query and monitor login information to identify users and group memberships via standard Lightweight Directory Access Protocol (LDAP) queries on eDirectory servers.
- **Client probing and terminal services:** This technique enables organizations to configure User-ID to monitor Windows clients or hosts to collect the identity and map it to the IP address. In environments where the user identity is obfuscated by Citrix XenApp or Microsoft Terminal Services, the User-ID Terminal Services agent can be deployed to determine which applications are being accessed by users. The following techniques are available:
- **Client probing:** If a user cannot be identified via monitoring of authentication events, User-ID actively probes Microsoft Windows clients on the network for information about the currently logged-in user. With client probing, laptop users who often switch from wired to wireless networks can be reliably identified.
- **Host probing:** User-ID also can be configured to probe Windows servers for active network sessions of a user. As soon as a user accesses a network share on the server, User-ID identifies the origin IP address and maps it to the username provided to establish the session.
- **Terminal services:** Users sharing IP addresses while working on Microsoft Terminal Services or Citrix can be identified. Every user session is assigned a certain port range on the server, which is completely transparent to the user and allows the next-generation firewall to associate network connections with users and groups sharing one host on the network.

- **XML API:** In some cases, organizations already may have a user repository or an application that is used to store information about users and their current IP address. In these scenarios, the XML API within User-ID enables rapid integration of user information with security policies. The XML API provides a programmatic way to map users to IP addresses through integrations with partner technologies, such as Aruba ClearPass and Aruba Mobility Controllers. Use of the XML API to collect user and IP address information includes:
- **Wireless environments:** Organizations using 802.1x to secure corporate wireless networks can leverage a syslog-based integration with the User-ID XML API to identify users as they authenticate to the wireless infrastructure.
- **Proxies:** Authentication prompted by a proxy server can be provided to User-ID via its XML API by parsing the authentication log file for user and IP address information.
- **Network access control (NAC):** The XML API enables organizations to harvest user information from NAC environments. As an example, a NAC solution provider could use the User-ID XML API to populate user logins and logouts of its 802.1x solution. This integration enables organizations to identify users as soon as they connect to the network and set user-based enablement policies.
- **Syslog listener:** In environments with existing network services that authenticate users (for example, wireless controllers, 802.1x, or NAC products), User-ID can monitor syslog messages for user mapping. Extensible syslog filters control the parsing of syslog messages. Syslog filters can be user-defined, but several predefined filters are available, including those for Blue Coat proxy, wireless local-area networks (WLANs), and Pulse Policy Secure.

To enable organizations to specify security rules based on user groups and resolve the group members automatically, User-ID integrates with directory servers by using a standards-based protocol and a flexible configuration. After integration with the directory server is configured, the firewall automatically retrieves user and user group information and keeps the information updated to automatically adjust to changes in the user base or organization.

After User-ID gathers the user information, the next-generation firewall uses LDAP to obtain group information for that user. Also, as in the case of user mapping, the XML API can serve as a programmatic interface for a flexible group mapping ability. With group mapping, User-ID can express security policies in terms of groups, enabling existing policies to update dynamically as User-ID adds or removes users from groups.

User-ID gives you only half the view when associating IP addresses to specific users. Servers and many other devices cannot utilize a user to identify their security access requirements. Dynamic Address Groups (DAGs) enable you to create policies that automatically adapt to server additions, moves, or deletions. They also enable the flexibility to apply security policy to the device based on its role on the network.

Visibility into a user's activity

The power of User-ID becomes evident when App-ID finds a strange or unfamiliar application on the network. An administrator can use either the ACC or the log viewer to identify the application, who is using the application, the bandwidth and session consumption, the sources and destinations of the application traffic, and any associated threats.

Visibility into the application activity at a user level, not just at an IP address level, allows organizations to more effectively enable the applications traversing the network. Administrators can align application use with business unit requirements and, if appropriate, can choose to inform the user that they are in violation of policy, or they can take the more direct approach of blocking the user's application use.

Content identification
Content identification infuses next-generation firewalls with capabilities not possible in legacy, port-based firewalls. Application identification eliminates threat vectors through the tight control of all types of applications. This capability immediately reduces the attack surface of the network, after which all allowed traffic is analyzed for exploits, malware, dangerous URLs, and dangerous or restricted files or content. Content identification then goes beyond stopping known threats to proactively identify and control unknown malware, which is often used as the leading edge of sophisticated network attacks.

2.28 Describe Palo Alto Networks firewall subscription services

2.28.1 WildFire

Zero-day malware prevention (WildFire)
The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention. Although basic WildFire support is included as part of the Threat Prevention license, the WildFire subscription service provides enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding (APK, PDF, Microsoft Office, and Java Applet), and the ability to upload files by using the WildFire API.

As part of the next-generation firewall's inline threat prevention capability, the firewall performs a hash calculation for each unknown file, and the hash is submitted to WildFire. If any WildFire subscriber has seen the file before, then the existing verdict for that file is immediately returned. Links from inspected emails also are submitted to WildFire for analysis. Possible verdicts include:

- **Benign:** Safe and does not exhibit malicious behavior
- **Grayware:** No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)
- **Malware:** Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits)
- **Phishing:** Malicious attempt to trick the recipient into revealing sensitive data

If WildFire has never seen the file, the next-generation firewall is instructed to submit the file for analysis. If the file size is under the configured size limit, the next-generation firewall securely transmits the file to WildFire. Next-generation firewalls with an active WildFire license perform scheduled auto-updates to their WildFire signatures, with update checks configured as often as every minute.

WildFire leverages inline machine learning based malware and phishing prevention (real-time WildFire verdict and anti-malware dynamic classification) to determine whether the corresponding webpages for email links submitted to the service host any exploits, malware, or phishing capabilities. The behaviors and properties of the website are taken into consideration when a verdict on the link is made.

To support dynamic malware analysis across the network at scale, WildFire is built on a cloud-based architecture. Where regulatory or privacy requirements prevent the use of public cloud infrastructure, a private cloud solution can be built in an on-premises data center.

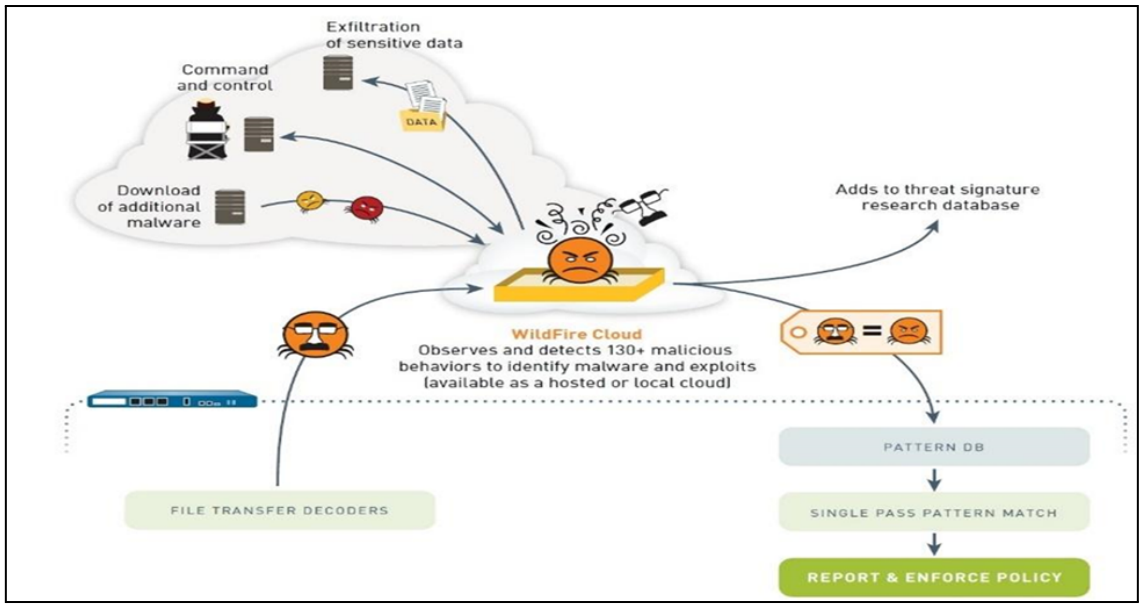


Figure: WildFire provides cloud-based malware analysis and threat prevention.

Organizations can leverage either public cloud or private cloud deployments, and also can use both within the same environment. The hybrid cloud capabilities of WildFire allow security teams more file analysis flexibility because they can define which file types are sent to the WildFire public cloud versus the on-premises appliance, or private cloud. The WildFire hybrid cloud capability enables organizations to alleviate privacy or regulatory concerns by using the WildFire appliance for file types containing sensitive data. Organizations also benefit from the comprehensive analysis and global threat intelligence services of the WildFire public cloud for all others. AutoFocus is the centerpiece of WildFire threat intelligence.

The product portfolio proactively blocks known threats, which provides baseline defenses against known exploits, malware, malicious URLs, and C2 activity. When new threats emerge, the product portfolio automatically routes suspicious files and URLs to WildFire for deep analysis.

WildFire inspects millions of samples per week from its global network of customers and threat intelligence partners, looking for new forms of previously unknown malware, exploits, malicious domains, and outbound C2 activity. The cloud-based service automatically creates new protections that can block targeted and unknown malware, exploits, and outbound C2 activity by using observations of their actual behavior, rather than relying on pre-existing signatures. The protections are delivered globally in minutes. The result is a closed-loop, automated approach to preventing cyberthreats that includes:

- Positive security controls to reduce the attack surface
- Inspection of all traffic, ports, and protocols to block all known threats
- Rapid detection of unknown threats by observing the actions of malware in a cloud-based execution environment
- Automatic deployment of new protections to ensure that threats are known to all and blocked across the attack lifecycle

2.28.2 URL Filtering

To complement the threat prevention and application control capabilities, a fully integrated, on-box URL filtering database enables security teams to not only control end-user web surfing activities but also to combine URL context with application and user rules. The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages. You can use the URL category as a match criterion in policies, which permits exception-based behavior and granular policy enforcement. For example, you can deny access to malware and hacking sites for all users but allow access to users that belong to the IT security group.

When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories. The malware and phishing URL categories in PAN-DB are updated in real time, which can prevent subsequent attempts to access the site based on the URL category, instead of treating each attempt as unknown. User-credential detection, a part of URL Filtering, allows you to alert on or block users from submitting credentials to untrusted sites. If corporate credentials are compromised, user-credential detection allows you to identify who submitted credentials so that you can remediate.

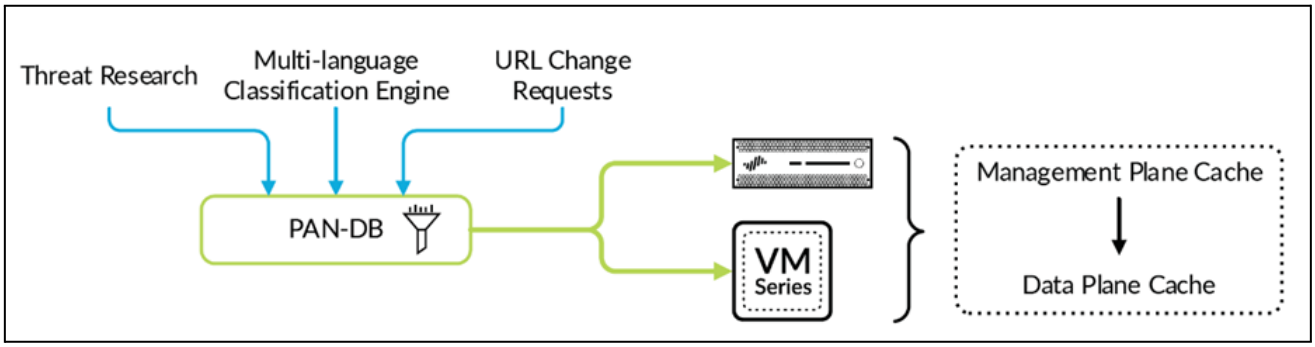


Figure: URL Filtering service

The on-box URL database can be augmented to fit the traffic patterns of the local user community with a custom URL database. For fast and easy access to frequently visited URLs, PAN-DB provides high-performance local caching. This means URLs that are not categorized by the local URL database can be pulled into cache from a hosted URL database. In addition to database customization, administrators can create unique URL categories to further customize the URL controls to fit their specific needs.

URL categorization can be combined with application and user classification to further target and define policies. For example, SSL decryption can be invoked for select high-risk URL categories to ensure that threats are exposed, and QoS controls can be applied to streaming media sites. URL filtering visibility and policy controls can be bound to specific users through transparent integration with enterprise directory services (such as Active Directory, LDAP, and eDirectory), with additional insight provided through customizable reporting and logging.

Administrators can configure a custom block page to notify end users of any policy violations. The page can include references to the username, the IP address, the URL they are attempting to access, and the URL category. To place some of the web activity ownership back to the user, administrators can allow users to continue to the website or webpage after being presented with a warning page, or they can use passwords to override the URL Filtering policy.

2.28.3 Threat Prevention

Threat Prevention blocks known malware, exploits, and C2 activity on the network. Addition of the Threat Prevention subscription brings further capabilities to your next-generation firewall that identify and prevent known threats hidden within allowed applications. The Threat Prevention subscription includes malware/antivirus, C2, and vulnerability protection.

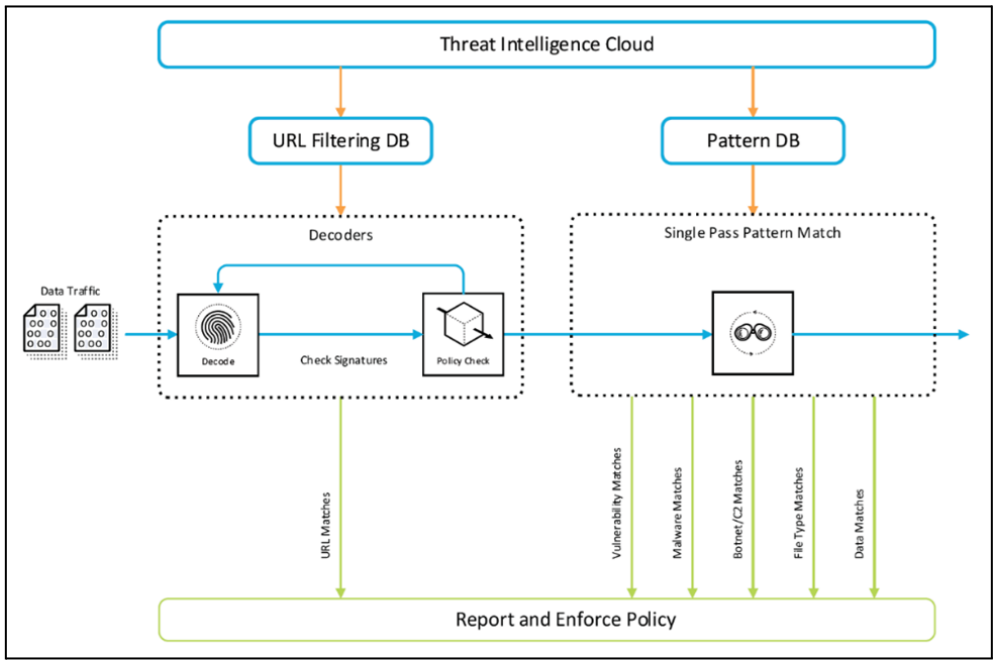


Figure: Threat Prevention service

2.28.4 DNS Security

The Palo Alto Networks DNS Security service applies predictive analytics to disrupt attacks that use DNS for C2 or data theft. Tight integration with Palo Alto Networks Next-Generation Firewalls gives you automated protection and eliminates the need for independent tools. Threats hidden in DNS traffic are rapidly identified with shared threat intelligence and machine learning. Cloud-based protections scale infinitely and are always up to date, thus giving your organization a critical new control point to stop attacks that use DNS.

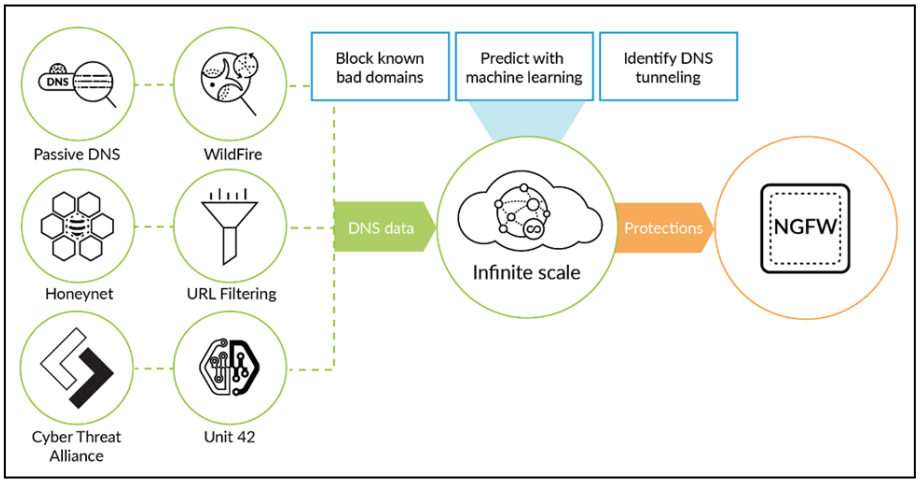


Figure: Rich DNS data powers machine learning for protection.

DNS is a massive and often overlooked attack surface present in every organization. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack, including reliable C2. Security teams struggle to understand new malicious domains and enforce consistent protections for millions of emerging domains at the same time.

The DNS Security service takes a different approach to predicting and blocking malicious domains, thus giving the advantage back to overwhelmed network defenders.
Next-generation firewalls protect you against tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence. Your protection continues to grow with data from a large, expanding threat intelligence-sharing community. The Palo Alto Networks malicious domain database has been gathered over years, with sources including:

- WildFire malware prevention service to find new C2 domains, file download source domains, and domains in malicious email links
- URL Filtering to continuously crawl newly found or uncategorized sites for threat indicators
- Passive DNS and device telemetry to understand domain resolution history seen from thousands of deployed next-generation firewalls, generating petabytes of data per day
- Unit 42 threat research to provide human-driven adversary tracking and malware reverse engineering, including insight from globally deployed honeypots
- More than 30 third-party sources of threat intelligence to enrich understanding

With the DNS Security service, your next-generation firewalls can predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement. Malware's use of domain generation algorithms (DGAs) continues to grow, limiting the effectiveness of blocking known malicious domains alone. DGA malware uses a list of randomly generated domains for C2, which can overwhelm the signature capability of traditional security approaches. DNS Security handle DGA malware by using:

- Machine learning to detect new and never-before-seen DGA domains by analyzing DNS queries as they are performed
- Easy-to-set policy for dynamic action to block DGA domains or sinkhole DNS queries
- Threat attribution and context to identify the malware family with machine learning for faster investigation efforts

A cloud-based database scales infinitely to provide limitless protection against malicious domains. Your protections are always up to date, whether 10,000 or 100 million new malicious domains are created in a single day. As part of the cloud-based service, all DNS queries are checked against the Palo Alto Networks infinitely scalable, cloud-based database in real time to determine appropriate enforcement action. The DNS Security service removes one of the most effective and widely used methods by which attackers establish C2, and its protection scales infinitely, ensuring your next-generation firewalls can process new malicious domains before any harm is done.

Neutralize DNS tunneling

Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. The sheer volume of DNS traffic often means defenders simply lack the visibility or resources to universally inspect it for threats. The DNS Security service enables you to:

- Use machine learning to quickly detect C2 or data theft hidden in DNS tunneling. Using historical and real-time shared threat intelligence, Palo Alto Networks algorithms observe the features of DNS queries, including query rate and patterns, entropy, and n-gram frequency analysis of the domains to accurately detect tunneling behavior.

- Extend PAN-OS signature-based protection to identify advanced tunneling attempts. DNS Security expands the native ability of next-generation firewalls to detect and prevent DNS tunneling. Protections are scalable and evasion-resistant, thus covering known and unknown variants of DNS tunneling.
- Rapidly neutralize DNS tunneling with automated policy action. DNS tunneling is automatically stopped with the combination of easy-to-set policy actions on the next-generation firewall and blockage of the parent domain for all customers.

Simplify security with automation and replace standalone tools

Security teams need integrated innovations that extend the value of their existing security investments without complicating operations. DNS Security takes advantage of the next-generation firewall to stop attacks using DNS, with full automation to reduce manual effort.

Tight integration with the next-generation firewall provides a critical new control point to stop attacks that use DNS. The service ensures that you have one device to deploy, with a single set of policies to manage. Alerts are coordinated across your entire security stack, including firewall policy violations, IDS/IPS, web security, and malware analysis.

When attacks using DNS are identified, security administrators can automate the process of sinkholing malicious domains on the firewall to eliminate C2 and rapidly identify infected users on the network. The combination of malicious domain sinkholing, DAGs, and logging actions automates detection and response workflows, thus saving analysts time by removing slow and manual processes.

The DNS Security service is built on a modular, cloud-based architecture to seamlessly add new detection, prevention, and analytics capabilities with zero impact to production next-generation firewalls.

2.28.5 IoT Security

The IoT Security solution works with next-generation firewalls to dynamically discover and maintain a real-time inventory of the IoT devices on your network. Through AI and machine-learning algorithms, the IoT Security solution achieves a high level of accuracy, even classifying IoT device types encountered for the first time. And because it's dynamic, your IoT device inventory is always up to date. IoT Security also provides the automatic generation of policy recommendations to control IoT device traffic, as well as the automatic creation of IoT device attributes for use in firewall policies.

2.28.6 SD-WAN

PAN-OS® SD-WAN from Palo Alto Networks lets you easily adopt an end-to-end SD-WAN architecture with integrated, best-in-class security to deliver consistent, integrated security across branches, data centers, and the cloud by leveraging the industry's leading ML-powered NGFW to protect applications, users, and devices against all threats. It provides optimized performance by gaining the flexibility to leverage Prisma® Access hubs, data center hubs, or branches for application access. Customers can now simplify branch onboarding using Prisma Access hubs and data centers together as the global backbone; intelligently route traffic based on application performance with zero restrictions on bandwidth availability; and centrally manage security and networking policies for data centers, hubs, and branches to reduce operational complexity and cost while improving collaboration between network and security operations center (NOC and SOC) teams.

It delivers consistent security across branches, data centers, and the cloud by leveraging the industry's leading ML-powered NGFW to protect applications, users, and devices against all threats while

delivering predictive performance. It embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts while, in turn, leveraging cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW. In addition, it uses behavioral analysis to detect IoT devices and make policy recommendations as part of a cloud-delivered and natively integrated service on the NGFW.

It improves the end user experience by gaining the flexibility to leverage Prisma Access hubs, data center hubs, or branches for application access. In addition, it intelligently routes traffic based on application performance, with no restriction on bandwidth availability, by measuring and monitoring specific paths as well as dynamically moving sessions to the optimal path, guaranteeing the best branch user experience. You can simply enable the subscription on your Next-Generation Firewalls and begin intelligently, securely routing branch traffic to your cloud applications and between other sites. Through a concept called “link tag,” the Firewall will automatically combine all service provider links labeled with the same link to its own set of thresholds and path forwarding rules. With DIA AnyPath, you can tailor exactly how an internet application fails over—either to another DIA internet path at the same site or through a private VPN path to another location to get the better internet service. This ensures that all mission-critical applications are performing at their best to provide the highest level of usability.

2.28.7 Advanced Threat Prevention

Advanced Threat Prevention is a cloud-delivered security service that works in conjunction with your existing Threat Prevention license to deliver protections for advanced and evasive command-and-control (C2) threats. This allows you to prevent unknown threats using real-time traffic inspection of inline detectors. These deep learning, ML-based detection engines in the Advanced Threat Prevention cloud analyze traffic for advanced C2 and spyware threats to protect users against zero-day threats. By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages or operate process-intensive, firewall-based analyzers which can consume copious resources. The cloud-based detection engine logic is continuously monitored and updated using C2 traffic datasets from WildFire, with additional support from Palo Alto Networks threat researchers, who provide human intervention for highly accurized detection enhancements. Advanced Threat Prevention deep learning engines support analysis of C2-based threats over HTTP, HTTP2, SSL, unknown-UDP, and unknown-TCP applications. Additional analysis models are delivered through content updates; however, enhancements to existing models are performed as a cloud-side update, requiring no firewall update. Advanced Threat Prevention is enabled and configured under inline cloud analysis located in the anti-spyware security profile.

2.28.8 Advanced URL Filtering

Palo Alto Networks URL filtering solution, the Advanced URL Filtering subscription, provides real time URL analysis and malware prevention. In addition to PAN-DB access, the Palo Alto Networks-developed URL filtering database for high-performance URL lookups also offers coverage against malicious URLs and IP addresses. This multi-layered protection solution is configured through your URL filtering profile.

2.28.9 GlobalProtect

The GlobalProtect app provides a simple way to extend the enterprise security policies out to mobile endpoints. As with other remote endpoints running the GlobalProtect app, the mobile app provides secure access to your corporate network over an IPsec or SSL VPN tunnel. The app automatically connects to the gateway that is closest to the end user's current location. In addition, traffic to and from the endpoint is automatically subject to the same security policy enforcement as other hosts on your corporate network. The mobile app also collects information about the host configuration and can use this information for enhanced HIP-based security policy enforcement.

There are two primary methods for installing the GlobalProtect app: You can deploy the app from your third-party MDM and transparently push the app to your managed endpoints, or you can install the app directly from the official store for your endpoint:

- iOS endpoints—App Store
- Android endpoints and Chromebooks—Google Play

Starting with GlobalProtect app 5.0, the GlobalProtect app for Chrome OS is not supported; use the GlobalProtect app for Android instead.

- Windows 10 phones and Windows 10 UWP endpoints—Microsoft Store

2.28.10 Enterprise DLP

Data loss prevention (DLP) is a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing.

Enterprise DLP is a cloud-based service that uses supervised machine learning algorithms to sort sensitive documents into Financial, Legal, Healthcare, and other categories for document classification, which helps to guard against exposures, data loss, and data exfiltration. These patterns can identify the sensitive information in traffic flowing through your network and protect them from exposure.

Enterprise DLP allows you to protect sensitive data in the following ways:

- **Prevent file uploads and non-file based traffic from leaking to unsanctioned web applications**—Discover and conditionally stop sensitive data from being leaked to untrusted web applications.
- **Monitor uploads to sanctioned web applications**—Discover and monitor sensitive data when it is uploaded to sanctioned corporate applications.

Enterprise DLP is enabled through a cloud service to help you inspect content and analyze the data in the correct context so that you can accurately identify sensitive data and secure it to prevent incidents. Enterprise DLP supports over 380 data patterns and many predefined data filtering profiles. Enterprise DLP is designed to automatically make new patterns and profiles available to you for use in Security policy rules as soon as they are added to the cloud service.

Use the following tools to configure Enterprise DLP:

- Data Patterns—Help you detect sensitive content and determine how that content is being shared or accessed on your network.

  Predefined data patterns and built-in settings make it easy for you to protect data that contain certain properties (such as document title or author), credit card numbers, regulated information from different countries (such as driver's license numbers), and third-party DLP labels. To improve detection rates for sensitive data in your organization, you can supplement predefined data patterns by creating custom data patterns that are specific to your content inspection and data protection requirements. In a custom data pattern, you can also define regular expressions and data properties to look for metadata or attributes in the file's custom or extended properties and use it in a data filtering profile.

- Data Filtering Profiles—Power the data classification and monitor capabilities available on your managed firewalls to prevent data loss and mitigate business risk.

  Data filtering profiles are a collection of data patterns that are grouped together to scan for a specific object or type of content. To perform content analysis, the predefined data filtering profiles have data patterns that include industry-standard data identifiers, keywords, and built-in logic in the form of machine learning, regular expressions, and checksums for legal and financial data patterns. When you use the data filtering profile in a Security policy rule, the firewall can inspect the traffic for a match and take action.

  After you utilize the data patterns (either predefined or custom), you manage the data filtering profiles from Panorama. You can use a predefined data filtering profile, or create a new profile and add data patterns to it. Then, create security policies and apply the profiles you added to the policies you create. For example, if a user uploads a file and data in the file matches the criteria in the policies, the managed firewall either creates an alert notification or blocks the file upload.

When traffic matches a data filtering profile that a security rule is using, a data filtering log is generated. The log entry contains detailed information regarding the traffic that matches one or more data patterns in the data filtering profile. The log details enable forensics by allowing you to verify when matched data generated an alert notification or was blocked.

You can view the snippets in the Data Filtering logs. By default, data masking partially masks the snippets to prevent the sensitive data from being exposed. You can completely mask the sensitive information, unmask snippets, or disable snippet extraction and viewing entirely.

To improve detection accuracy and reduce false positives, you can also specify:

- **Proximity keywords**—An asset is assigned a higher accuracy probability when a keyword is within a 200-character distance of the expression. If a document has a 16-digit number immediately followed by Visa, that's more likely to be a credit card number. But if Visa is the title of the text and the 16-digit number is on the last page of the 22-page document, that's less likely to be a credit card number.

You can also use more than one keyword in a keyword group and include or exclude keywords to find when occurrences of specific words appear or do not appear within 200 characters of the expression.

- **Confidence levels**—Along with proximity keywords, confidence levels allow you to specify the probability of the occurrence of proximity keywords in a pattern match. With a Low confidence the managed firewall does not use proximity keywords to identify a match; with a High confidence the managed firewall looks for the proximity keywords within 200 characters of the regular expressions in the pattern before it considers the data pattern in a file or non-file based traffic to be a match.
- **Basic and weighted regular expressions**—A regular expression (regex for short) describes how to search for a specific text pattern and then display the match occurrences when a pattern match is found. There are two types of regular expressions—basic and weighted.
    - A basic regular expression searches for a specific text pattern. When a pattern match is found, the service displays the match occurrences.
    - A weighted regular expression assigns a score to a text entry. When the score threshold is exceeded, the service returns a match for the pattern.

      To reduce false positives and maximize the search performance of your regular expressions, you can assign scores using the weighted regular expression builder when you create data patterns to find and calculate scores for the information that is important to you. Scoring applies a match threshold, and when a score threshold is exceeded, such as enough expressions from a pattern match an asset, the asset will be indicated as a match for the pattern.

      For more information, including a use case and best practices, see Configure Regular Expressions in the Prisma SaaS Administrator's Guide.

Key Idea

- Data filtering profiles are a collection of data patterns that are grouped together to scan for a specific object or type of content.

2.28.11 SaaS Security Inline

SaaS Security Inline natively integrates with your NGFW, Panorama Managed Prisma Access, and Cloud Managed Prisma Access to provide granular SaaS application visibility and control of unsanctioned SaaS apps through advanced analytics, reporting, visualization, categorizations, and Security policy authoring so that you can minimize data security risks to your organization. Employees already inadvertently use SaaS apps that violate compliance agreements or that carry risks that exceed your organization's tolerance. SaaS Security Inline discovers such risks so that you can understand them and take action.

SaaS Security Inline provides easy deployment and inline policy enforcement. SaaS Security Inline leverages ACE (App-ID Cloud Engine) technology and SaaS policy rule recommendations to provide greater and faster SaaS app discovery and a seamless SaaS security workflow between your organization's administrators for improved security posture.

SaaS Security Inline provides:

- **Shadow IT discovery**—Using ACE (App-ID Cloud Engine) technology, it automatically discovers new SaaS apps to keep pace with the new and emerging SaaS apps, identifying approximately 15,000 SaaS apps using machine-learning algorithms to achieve a high-level of accuracy and speed.
- **Shadow IT control**—Enables you to author SaaS policy rule recommendations based on a combination of applications, users and groups, categories, activities, device posture (personal vs. corporate) and Enterprise DLP data profiles. Also allows you to collaborate with your firewall administrator on SaaS security policy rules to control intentional and unintentional risky SaaS apps and user activity, permitting access to corporate SaaS apps only for the legitimate users.
- **Shadow IT visibility and reporting**—Delivers an up-to-date combined view of both unsanctioned and sanctioned SaaS application usage across categories and subcategories, including Content Marketing, Collaboration & Productivity, and ERP:
    - **Risk assessment**—Exposes risky SaaS applications being used in your application ecosystem. The risk score is between 1 (low risk) and 10 (high risk) and is based on over 32 compliance attributes, including COPPA, CJIS, and GDPR; vendor attributes, including Founded, App Domains, and Employee Count, and SaaS Security Inline Report with visibility data aggregated across all SaaS apps; and risk score customizing tools to enable you to manually change risk score for individual SaaS applications without changing the underlying calculation method. You can also adjust the weights for the underlying attributes and allow SaaS Security Inline to recalculate and apply the risk score automatically.
    - **Risk categorization**—Identifies safer alternatives to risky SaaS applications with advanced filters, including drill-down views for granularity to locate the SaaS app that meets your organization's risk tolerance; NPS score metric to assess customer satisfaction with SaaS applications; and tagging, both custom and default, to differentiate sanctioned SaaS apps from unsanctioned SaaS apps being used by employees in your organization. This permits efficient monitoring and policy enforcement.

SaaS Security Inline complements SaaS Security API capabilities to provide an integrated CASB (Cloud Access Security Broker) solution.

2.28.12 Virtual Systems

Virtual systems are separate, logical firewall instances within a single physical Palo Alto Networks firewall. Rather than using multiple firewalls, managed service providers and enterprises can use a single pair of firewalls (for high availability) and enable virtual systems on them. Each virtual system (vsys) is an independent, separately-managed firewall with traffic kept separate from the traffic of other virtual systems.

- Virtual System Components and Segmentation
- Benefits of Virtual Systems
- Use Cases for Virtual Systems
- Platform Support and Licensing for Virtual Systems
- Administrative Roles for Virtual Systems
- Shared Objects for Virtual Systems

2.28.13 References

- Mayan, Gilad David. “The IoT Rundown for 2020: Stats, Risks, and Solutions.” Security Today. January 13, 2020, https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.
- Advanced threat prevention, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/about-threat-prevention/advanced-threat-prevention
- PAN-OS SD-WAN, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pan-os-sd-wan
- SaaS security inline, https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-inline/get-started-with-saas-security-inline/whats-saas-security-inline
- Enterprise DLP, https://docs.paloaltonetworks.com/enterprise-dlp/enterprise-dlp-admin/enterprise-dlp-overview/about-enterprise-data-loss-prevention
- GlobalProtect, https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-apps/deploy-the-globalprotect-app-software/download-and-install-the-globalprotect-mobile-app
- Advanced URL Filtering Subscription, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/enable-advanced-url-filtering
- Virtual systems overview, https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/virtual-systems/virtual-systems-overview
- Activate Licenses and Subscriptions, https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions

2.29 Describe network security management

2.29.1 Identify the deployment modes of Panorama

Panorama enables you to manage all key features of the Palo Alto Networks Next-Generation Firewalls by using a model that provides central oversight and local control. You can deploy Panorama as either an on-premises hardware appliance or a virtual appliance, and you also can deploy it as a virtual appliance in the public cloud.

Three deployment mode options are available for Panorama, which (if necessary) allows for the separation of management and log collection:

- **Panorama mode:** Panorama controls both policy and log management functions for all the managed devices.
- **Management only mode:** Panorama manages configurations for the managed devices but does not collect or manage logs.
- **Log collector mode:** One or more Log Collectors collect and manage logs from the managed devices. This mode assumes that another deployment of Panorama is operating in management only mode.

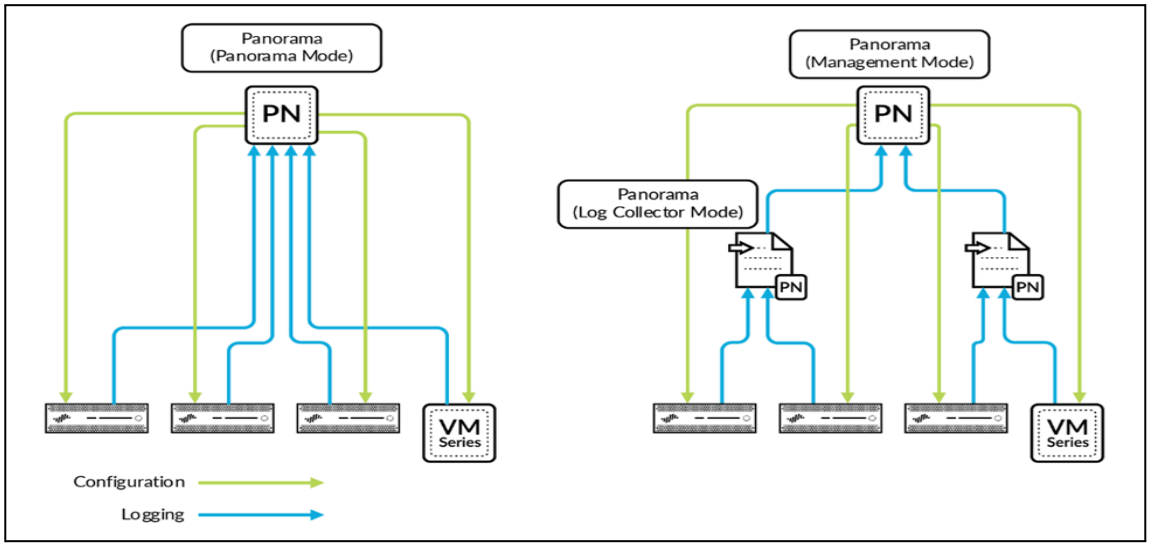


Figure: Panorama deployment modes

The separation of management and log collection enables the Panorama deployment to meet scalability, organizational, and geographical requirements. The choice of form factor and deployment mode gives you the maximum flexibility for managing Palo Alto Networks Next-Generation Firewalls in a distributed network.

Key Idea

- The three deployment mode options available for Panorama are:
  - Panorama mode
  - Management only mode
  - Log collector mode

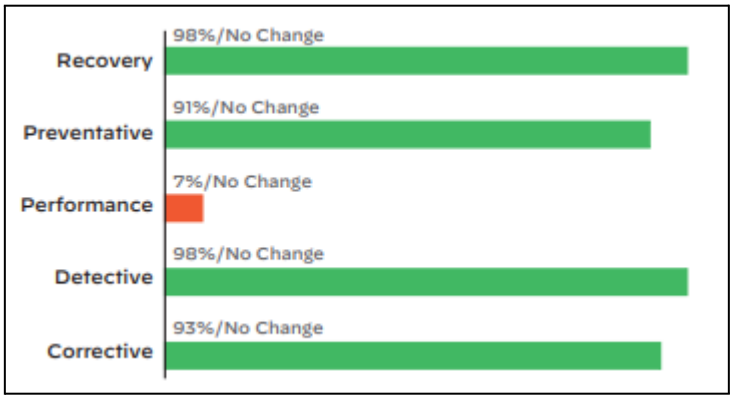
2.29.2 Describe the three components of Best Practice Assessment (BPA)

The BPA consists of three parts: the assessment itself, a Security Policy Capability Adoption Heatmap, and an executive summary.

The **Best Practice Assessment** is a focused evaluation of your adoption of security configuration best practices for Next-Generation Firewalls or Panorama™ network security management, grouped by policies, objects, networks, and devices.

The **Security Policy Capability Adoption Heatmap** shows gaps in your capability adoption, displaying your current adoption percentage rating for each metric as well as a comparison against industry averages. When receiving deep insight into how you are leveraging prevention capabilities, you can continuously improve your security.

The **BPA Executive Summary** is designed for management and executives to better understand the current state of security capability adoption at a glance—including information on progress from prior reports, if available—to help your organization confidently progress toward best practice implementation.



2.29.3 References

- Best Practice Assessment (BPA), https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technology-solutions-briefs/best-practice-assessment-solution-brief.pdf

2.30 Summary of key ideas

- ARPANET was the first packet-switched network created by the U.S. Defense Advanced Research Project Agency (DARPA).
- Open Shortest Path First (OSPF) is an example of a link-state routing protocol that is often used in large enterprise networks.
- Border Gateway Protocol (BGP) is an example of a path-vector protocol used between separate autonomous systems.
- Two basic network topologies which are commonly used in LANs are star and mesh.
- An IP address can be represented with its subnet mask value, using “netbit” or CIDR notation.
- IPv4 is the most widely deployed version of IP consisting of a 32-bit logical IP address.
- A single Internet Key Exchange (IKE) security association is established between communicating entities to initiate the IPsec VPN tunnel.

- Data filtering profiles are a collection of data patterns that are grouped together to scan for a specific object or type of content.
- The three deployment mode options available for Panorama are:
    - Panorama mode
    - Management only mode
    - Log collector mode

Domain 3: Cloud Technologies

3.1 Describe the NIST cloud service and deployment models

The U.S. National Institute of Standards and Technology (NIST) defines cloud computing in Special Publication (SP) 800-145 as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The value of cloud computing is the ability to pool resources to achieve economies of scale and agility. This ability is true for private or public clouds. Instead of requiring many independent and often under-used servers deployed for your enterprise applications, pools of resources are aggregated, consolidated, and designed to be elastic enough to scale with the needs of your organization.

The move toward cloud computing not only brings cost and operational benefits but also technology benefits. Data and applications are easily accessed by users regardless of where they reside, projects can scale easily, and consumption can be tracked effectively. Virtualization is a critical part of a cloud computing architecture that, when combined with software orchestration and management tools, allows you to integrate disparate processes so that they can be automated, easily replicated, and offered on an as-needed basis.

Cloud Service Models

NIST defines three distinct cloud computing service models:

- Software as a service (SaaS): Customers are provided access to an application running on a cloud infrastructure. The application is accessible from various client devices and interfaces, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer may have access to limited user-specific application settings, and security of the customer data still is the responsibility of the customer.
- Platform as a service (PaaS): Customers can deploy supported applications onto the provider's cloud infrastructure, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over the deployed applications and limited configuration settings for the application-hosting environment. The company owns the deployed applications and data, and therefore it is responsible for the security of those applications and data.
- Infrastructure as a service (IaaS): Customers can provision processing, storage, networks, and other computing resources, and deploy and run operating systems and applications. However, the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, along with some networking components (for example, host firewalls). The company owns the deployed applications and data, and is therefore responsible for the security of those applications and data.

Key Idea

- The U.S. National Institute of Standards and Technology (NIST) defines cloud computing in Special Publication (SP) 800-145 as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Cloud Deployment Models

NIST also defines these four cloud computing deployment models:

- Public: A cloud infrastructure that is open to use by the general public. It is owned, managed, and operated by a third party (or parties), and it exists on the cloud provider’s premises.
- Community: A cloud infrastructure that is used exclusively by a specific group of organizations
- Private: A cloud infrastructure that is used exclusively by a single organization. It may be owned, managed, and operated by the organization or a third party (or a combination of both), and it may exist on-premises or off-premises.
- Hybrid: A cloud infrastructure that comprises two or more of the aforementioned deployment models, bound by standardized or proprietary technology that enables data and application portability (for example, fail over to a secondary data center for disaster recovery or content delivery networks across multiple clouds).

3.2 Recognize and list cloud security challenges

3.2.1 Describe the vulnerabilities in a shared community environment

Software composition analysis (SCA) safely enables developers to leverage open source packages without exposing organizations to unnecessary vulnerabilities or legal and compliance issues.

Open source components have become pervasive in modern software development, with the majority of modern applications’ codebases made up of such packages. This method allows developers to move quickly, since they don't need to re-create code that is already freely available and vetted by the community. However, this process also comes with its own set of risks.

What Are the Risks of Using Open Source Components?

Before building container images with these components, developers need to be aware of security concerns stemming from previously discovered vulnerabilities in the packages. They also need to ensure they are meeting compliance requirements around software use licenses.

Community members frequently find and patch vulnerabilities, but the burden is on developers to update their code. When a vulnerability is found, it’s only a matter of time before a public exploit is made available, opening the door for even low-level attackers to take advantage of the issue. Additionally, there are dozens of open source licenses with a variety of rules. For example, some require attribution while others require the source code for the application that uses the component to also be published. Keeping track of all of the licenses and their rules can be difficult.

3.2.2 Describe cloud security responsibilities

The security risks that threaten your network today do not change when you move to the cloud. The *shared responsibility model* defines who (customer and/or provider) is responsible for what (related to security) in the public cloud.

In general terms, the cloud provider is responsible for security *of* the cloud, including the physical security of the cloud data centers, and foundational networking, storage, compute, and virtualization services. The cloud customer is responsible for security *in* the cloud, which is further delineated by the cloud service model (see Figure 3-1).

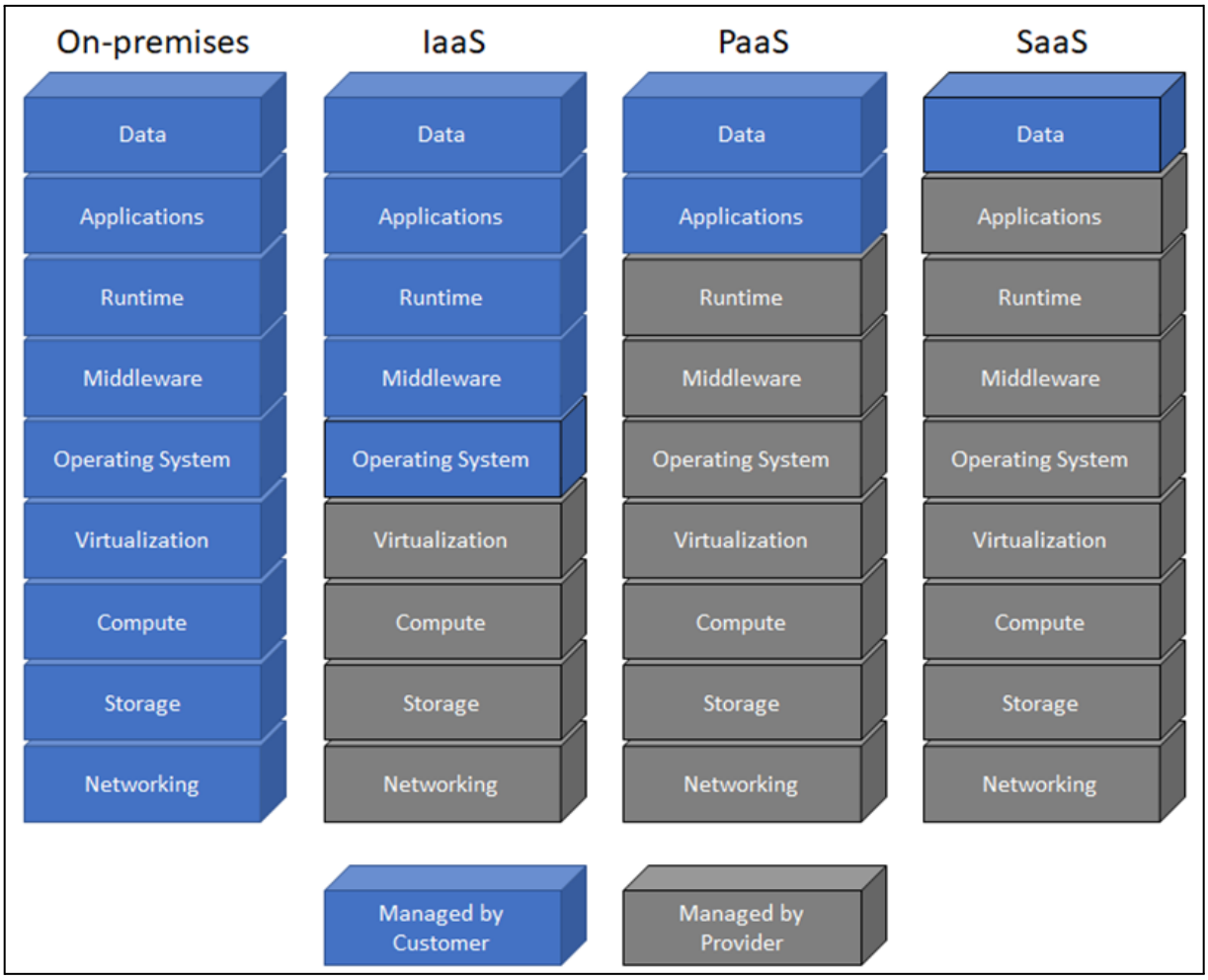


Figure: The shared responsibility model

For example, in an infrastructure-as-a-service (IaaS) model, the cloud customer is responsible for the security of the operating systems, middleware, runtime, applications, and data. In a platform-as-a-service (PaaS) model, the cloud customer is responsible for the security of the applications and data, and the cloud provider is responsible for the security of the operating systems, middleware, and runtime. In a SaaS model, the cloud customer is responsible only for the security of the data, and the cloud provider is responsible for the full stack from the physical security of the cloud data centers to the application. Multitenancy in cloud environments, particularly in SaaS models, means that customer controls and resources are necessarily limited by the cloud provider.

With the use of cloud computing technologies, your data center environment can evolve from a fixed environment where applications run on dedicated servers toward an environment that is dynamic and automated, where pools of computing resources are available to support application workloads that can be accessed anywhere, anytime, from any device.

Security remains a significant challenge when you adopt this new dynamic, cloud-computing fabric environment. Many of the principles that make cloud computing attractive are counter to network security best practices:

- **Cloud computing doesn't mitigate existing network security risks.** The security risks that threaten your network today do not change when you move to the cloud. The shared responsibility model defines who (customer and/or provider) is responsible for what (related to security) in the public cloud. In general terms, the cloud provider is responsible for security of the cloud, including the physical security of the cloud data centers and foundational networking, storage, compute, and virtualization services. The cloud customer is responsible for security in the cloud, which is further delineated by the cloud service model. For example, in an infrastructure-as-a-service (IaaS) model, the cloud customer is responsible for the security of the operating systems, middleware, runtime, applications, and data. In a platform-as-a-service (PaaS) model, the cloud customer is responsible for the security of the applications and data, and the cloud provider is responsible for the security of the operating systems, middleware, and runtime. In a SaaS model, the cloud customer is responsible only for the security of the data, and the cloud provider is responsible for the full stack, from the physical security of the cloud data centers to the application.

- **Security requires isolation and segmentation; the cloud relies on shared resources.** Security best practices dictate that mission-critical applications and data be isolated in secure segments on the network using the Zero Trust principle of "never trust, always verify." On a physical network, Zero Trust is relatively straightforward to accomplish using firewalls and policies based on application and user identity. In a cloud computing environment, direct communication between VMs within a server and in the data center (east-west traffic) occurs constantly, in some cases across varied levels of trust, thus making segmentation a difficult task. Mixed levels of trust, when combined with a lack of intra-host traffic visibility by virtualized port-based security offerings, may weaken an organization's security posture.

- **Security deployments are process-oriented; cloud computing environments are dynamic.** The creation or modification of your cloud workloads often can be done in minutes, yet the security configuration for this workload may take hours, days, or weeks. Security delays are not intentional; they're the result of a process that is designed to maintain a strong security posture. Policy changes need to be approved, the appropriate firewalls need to be identified, and the relevant policy updates need to be determined. In contrast, the cloud is a highly dynamic environment, with workloads (and IP addresses) constantly being added, removed, and changed. The result is a disconnect between security policy and cloud workload deployments that results in a weakened security posture. Security technologies and processes must leverage capabilities such as cloning and scripted deployments to automatically scale and take advantage of the elasticity of the cloud while maintaining a strong security posture.

- **Multitenancy is a key characteristic of the public cloud, and an important risk.** Although public cloud providers strive to ensure isolation between their various customers, the infrastructure and resources in the public cloud are shared. Inherent risks in a shared environment include misconfigurations, inadequate or ineffective processes and controls, and the "noisy neighbor" problem (excessive network traffic, disk I/O, or processor use can negatively impact other customers sharing the same resource). In hybrid and multicloud environments that connect numerous public and/or private clouds, the delineation becomes blurred, complexity increases, and security risks become more challenging to address.

- **Traditional network and host security models don't work in the cloud for serverless applications.** Defense in depth mostly has been performed through Network layer controls. Advanced threat prevention tools can recognize the applications that traverse the network and determine whether they should be allowed. This type of security still is very much required in cloud native environments, but is no longer sufficient on its own. Public cloud providers offer a rich portfolio of services, and the only way to govern and secure many of them is through Identity and Access Management (IAM). IAM controls the permissions and access for users and cloud resources. IAM policies are sets of permission policies that can be attached to either users or cloud resources to authorize what they access and what they can do with what they access.

Key Terms

- **Identity and Access Management (IAM)** is a framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities.

As organizations transition from a traditional data center architecture to a public, private, or hybrid cloud environment, enterprising security strategies must be adapted to support changing requirements in the cloud. Important requirements for securing the cloud include:

- **Consistent security in physical and virtualized form factors:** The same levels of application control and threat prevention should be used to protect both your cloud computing environment and your physical network. First, you need to be able to confirm the identity of your applications, validating their identity and forcing them to use only their standard ports. You also need to be able to block the use of rogue applications while simultaneously looking for and blocking misconfigured applications. Finally, application-specific threat prevention policies should be applied to block both known and unknown malware from moving into and across your network and cloud environment.

- **Your business applications segmented using Zero Trust principles:** To fully maximize the use of computing resources, a relatively common current practice is to mix application workload trust levels on the same compute resource. Although mixed levels of trust are efficient in practice, they introduce security risks in the event of a compromise. Your cloud security solution needs to be able to implement security policies based on the concept of Zero Trust as a means of controlling traffic between workloads while preventing lateral movement of threats.

- Centrally managed business applications; streamlined policy updates: Physical network security still is deployed in almost every organization, so the ability to manage both hardware and virtual form factor deployments from a centralized location using the same management infrastructure and interface is critical. To ensure that security keeps pace with the speed of change that your workflows may exhibit, your security solution should include features that will allow you to reduce, and in some cases eliminate, the manual processes that security policy updates often require.

Regardless of which type of cloud service you use, the burden of securing certain types of workloads will always fall on you instead of your vendor. To maximize your cloud environment security, consider the following best practices:

- **Review default settings:** Although certain settings are automatically set by the provider, some must be manually activated. You should have your own set of security policies rather than assume that the vendor is handling a particular aspect of your cloud native security.
- **Adapt data storage and authentication configurations to your organization:** All locations where data will be uploaded should be password protected. Password expiration policies also should be carefully selected to meet the needs of your organization.
- **Don't assume your cloud data is safe:** Never assume that vendor-encrypted data is totally safe. Some vendors provide encryption services before upload, and some do not. Whichever the case, make sure to encrypt your data in transit and at rest by using your own keys.
- **Integrate with your cloud's data retention policy:** You must understand your vendor's data retention and deletion policy. You must have multiple copies of your data and a fixed data retention period. But what happens when you delete data from the cloud? Is it still accessible to the vendor? Are there other places where it might have been cached or copied? You should verify these issues before you set up a new cloud environment.
- **Set appropriate privileges:** Appropriate settings for privilege levels are helpful for making your cloud environment more secure. When you use role-based access controls (RBACs) for authorization, you can ensure that every person who views or works with your data has access only to the things that are absolutely necessary.
- **Keep cloud software up to date:** Your vendor may provide infrastructure and, in some cases, a prebuilt software environment or cloud native firewall. But anything that you add is your responsibility to secure. Thus, you as a user are responsible for ensuring that your security patches, operating systems, and so on, are up to date. The simplest way to prevent technical debt and backlogs is to automate the updates.
- **Build security policies and best practices into your cloud images:** If you leave your cloud native security to different developers on your DevOps security team, the result could be policy discrepancies. A good way to combat this effect is to create cloud images with security tools configured and policies applied so that developers can simply create instances of them.
- **Isolate your cloud resources:** To reduce the risk of hackers gaining complete control of your system, you should separate admin accounts for development, deployment, testing, and so on.

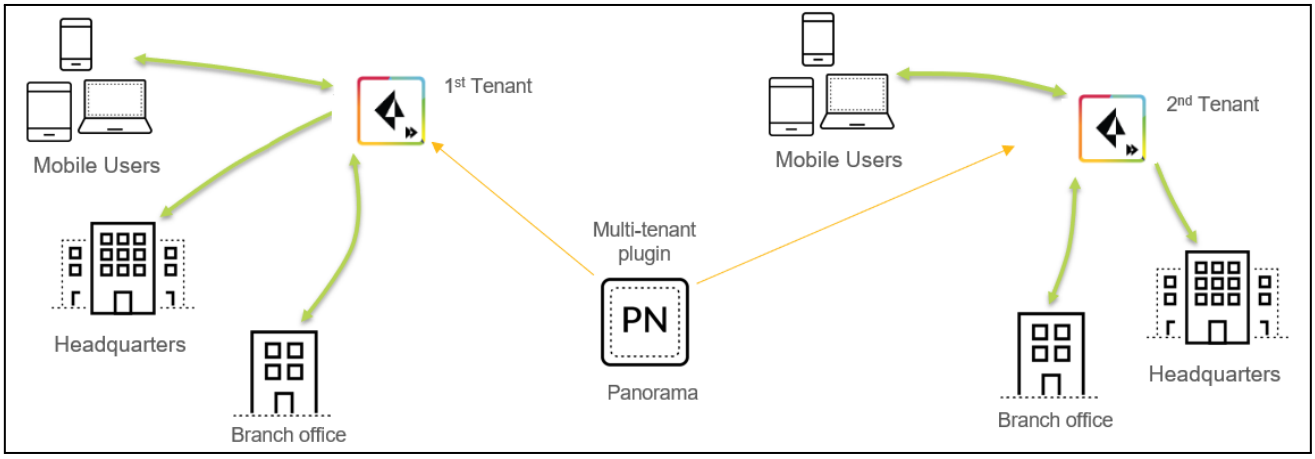
Key Terms

- **Technical debt** is a software development concept, which has also been applied more generally to IT, in which additional future costs are anticipated for rework due to an earlier decision or course of action that was necessary for agility but was not necessarily the most optimal or appropriate decision or course of action.

3.2.3 Describe cloud multitenancy

Enabling multitenancy allows you to host multiple instances of Prisma Access on a single Panorama appliance. Each instance is known as a Tenant.

Prisma Access tenants get their own dedicated Prisma Access instances. They are not shared between tenants.



3.2.4 Differentiate between security tools in various cloud environments

Cloud security, or cloud computing security, consists of various technologies and tools designed to protect each aspect of the Shared Responsibility Model. Although cloud users aren't responsible for the security of the underlying infrastructure, they are responsible for protecting their information from theft, data leakage, and deletion. Many security approaches in the cloud are the same as those of traditional IT security, but there are some fundamental differences. Whether you implement public, private, or hybrid cloud environments, it's important to adopt security controls that facilitate frictionless deployment and don't hinder the dynamic, agile nature for which cloud environments are renowned.

Public Cloud

The public cloud is a cloud computing model in which IT services are delivered via the public internet. In this case, the entire underlying infrastructure is completely owned and operated by a third-party cloud provider, such as Google Cloud, Amazon or Microsoft. Public cloud deployments are often used to provide common services like web-based applications or storage, but they can also be used for complex computations or to test and develop new services. These environments are generally billed via annual or use-based subscriptions based on the number of cloud resources used and traffic processed. Within a public cloud environment, you share the foundational infrastructure with other organizations, and you can access your services as well as deploy and manage your resources through your account. The public cloud yields many potential advantages for businesses, including the ability to deploy highly scalable, globally available applications quickly and without costly upfront investments.

Private Cloud
In a private cloud, infrastructure is provisioned for exclusive use by a single business or organization. It can be owned, managed and operated by the business, a third-party service provider, or a combination of the two. It can also be located on the business's premises or off, similar to the public cloud. Any application can be run in a private cloud environment, including websites, big data and machine learning applications, and databases. The private cloud offers many of the same benefits as the public cloud, such as elastic scalability and cost savings, but it also guarantees resource availability, total control, privacy, and regulatory compliance. This makes private clouds highly desirable to organizations with strict compliance requirements or that demand absolute control over their data location, such as government agencies or financial institutions.

Hybrid Cloud
A hybrid cloud is a combination of on-premises, private, and/or public cloud environments that remain separate yet orchestrated. In a hybrid cloud environment, data and applications can move between environments, enabling greater flexibility – especially for organizations looking to extend their existing on-premises footprints with specific use cases ideally suited for the cloud. As an example, public clouds can be used for high-volume, lower-security needs, such as web-based applications, while private clouds can be used for more sensitive, business-critical operations like financial reporting. Often referred to as the best of both worlds, its adaptability makes it attractive for many enterprises.

3.2.5 Describe identity and access management controls for cloud resources

Identity and Access Management (IAM) provides authentication, authorization, and access control functions. IAM tools provide control for the provisioning, maintenance, and operation of user identities and the level of access to network, data center, and cloud resources that different identities are permitted.

Prisma Cloud IAM Security helps you address the security challenges of managing IAM in cloud environments. Prisma Cloud IAM Security capabilities automatically calculate effective permissions across cloud service providers, detect overly permissive access, and suggest corrections to reach least privilege entitlements. It includes out-of-the-box policies that govern IAM best practices to help you identify risky permissions and achieve the ideal set of privileges for your deployment.

Because Prisma Cloud can correlate identity information with configuration data, it gives you the depth of visibility and control. For example, if you use the AWS S3 storage service, the Prisma Cloud Data Security module can discover and identify sensitive data, the CSPM capability can calculate true internet exposure, and the CIEM capability can provide granular insights into exactly who has access to the data and make appropriate recommendations to enforce least-privilege access.

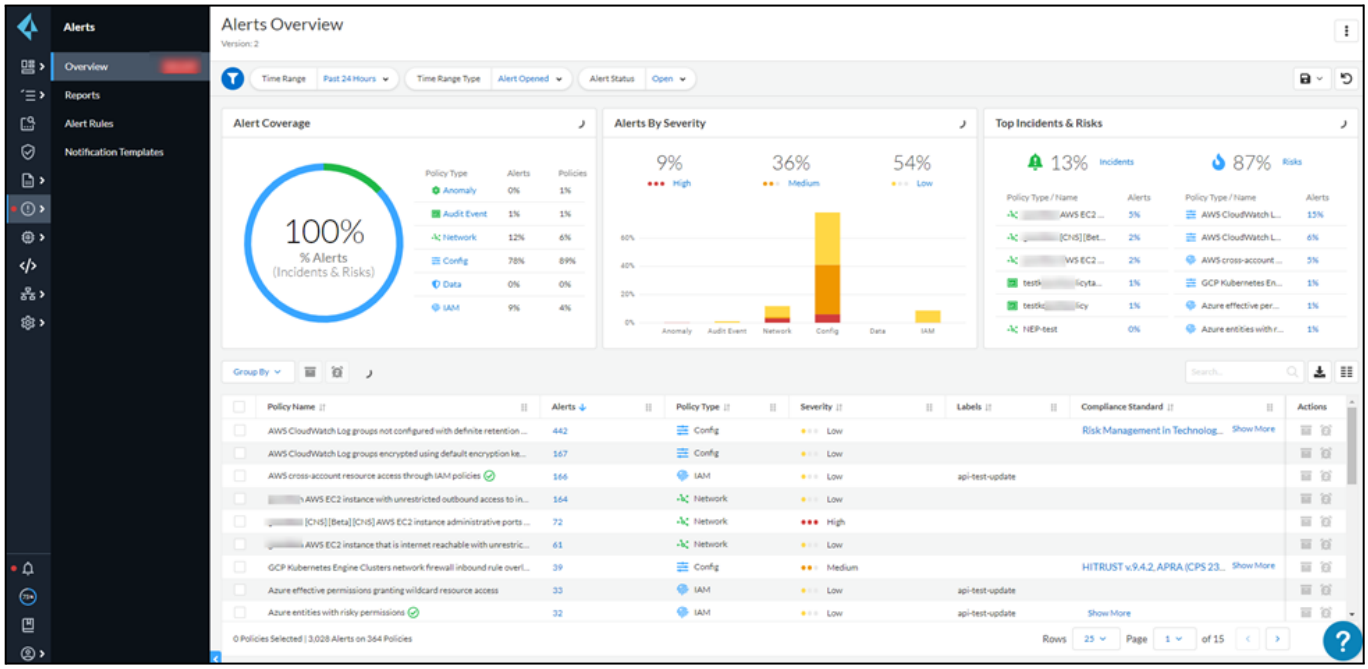
- What is Prisma Cloud IAM Security?
- Enable IAM Security
- Investigate IAM Incidents on Prisma Cloud
- Create an IAM Policy
- Integrate Prisma Cloud with IdP Services
- Remediate Alerts for IAM Security
- Context Used to Calculate Effective Permissions

3.2.6 Describe different types of cloud security alerts and notifications

Prisma Cloud continually monitors all of your cloud environments to detect misconfigurations (such as exposed cloud storage instances), advanced network threats (such as cryptojacking and data exfiltration), potentially compromised accounts (such as stolen access keys), and vulnerable hosts. Prisma Cloud then correlates configuration data with user behavior and network traffic to provide context around misconfigurations and threats in the form of actionable alerts.

Although Prisma Cloud begins monitoring and correlating data as soon as you onboard the cloud account, there are tasks you need to perform before you view alerts generated by policy violations in your cloud environments. The first task to Enable Prisma Cloud Alerts is to add the cloud account to an account group during onboarding. Next, create an alert rule that associates all of the cloud accounts in an account group with the set of policies for which you want Prisma Cloud to generate alerts. You can view the alerts for all of your cloud environments directly from Prisma Cloud and drill down into each to view specific policy violations. If you have internal networks that you want to exclude from being flagged in an alert, you can add Trusted IP Addresses on Prisma Cloud.

From the Alerts Overview page, you can see the alert coverage, based on percentage as well as severity, and also drill down based on policies. You can easily access the policy that triggered the alert, and view the details on the resources and the policy recommendations in separate tabs.



In addition, Prisma Cloud provides out-of-box ability to Configure External Integrations on Prisma Cloud with third-party technologies, such as SIEM platforms, ticketing systems, messaging systems, and automation frameworks so that you can continue using your existing operational, escalation, and notification tools. To monitor your cloud infrastructures more efficiently and provide visibility into actionable events across all your cloud workloads, you can also:

- Generate Reports on Prisma Cloud Alerts on-demand or scheduled reports on open alerts.
- Send the Alert Payload to a third-party tool.

3.2.7 Reference

- Prisma Cloud Alerts and Notifications. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/manage-prisma-cloud-alerts/prisma-cloud-alert-notifications#id1fc26554-036c-42bf-88a6-3687c8e8dbb6
- Multitenancy. https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/manage-multiple-tenants-in-prisma-access/multitenancy-overview
- Identity and access management controls. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/prisma-cloud-iam-security
- What is SCA? https://www.paloaltonetworks.com/cyberpedia/what-is-sca
- What is Cloud Security? https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-security

3.3 Identify the four Cs of cloud native security

Application development methodologies are moving away from the traditional "waterfall" model toward more agile continuous integration/continuous delivery (CI/CD) processes with end-to-end automation. This new approach brings a multitude of benefits, such as shorter time to market and faster delivery, but it also introduces security challenges because traditional security methodologies weren't designed to address these modern application workflows. As developer teams embrace cloud native technologies, security teams find themselves scrambling to keep pace. Limited prevention controls, poor visibility, and tools that lack automation yield incomplete security analytics; all of these things increase the risk of compromise and the likelihood of successful breaches in cloud environments. Meanwhile, the demand for an entirely new approach to security emerges: cloud Native Security Platforms (CNSPs).

The term "cloud native" refers to an approach to building and running applications that takes full advantage of a cloud computing delivery model instead of an on-premises data center. This approach takes the best of what cloud has to offer (scalability, deployability, manageability, and limitless on-demand compute power) and applies these principles to software development, combined with CI/CD automation, to radically increase productivity, business agility, and cost savings.

Cloud native architectures consist of cloud services such as containers, serverless security, platform as a service (PaaS), and microservices. These services are loosely coupled, meaning they are not hardwired to any infrastructure components, thus allowing developers to make changes frequently and without affecting other pieces of the application or other team members' projects, across all technology boundaries such as public, private, and multicloud deployments.

"Cloud native" refers to a methodology of software development that essentially is designed for cloud delivery and exemplifies all the benefits of the cloud by nature.

As more organizations have adopted DevOps, developer teams have begun to update their application development pipelines, security teams quickly realized their tools were not well-suited for the developer-driven, API-centric, infrastructure-agnostic patterns of cloud native security. As a result, cloud native security point products began to appear on the market. These products were each engineered to address one part of the problem or one segment of the software stack, but on their own they could not collect enough information to accurately understand or report on the risks across cloud native environments. This situation forced security teams to juggle multiple tools and vendors, which increased cost, complexity, and risk, in addition to creating blind spots where the tools overlapped but didn't integrate.

The solution to this problem requires a unified platform approach that can envelop the entire CI/CD lifecycle and integrate with the DevOps workflow. Just as cloud native approaches have fundamentally changed how cloud is used, CNSPs are fundamentally restructuring how the cloud is secured.

CNSPs share context about infrastructure, PaaS, users, development platforms, data, and application workloads across platform components to enhance security. They also:

- Provide unified visibility for SecOps and DevOps teams
- Deliver an integrated set of capabilities to respond to threats and protect cloud native applications
- Automate the remediation of vulnerabilities and misconfigurations consistently across the entire build-deploy-run lifecycle

In the past, organizations that wanted to embrace new compute options were stifled by the need to buy more security products to support those options. Stitching together disparate solutions in an attempt to enforce consistent policies across technology boundaries became more of a problem than a solution. CNSPs, however, provide coverage across the continuum of compute options, multicloud, and the application development lifecycle. This coverage allows organizations to choose the correct compute options for any given workload, thus granting them freedom without worry over how to integrate solutions for security. CNSPs epitomize the benefits of a cloud native strategy, enabling agility, flexibility, and digital transformation.

The Palo Alto Networks CNSP includes the following solutions to secure the cloud: Prisma Cloud, Prisma Access, and Prisma SaaS.

Prisma Cloud is the most comprehensive cloud native security platform, designed to protect all aspects of cloud use with the industry's leading technology. Prisma Cloud provides broad security and compliance coverage for the entire cloud native technology stack and applications and data throughout the entire application lifecycle, across multicloud and hybrid cloud environments. Prisma Cloud takes an integrated approach that enables SecOps and DevOps teams to accelerate cloud native application deployment by implementing security early in the development cycle.

Prisma Cloud comprises four pillars:

- **Visibility, governance, and compliance.** Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.
- **Compute security.** Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your *integrated development environment* (IDE), *software configuration management* (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.
- **Network protection.** Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.
- **Identity security.** Monitor and leverage *user and entity behavior analytics (UEBA)* across your environments to detect and block malicious actions. Gain visibility into and enforce governance policies on user activities, and manage the permissions of both users and workloads.

Key Terms

- An **integrated development environment (IDE)** is a software application that provides comprehensive tools such as a source code editor, build automation tools, and a debugger for application developers.
- **Software configuration management (SCM)** is the task of tracking and controlling changes in software.
- **User and entity behavior analytics (UEBA)** is a type of cybersecurity solution or feature that discovers threats by identifying activity that deviates from a baseline.

Cloud governance and compliance

Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

Despite the availability of numerous tools, most organizations struggle to effectively control their data exposure and enforce security policies across ever-changing cloud environments and SaaS applications. Furthermore, ensuring compliance where data is stored across distributed environments puts a significant burden on your already strained security teams.

Compute security

The cloud native landscape is constantly evolving with new technologies and levels of abstraction. Hosts, containers, and serverless workloads provide unique benefits and have different security requirements. Prisma Cloud provides best-in-class solutions for securing any type of cloud native workload throughout the development lifecycle.

Prisma Cloud provides cloud native computing security from build to run, including:

- **Vulnerability management.** Detect and prevent vulnerabilities and misconfigurations throughout the entire development process. Prioritize vulnerabilities based on your unique environment and prevent vulnerable code from ever reaching production.
- **Runtime security.** Prevent threats and anomalies across your hosts, containers, serverless functions, and orchestrators. Build automated, machine learning-driven models that define known good behaviors across process, network, file system, and system call sensors. Models are correlated to image IDs, so every time you build your app, you get a model uniquely calculated and customized for that specific build.
- **Application security.** Protect applications and APIs through a powerful combination of web traffic inspection and *runtime application self-protection* (RASP). Adopt an "explicit allow" model where only the specific activities and capabilities required by your application are allowed and everything else is treated as anomalous and is therefore prevented.
- **DevSecOps enabled.** Integrate security into your IDE, SCM, and CI workflows to detect and prevent issues as early as possible. Powerful plugins allow developers to inspect images, IaC templates, and functions and to see the vulnerability status every time developers run a build. Security teams can prevent compromised assets from ever progressing down the pipeline.

Key Idea

- Integrate security into your IDE, SCM, and CI workflows to detect and prevent issues as early as possible.

Key Terms

- **Runtime application self-protection (RASP)** detects attacks against an application in real time. RASP continuously monitors an app's behavior and the context of behavior to immediately identify and prevent malicious activity.

Network protection

Network protection must be adapted for cloud native environments while still enforcing consistent policies across hybrid environments. Prisma Cloud detects and prevents network anomalies by enforcing container-level micro-segmentation, inspecting traffic flow logs, and leveraging advanced Layer 7 threat protection.

Prisma Cloud network protection capabilities include:

- Network visibility and anomaly detection: Ingest network traffic flow logs from multiple sources and gain deep visibility into network behavior to detect and prevent anomalies.
- Identity-based micro-segmentation: Enforce cloud native micro-segmentation at the container and host levels with Layer 4 and Layer 7 distributed firewalls. Segment cloud networks and deploy policies based on logical workload and application identities, rather than dynamic IP addresses.
- Cloud native firewalling: Automatically model traffic flows between microservices and dynamically create filters that allow valid connections and drop suspicious ones. Protect networks with Layer 4 and Layer 7 security capabilities, such as DNS security and URL filtering.

Identity security

Management of a large number of privileged users with access to an ever-expanding set of sensitive resources can be challenging. Cloud resources themselves also have permission sets that must be managed. Prisma Cloud helps you leverage the identity of cloud resources to enforce security policies and ensure secure user behavior across your cloud environments.

Key capabilities include:

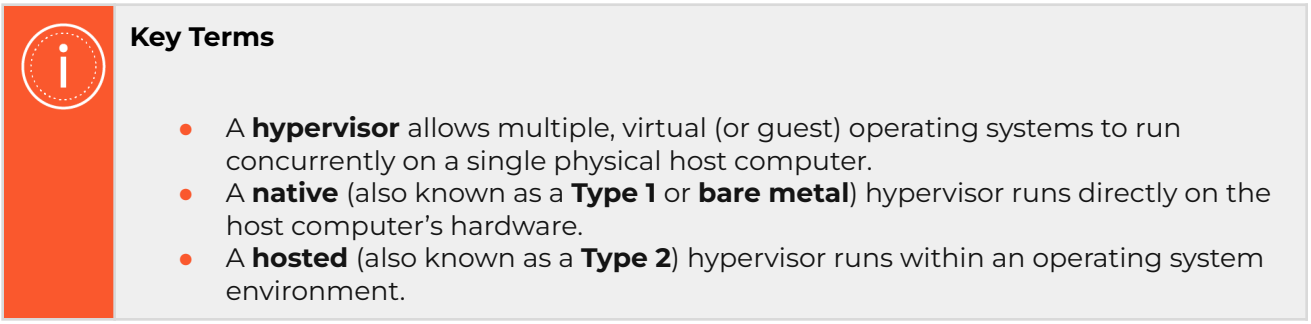
- Identity and Access Management (IAM) security: Secure and manage the relationships between users and cloud resources. Enforce governance policies to ensure that users and resources behave only as intended and do not introduce risk to the environment.
- Access management: Ensure least-privileged access to cloud resources and infrastructure and decouple user permissions from workload permissions.
- Machine identity: Decouple workload identity from IP addresses. Leverage tags and metadata to assign a logical identity to applications and workloads, then use it to enforce ID-based micro-segmentation and security policies that adapt to your dynamic environments.
- UEBA: Continuously analyze the behavior of users and resources in your cloud to detect and prevent anomalous behavior, such as an admin logging in from an unknown location or a container accessing a file it should not be able to access.

3.4 Describe the purpose of virtualization in cloud computing

3.4.1 Describe the types of hypervisors

A *hypervisor* allows multiple, virtual ("guest") operating systems to run concurrently on a single physical host computer. The hypervisor functions between the computer operating system and the hardware kernel. The two types of hypervisors are:

- **Type 1** (*native* or *bare metal*). Runs directly on the host computer's hardware
- **Type 2** (*hosted*). Runs within an operating system environment



Key Terms

- A **hypervisor** allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer.
- A **native** (also known as a **Type 1** or **bare metal**) hypervisor runs directly on the host computer's hardware.
- A **hosted** (also known as a **Type 2**) hypervisor runs within an operating system environment.

3.4.2 Describe characteristics of various cloud providers

As data center managers face a burgeoning population of mobile users, the distributed workforce – with multiple endpoints and cloud applications – is forcing organizations to evolve both their in-house and cloud cybersecurity infrastructures. The traditional approach of backhauling traffic to the corporate network or using multiple point products to extend security to remote networks and mobile users proves difficult to manage, costly, and prone to introducing inconsistencies in security policies and protections.

When hundreds or thousands of devices must be delivered, deployed and maintained across all remote locations, the result is too often a limited security solution with a heavy footprint and gaps in security that expose organizations to breaches and cyberattacks. The topic is further complicated by various environments in cloud computing and storage, including public, private, and hybrid cloud adoption scenarios, each of which pose unique opportunities, challenges, and risks.

3.4.3 Describe economic benefits of cloud computing and virtualization

Virtual systems provide the same basic functions as a physical firewall, along with additional benefits:

- **Segmented administration**—Different organizations (or customers or business units) can control (and monitor) a separate firewall instance so that they have control over their own traffic without interfering with the traffic or policies of another firewall instance on the same physical firewall.
- **Scalability**—After the physical firewall is configured, adding or removing customers or business units can be done efficiently. An ISP, managed security service provider, or enterprise can provide different security services to each customer.

- **Reduced capital and operational expenses**—Virtual systems eliminate the need to have multiple physical firewalls at one location because virtual systems co-exist on one firewall. By not having to purchase multiple firewalls, an organization can save on the hardware expense, electric bills, and rack space, and can reduce maintenance and management expenses.
- **Ability to share IP-address-to-username mappings**—By assigning a virtual system as a User-ID hub, you can share the IP-address-to-username mappings across virtual systems to leverage the full User-ID capacity of the firewall and reduce operational complexity.

3.4.4 Describe the security implications of virtualization

Virtualization is an important technology used in data centers and cloud computing to optimize resources. Important security considerations associated with virtualization include:

- **Dormant virtual machines (VMs):** In many data center and cloud environments, inactive VMs are routinely (often automatically) shut down when they are not in use. VMs that are shut down for extended periods (weeks or months) may be inadvertently missed when anti-malware updates and security patches are applied.
- **Hypervisor vulnerabilities:** In addition to vulnerabilities within the hosted applications, VMs, and other resources in a virtual environment, the hypervisor itself may be vulnerable, which can expose hosted resources to attack.
- **Intra-VM communications:** Network traffic between virtual hosts, particularly on a single physical server, may not traverse a physical switch. This lack of visibility increases troubleshooting complexity and can increase security risks because of inadequate monitoring and logging capabilities.
- **VM sprawl:** Virtual environments can grow quickly, thus resulting in a breakdown in change management processes and exacerbating security issues, such as dormant VMs, hypervisor vulnerabilities, and intra-VM communications.

3.4.5 Reference

- Cloud Security Service, Cloud Storage and Cloud Technology – Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/cloud-security-service-cloud-storage-and-cloud-technology

3.5 Explain the purpose of containers in application deployment

3.5.1 Differentiate containers versus virtual machines

Containers

Containers deliver all three cloud native system characteristics and provide a balanced set of capabilities and trade-offs across the continuum. Containers were popularized and are best known by the Docker project. They have existed in various forms for many years and have their roots in technologies such as Solaris Zones and BSD Jails. Although Docker is a well-known brand, other vendors are adopting Docker's underlying technologies of runc and containerd to create similar but separate solutions.

Containers balance separation (though not as well as VMs), excellent compatibility with existing apps, and a high degree of operational control with good density potential and easy integration into software development flows. Containers can be complex to operate, primarily due to their broad configurability and the wide variety of choices they present to operational teams. Depending on these choices, containers can be either completely stateless, dynamic, and isolated; highly intermingled with the host operating system and stateful; or anywhere in between. This degree of

choice is both the greatest strength and the great weakness of containers. In response, the market has created systems to their right on the continuum (as seen in the following figure), such as serverless, to both make them easier to manage at scale and abstract some of their complexity by reducing some configurability.

Virtual machines

Although a discussion of VMs in the context of cloud native may be surprising, the reality is that the vast majority of the world's workloads today run "directly" (non-containerized) in VMs. Most organizations do not see VMs as a legacy platform to eliminate, nor simply as a dumb host on which to run containers. Rather, they acknowledge that many of their apps have not yet been containerized and that the traditional VM still is a critical deployment model for them. Although a VM not hosting containers doesn't meet all three attributes of a cloud native system, it nevertheless can be operated dynamically and run microservices.

VMs provide the greatest levels of isolation, compatibility, and control in the continuum (see the following figure) and are suitable for running nearly any type of workload. Examples of VM technologies include VMware vSphere, Microsoft Hyper-V, and the instances provided by virtually every IaaS cloud provider, such as Amazon EC2. VMs are differentiated from "thin VMs" to their right on the continuum because they often are operated in a stateful manner with little separation between OS, app, and data.

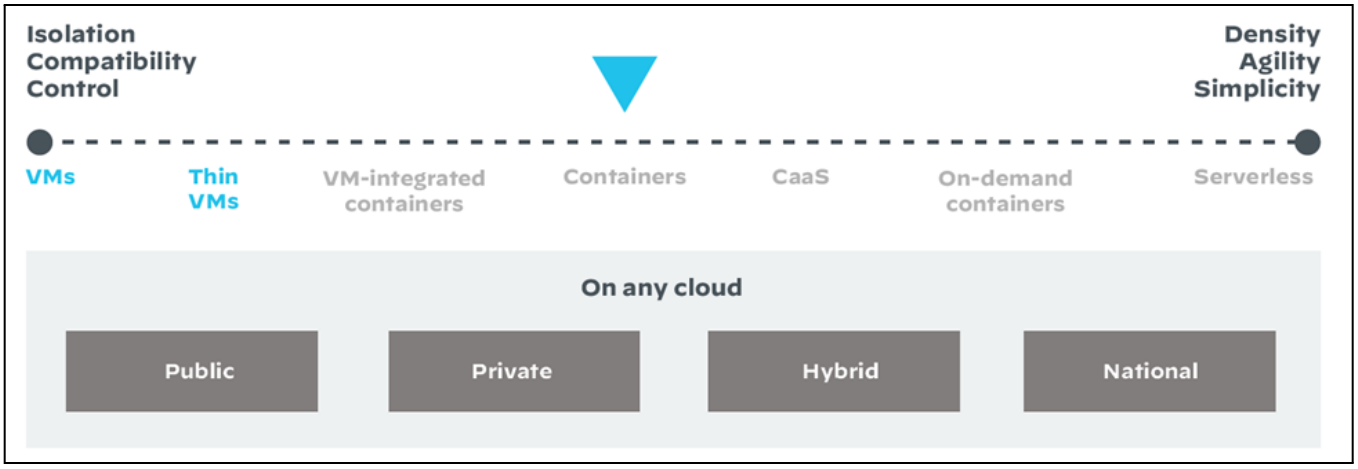


Figure: VMs and thin VMs on the continuum of cloud native technologies

Key Idea

- Virtual machines provide the greatest levels of isolation, compatibility and control in the continuum and are suitable for running nearly any type of workload.

3.5.2 Describe Container as a Service

Containers as a Service

As containers grew in popularity and used diversified orchestrators such as Kubernetes (and its derivatives, such as OpenShift), Mesos, and Docker Swarm, it became increasingly important to deploy and operate containers at scale. Although these orchestrators abstract much of the complexity required to deploy and operate large numbers of microservices composed of many containers and running across many hosts, they can be complex to set up and maintain. These orchestrators also are focused on the container runtime and do little to assist with the deployment and management of underlying hosts. Although sophisticated organizations often use technologies such as thin VMs wrapped in automation tooling to address the deployment and management of underlying hosts, even these approaches do not fully unburden the organization from managing the underlying compute, storage, and network hardware. Containers-as-a-service (CaaS) platforms provide all three cloud native characteristics by default and, although assembled from many more generic components, are highly optimized for container workloads.

Because major public cloud IaaS providers already have extensive investments in lower-level automation and deployment, many have chosen to leverage this advantage to build complete platforms for running containers that strive to eliminate management of the underlying hardware and VMs from users. These CaaS platforms include Google Kubernetes Engine, Azure Kubernetes Service, and Amazon EC2 Container Service. These solutions combine the container deployment and management capabilities of an orchestrator with their own platform-specific APIs to create and manage VMs. This integration allows users to more easily provision capacity without the need to manage the underlying hardware or virtualization layer. Some of these platforms, such as Google Kubernetes Engine, even use thin VMs running container-focused operating systems, such as Container-Optimized OS or CoreOS, to further reduce the need to manage the host operating system.

CaaS platforms are differentiated from containers on their left on the continuum (see Figure below) by providing a more comprehensive set of capabilities that abstract the complexities involved with hardware and VM provisioning. CaaS platforms are differentiated from the on-demand containers to their right on the continuum by typically still enabling users to directly manage the underlying VMs and host OS. For example, in most CaaS deployments, users can use SSH directly to a node and run arbitrary tools as a root user to aid in diagnostics or customize the host OS.

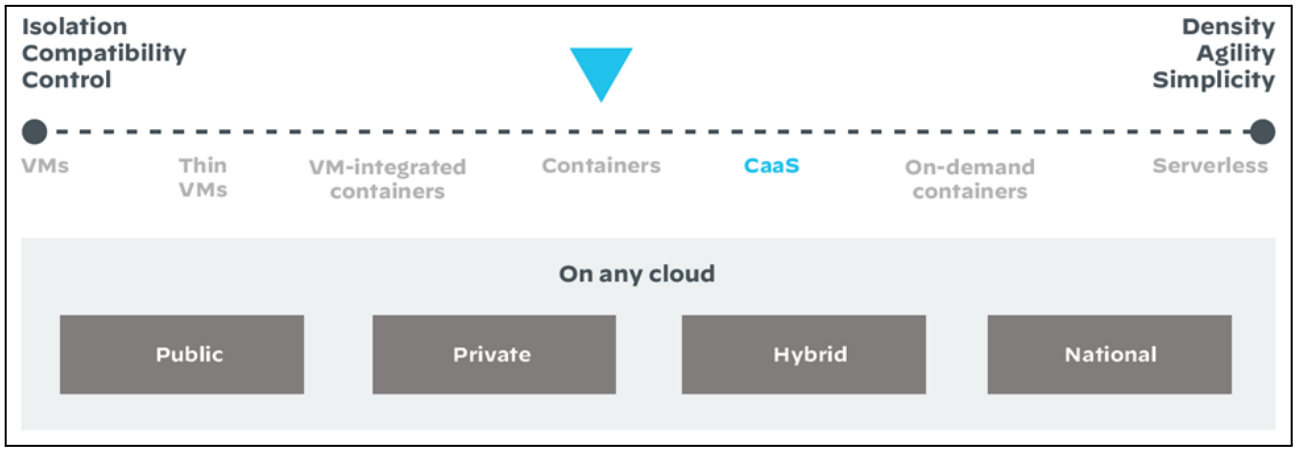


Figure: CaaS platform on the continuum of cloud native technologies

3.5.3 Differentiate a hypervisor from a Docker Container

Hypervisor
In the virtualized deployment, there is hardware, an operating system, a hypervisor that abstracts each virtual machine from the base OS, and (guest) virtual machines that have full operating systems installed in them with their respective libraries and applications.

Docker Container
Containers allow Dev teams to package apps and services in a standard and simple way. Containers can run anywhere and be moved easily. Docker containers are the most common.

Docker is a tool used by developers to package together dependencies into a single container (or image). What this means is that in order to use your integration, you are not required to "pip install" all of the packages required. They are part of a container that "docks" to the server and contains all the libraries you need. To learn more about docker, visit their site here.

Docker primarily runs python scripts and integrations in a controlled environment. Python scripts and integrations run isolated from the server to prevent someone from accidentally damaging the server. Packaging libraries and dependencies together prevents unknown issues from occurring because the environment is all the same.

3.5.4 Reference

- Docker.
  https://xsoar.pan.dev/docs/integrations/docker

3.6 Describe how serverless computing is used

Although on-demand containers greatly reduce the “surface area” exposed to end users, and thus, the complexity associated with managing them, some users prefer an even simpler way to deploy apps. Serverless is a class of technologies designed to allow developers to provide only their app code to a service, which then automatically instantiates the rest of the stack below it.

In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and then (if needed) instantiates the underlying host OS and VM and the hardware required to run them. In a serverless model, users make the most dramatic trade-offs of compatibility and control for the simplest, most efficient deployment and management experience.

Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

Serverless is differentiated from on-demand containers to the left side on the continuum by the complete inability to interact with the underlying host and container runtime, often to the extent of not even having visibility into the software it runs.

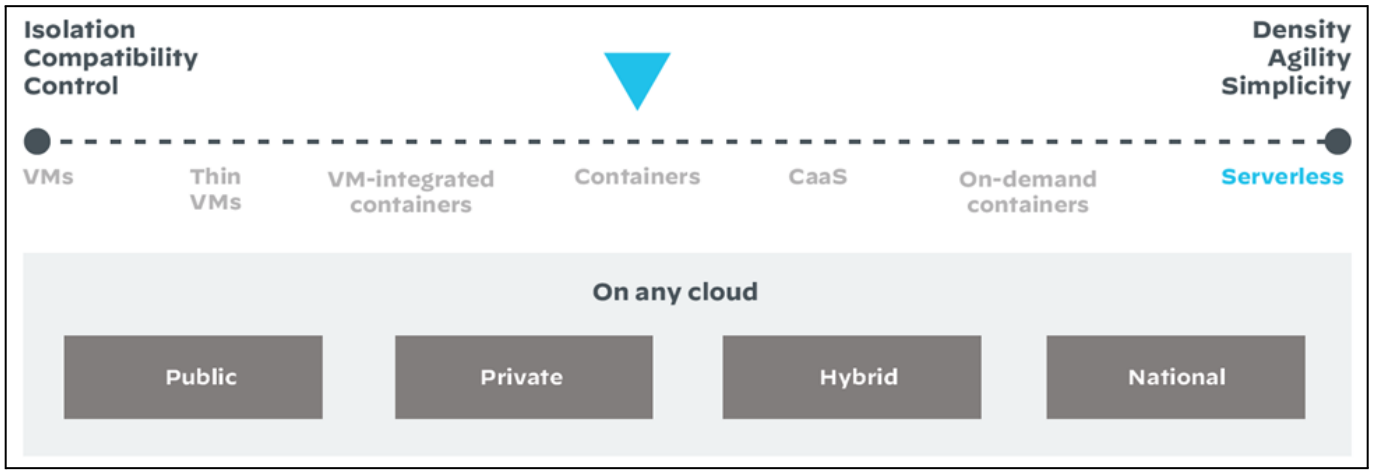


Figure: Serverless on the continuum of cloud native technologies

3.7 Describe DevOps

In a traditional software development model, developers write large amounts of code for new features, products, bug fixes, and such, and then pass their work to the Operations team for deployment, usually via an automated ticketing system. The Operations team receives this request in its queue, tests the code, and gets it ready for production. This process can take days, weeks, or months. Under this traditional model, if Operations runs into any problems during deployment, the team sends a ticket back to the developers to tell them what to fix. Eventually, after this back-and-forth interaction is resolved, the workload gets pushed into production.

This model makes software delivery a lengthy and fragmented process. Developers often see Operations as a roadblock, slowing down their project timelines, and Operations teams feel like a repository for development problems.

DevOps solves these problems by uniting Development and Operations teams throughout the entire software delivery process, enabling them to discover and remediate issues earlier, automate testing and deployment, and reduce time to market.
To better understand what DevOps is, let's first understand what DevOps is not.
DevOps is not:

- A combination of the Dev and Ops teams: There still are two teams, but they operate in a more communicative, collaborative way.
- Its own separate team: There is no such thing as a "DevOps engineer." Although some companies may appoint a "DevOps team" as a pilot when trying to transition to a DevOps culture, DevOps refers to a culture where developers, testers, and operations personnel cooperate throughout the entire software delivery lifecycle.
- A tool or set of tools: Although there are tools that work well with a DevOps model or help promote DevOps culture, DevOps ultimately is a strategy, not a tool.
- Automation: Although automation is very important for a DevOps culture, it alone does not define DevOps.

Now, let's discuss what DevOps is. Instead of developers coding huge feature sets before blindly handing them over to Operations for deployment., in a DevOps model, developers frequently deliver small amounts of code for continuous testing. Instead of communicating issues and requests through a ticketing system, the Development and Operations teams meet regularly, share analytics, and co-own projects from beginning to end.

Key Idea

- In the DevOps model, developers frequently deliver small amounts of code for continuous testing.

3.8 Describe DevSecOps

One problem in DevOps is that security often is neglected. Developers move quickly and their workflows are automated. Security is a separate team, and developers don't want to slow down for security checks and requests. As a result, many developers deploy without going through the proper security channels and inevitably make harmful security mistakes.

To solve the DevOps efficiency problem, organizations are adopting DevSecOps. DevSecOps takes the concept behind DevOps that developers and IT teams should work together closely, instead of separately, throughout software delivery and extends it to include security and integrate automated checks into the full CI/CD pipeline. The integration of the CI/CD pipeline takes care of the problem of security seeming like an outside force and instead allows developers to maintain their usual speed without compromising data security.

3.9 Illustrate the continuous integration/continuous delivery pipeline

CI/CD pipeline

DevOps is a cycle of continuous integration and continuous delivery (or continuous deployment), otherwise known as the CI/CD pipeline. The CI/CD pipeline integrates Development and Operations teams to improve productivity by automating infrastructure and workflows and continuously measuring application performance.

Continuous integration requires developers to integrate code into a repository several times per day for automated testing. Each check-in is verified by an automated build, thus allowing teams to detect problems early.

Continuous delivery means that the CI pipeline is automated, but the code must go through manual technical checks before it is implemented in production.

Continuous deployment takes continuous delivery one step further. Instead of manual checks, the code passes automated testing and is automatically deployed, thus giving customers instant access to new features.

3.10 Explain governance and compliance related to deployment of SaaS applications

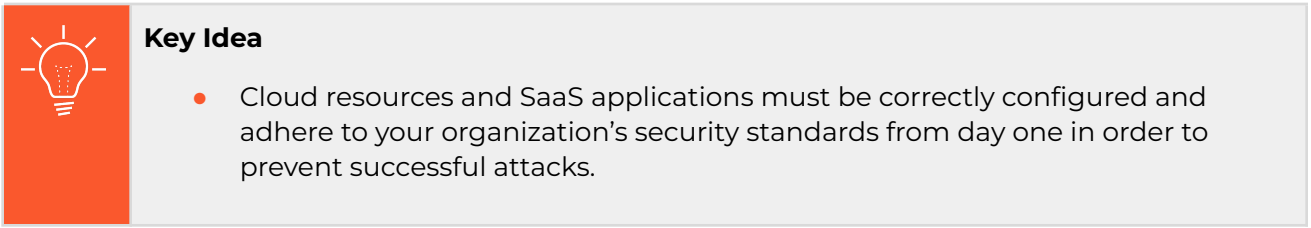
3.10.1 Describe security compliance to protect data

To prevent successful attacks, cloud resources and SaaS applications must be correctly configured and adhere to your organization's security standards from day one. Also, these applications, and the data they collect and store, must be properly protected and compliant to avoid costly fines, brand reputation damage, and loss of customer trust. Security teams must meet security standards and maintain compliant environments at scale and across SaaS applications.

Despite the availability of numerous tools, most organizations struggle to effectively control their data exposure and enforce security policies across ever-changing cloud environments and SaaS applications. Furthermore, ensuring compliance where data is stored across distributed environments puts a significant burden on constrained security teams.

Ensuring governance and compliance across multi-cloud environments and SaaS applications requires:

- Real-time discovery and classification of resources and data across dynamic SaaS and PaaS and IaaS environments
- Configuration governance, ensuring application and resource configurations match your security best practices as soon as they are deployed. This also prevents configuration drift
- Access governance using granular policy definitions to govern access to SaaS applications and resources in the public cloud and to apply network segmentation
- Compliance auditing by leveraging automation and built-in compliance frameworks to ensure compliance at any time and generate audit-ready reports on demand
- Seamless user experience that doesn't force additional steps or introduce significant latency in the use of applications as you add new security tools



Key Idea

- Cloud resources and SaaS applications must be correctly configured and adhere to your organization's security standards from day one in order to prevent successful attacks.

3.10.2 Describe privacy regulations globally

ATTRIBUTE	DESCRIPTION
Data Ownership	Based on the SaaS app's terms and conditions, one of the following values displays: • Customer Ownership–Your organization has full rights over the data when using the service. For example, the terms and conditions might state, "as between the parties, user owns all intellectual property rights in user data and user applications." • Vendor Ownership—Your organization grants the service access to use the data. For example, the terms and conditions might state, "You acknowledge and agree that any questions, comments, suggestions, ideas, feedback, or other information regarding the Site ("Submissions") provided by you to us are non-confidential and shall become our sole property" • Unknown—Attribute for the SaaS app is under research.
IP Based Restriction	IP-based restriction is the ability to restrict login access to the SaaS application for specific IP addresses. Based on the SaaS application's capabilities, one of the following values displays: • ✔—SaaS application offers the ability to configure IP based restriction. • No—SaaS application does not offer IP based restriction. • Unknown—Attribute for the SaaS app is under research.
MFA	Multi-factor Authentication (MFA) offers an additional layer of security for login access. Based on the SaaS application's capabilities, one of the following values displays: • ✔—SaaS application offers the ability to enable MFA. • No—SaaS application does not offer MFA. • Unknown—Attribute for the SaaS app is under research.
SAML	Security Assertion Markup Language (SAML) is an additional security control that enables users to authenticate to the SaaS application using Single sign-on (SSO) or company credentials. Based on the SaaS application's capabilities, one of the following values displays: • ✔—SaaS application offers the ability to enable SAML. • No—SaaS application does not offer SAML. • Unknown—Attribute for the SaaS app is under research.

3.10.3 Describe security compliance between local policies and SaaS Applications

Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

Despite the availability of numerous tools, most organizations struggle to effectively control their data exposure and enforce security policies across ever-changing cloud environments and SaaS applications. Furthermore, ensuring compliance where data is stored across distributed environments puts a significant burden on your already strained security teams.

Ensuring governance and compliance across multicloud environments and SaaS applications requires:

- **Real-time discovery and classification** of resources and data across dynamic SaaS, PaaS, and IaaS environments
- **Configuration governance**, ensuring that application and resource configurations match your security best practices as soon as they are deployed and also preventing configuration drift
- **Access governance**, by using granular policy definitions to govern access to SaaS applications and resources in the public cloud and to apply network segmentation
- **Compliance auditing** that leverages automation and built-in compliance frameworks to ensure compliance at any time and generate audit-ready reports on demand
- **Seamless user experience** that doesn't force additional steps or introduce significant latency in the use of applications as you add new security tools

3.11 Describe the cost of maintaining a physical data center

Data center architectures and requirements can differ significantly. For example, a data center built for a cloud service provider like Amazon satisfies facility, infrastructure, and security requirements that significantly differ from a completely private data center, such as one built for a government facility that is dedicated to securing classified data.

Regardless of classification, an effective data center operation is achieved through a balanced investment in the facility and the equipment it houses. In addition, since data centers often house an organization's business-critical data and applications, it's essential that both facility and equipment are secured against intruders and cyberattacks.

The primary elements of a data center break down as follows:

- Facility – the usable space available for IT equipment. Providing round-the-clock access to information makes data centers some of the world's most energy-consuming facilities. There should be an emphasis on designs that optimize space and environmental control to keep equipment within specific temperature/humidity ranges.
- Core components – equipment and software for IT operations and storage of data and applications. These may include storage systems; servers; network infrastructure, such as switches and routers; and various information security elements, such as firewalls.

- Support infrastructure – equipment contributing to securely sustaining the highest availability possible. The Uptime Institute has defined four tiers of data centers, with availability ranging from 99.671% to 99.995%. Some components for supporting infrastructure include:
- Uninterruptible Power Sources (UPS) – battery banks, generators, and redundant power sources.
- Environmental control – computer room air conditioners (CRAC); heating, ventilation and air conditioning (HVAC) systems; and exhaust systems.
- Physical security systems – biometrics and video surveillance systems.
- Operations staff – personnel available to monitor operations and maintain IT and infrastructure equipment around the clock.

3.11.1 References

- What is a Data Center? https://www.paloaltonetworks.com/cyberpedia/what-is-a-data-center

3.12 Differentiate between data-center security weaknesses of traditional solutions versus cloud environments

Traditional data center security solutions exhibit the same weaknesses found when they are deployed at a perimeter gateway on the physical network: They make their initial positive control network access decisions based on port, using stateful inspection, and then they make a series of sequential, negative control decisions using installed feature sets. This approach has several problems:

- **Limited visibility and control:** The "ports first" focus of traditional data security solutions limits the ability to see all traffic on all ports, which means that evasive or encrypted applications, and any corresponding threats that may or may not use standard ports, can evade detection. For example, many data center applications (such as Microsoft Lync, Active Directory, and SharePoint) use a wide range of contiguous ports to function properly. You therefore must open all those ports first, which then exposes those same ports to other applications or cyberthreats.

- **No concept of unknown traffic:** Unknown traffic is high risk but represents only a relatively small amount of traffic on every network. Unknown traffic can be a custom application, an unidentified commercial off-the-shelf application, or a threat. The common practice of blocking all unknown traffic may cripple your business. Allowing all traffic is highly risky. You need to be able to systematically manage unknown traffic using native policy management tools to reduce your organizational security risks.

- **Multiple policies, no policy reconciliation tools:** Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying the traffic. This situation is made worse when there are no policy reconciliation tools.

- **Cumbersome security policy update process.** Existing security solutions in the data center do not address the dynamic nature of your cloud environment, because your policies have difficulty contending with the numerous dynamic changes that are common in virtual data centers. In a virtual data center, VM application servers often move from one physical host to another, so your security policies must adapt to changing network conditions.

Many cloud security offerings are merely virtualized versions of port and protocol based security appliances with the same inadequacies as their physical counterparts.

3.13 Differentiate between east-west and north-south traffic patterns

In a virtual data center (private cloud), there are two different types of traffic, each of which is secured in a different manner (see Figure below):

- **North-south** refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center.
- **East-west** refers to data packets moving between virtual workloads entirely within the private cloud.

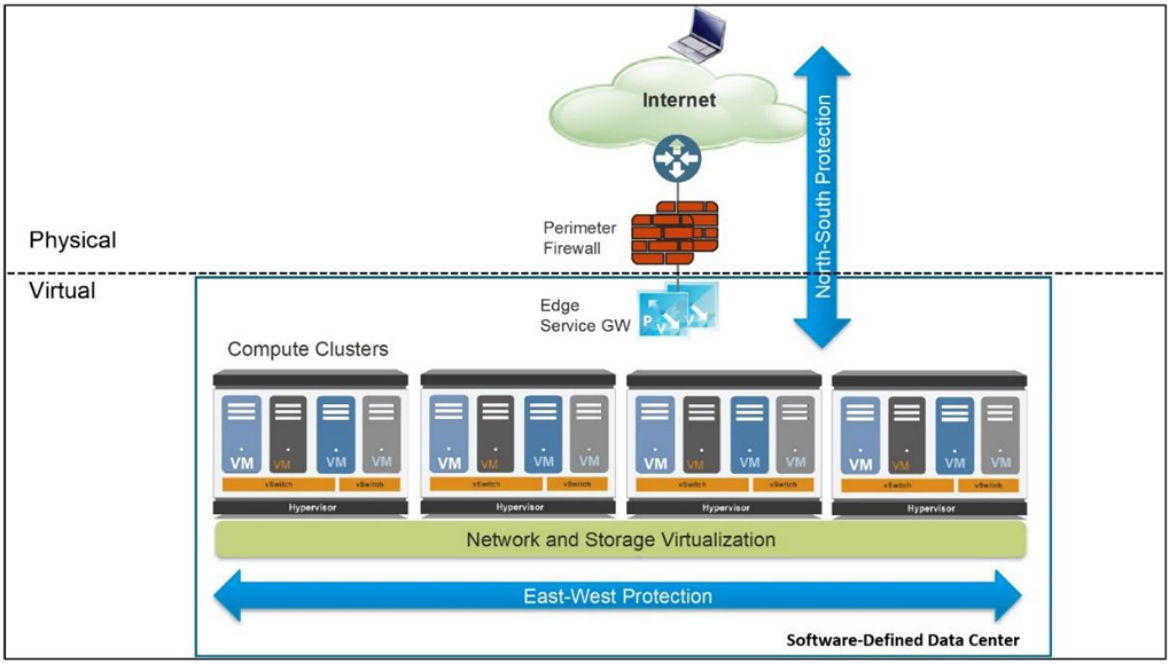


Figure: Typical virtual data center design architecture

The compute cluster is the building block for hosting the application infrastructure and provides the necessary resources in terms of compute, storage, networking, and security. Compute clusters can be interconnected using OSI model Layer 2 (Data Link) or Layer 3 (Network) technologies, such as virtual LAN (VLAN), virtual extensible LAN (VXLAN), or Internet Protocol (IP), thus providing a domain extension for workload capacity. Innovations in the virtualization space allow VMs to move freely in this private cloud while preserving compute, storage, networking, and security characteristics and postures.

Organizations usually implement security to protect traffic flowing north-south, but this approach is insufficient for protecting east-west traffic within a private cloud. To improve their security posture, enterprises must protect against threats across the entire network, both north-south and east-west.

One common practice in a private cloud is to isolate VMs into different tiers. Isolation provides clear delineation of application functions and allows a security team to easily implement security policies. Isolation is achieved using logical network attributes (such as a VLAN or a VXLAN) or logical software constructs (such as security groups). The figure here displays a simple three-tier application composed of a WEB-VM as the frontend, an APP-VM as the application, and a DB-VM providing database services.

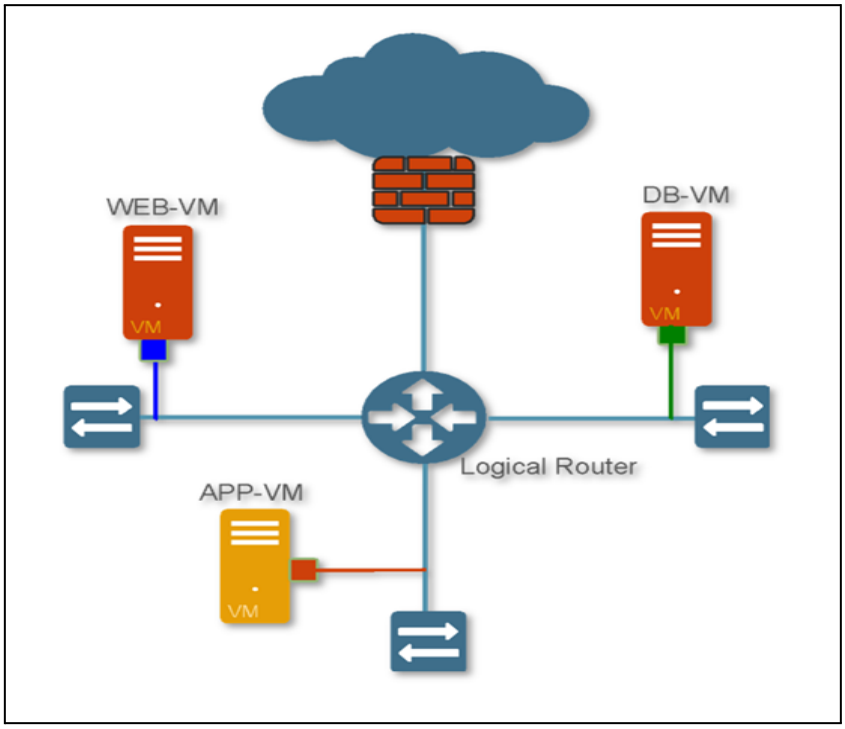


Figure: Three-tier application hosted in a virtual data center

An attacker has multiple options to steal data from the DB-VM. The first option is to initiate an SQL injection attack by sending HTTP requests containing normalized SQL commands that target an application vulnerability. The second option is to compromise the WEB-VM (using vulnerability exploits) and then move laterally to the APP-VM, initiating a brute-force attack to retrieve the SQL admin password.

After the DB-VM is compromised, the attacker can hide sensitive data extraction by using techniques such as DNS tunneling or by moving data across the network with NetBIOS and then off the network via FTP. In fact, attackers using applications commonly found on nearly every network have virtually unlimited options for stealing critical data in this environment. Infiltration into the environment and exfiltration of critical data can be completely transparent and undetected because the data is carried over the same legitimate protocols (such as HTTP and DNS) used for normal business activities.

Virtual data center security best practices dictate a combination of north-south and east-west protection. East-west protection provides the following benefits:

- Authorizes only allowed applications to flow inside the data center, between VMs
- Reduces lateral threat movement when a front-end workload has been compromised (the attacker breaches the front-end server by using a misconfigured application or unpatched exploit)
- Stops known and unknown threats that are sourced internally within the data center
- Protects against data theft by leveraging data and file filtering capability and blocking anti-spyware communications to the external world

An added benefit of using virtual firewalls for east-west protection is the unprecedented traffic and threat visibility that the virtualized security device can now provide. After traffic logs and threat logs are turned on, VM-to-VM communications and malicious attacks become visible. This virtual data center awareness allows security teams to optimize policies and enforce cyberthreat protection (for example, IPS, anti-malware, file blocking, data filtering, and DoS protection) where needed.

3.14 Describe the four phases of hybrid data-center security

The following approach to security in the evolving data center from traditional three-tier architectures to virtual data centers and to the cloud aligns with practical realities, such as the need to leverage existing best practices and technology investments and the likelihood that most organizations will transform their data centers incrementally.

This approach consists of four phases:

- **Consolidating servers within trust levels:** Organizations often consolidate servers within the same trust level into a single virtual computing environment, composed of either one physical host or a cluster of physical hosts. Intra-host communications generally are minimal and inconsequential. Most traffic routinely is directed “off box” to users and systems residing at different trust levels. When intra-host communications do happen, the absence of protective safeguards between these virtualized systems also is consistent with the organization’s security posture for non-virtualized systems. Live migration features typically are used to enable transfer of VMs only to hosts supporting workloads within the same subnet. Security solutions should incorporate a robust virtual systems capability in which a single instance of the associated countermeasures can be partitioned into multiple logical instances, each with its own policy, management, and event domains. This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus.

- **Consolidating servers across trust levels:** Workloads with different trust levels often coexist on the same physical host or cluster of physical hosts. Intra-host communications are limited, and live migration features are used to enable transfer of VMs only to hosts that are on the same subnet and that are configured identically with regard to routing of VM-to-VM traffic. Intra-host communication paths intentionally are not configured between VMs with different trust levels. Instead, all traffic is forced off box through a default gateway, such as a physical network security appliance, before it is allowed to proceed to the destination VM. This off-box routing typically can be accomplished by configuring separate virtual switches with separate physical network interface cards (NICs) for the VMs at each distinct trust level. As a best practice for virtualization, you should minimize the combination of workloads with different

trust levels on the same server. Live migrations of VMs also should be restricted to servers supporting workloads within the same trust levels and within the same subnet. Over time, and in particular as workloads move to the cloud, maintenance of segmentation based on trust levels becomes more challenging.

- **Selective network security virtualization:** Intra-host communications and live migrations are architected at this phase. All intra-host communication paths are strictly controlled to ensure that traffic between VMs at different trust levels is intermediated either by an on-box, virtual security appliance or by an off-box, physical security appliance. Long-distance live migrations (for example, between data centers) are enabled by a combination of native live migration features with external solutions that address associated networking and performance challenges. The intense processing requirements of solutions such as next-generation firewall virtual appliances will ensure that purpose-built physical appliances continue to play an important role in the virtual data center. However, virtual instances are ideally suited for scenarios where countermeasures need to migrate along with the workloads they control and protect.

- **Dynamic computing fabric:** Conventional, static computing environments are transformed into dynamic fabrics (private or hybrid clouds) where underlying resources such as network devices, storage, and servers can be fluidly engaged in whatever combination best meets the needs of the organization at any given point in time. Intra-host communication and live migrations are unrestricted. This phase requires networking and security solutions that not only can be virtualized but also are virtualization-aware and can dynamically adjust as necessary to address communication and protection requirements, respectively. Classification, inspection, and control mechanisms in virtualization-aware security solutions must not be dependent on physical and fixed Network layer attributes. In general, higher-layer attributes such as application, user, and content identification are the basis not only for how countermeasures deliver protection but also for how they dynamically adjust to account for whatever combination of workloads and computing resources exist in their sphere of influence. Associated security management applications also need to be capable of orchestrating the activities of physical and virtual instances of countermeasures, first with each other, and then with other infrastructure components. This capability is necessary to ensure that adequate protection is delivered optimally in situations where workloads are frequently migrating across data center hosts.

3.15 Describe how data centers can transform their operations incrementally

Organizations recognize the imperative to rapidly change their datacenter operations and technologies, centering approaches that don't impede the necessary transformations but can still protect an organization's most critical assets effectively. In order to maintain compliance and operational efficiency, security must scale and adapt at the same pace as the rest of the digital transformation journey. New application architectures and core technologies, such as containers and software-defined networks, strain traditional security techniques. As a result, embracing new forms of infrastructure is a key part of digitization as enterprises look to cloud providers for scale outside of their existing footprints in order to build hybrid environments. Datacenter networks and the security capabilities that the networks can wield need to provide the ability to enable those cloudy extensions in ways that allow organizations to grow efficiently while maintaining effective security controls. Key architectural decisions can be made today to pave the way for the future.
For more information refer to:
https://www.paloaltonetworks.com/resources/research/security-in-datacenter-transformation

3.16 Describe the cloud-native security platform

Application development methodologies are moving away from the traditional "waterfall" model and toward more agile continuous integration/continuous delivery (CI/CD) processes with end-to-end automation. This new approach brings a multitude of benefits, such as shorter time to market and faster delivery, but also introduces security challenges because traditional security methodologies weren't designed to address these modern application workflows. As developer teams embrace cloud native technologies, security teams find themselves scrambling to keep pace. Limited prevention controls, poor visibility, and tools that lack automation yield incomplete security analytics; all of these things increase the risk of compromise and the likelihood of successful breaches in cloud environments. Meanwhile, the demand for an entirely new approach to security emerges: cloud Native Security Platforms (CNSPs).

The term "cloud native" refers to an approach to building and running applications that take full advantage of a cloud computing delivery model instead of an on-premises data center. This approach combines the best of what cloud offers (scalability, deployability, manageability, and limitless on-demand compute power) and applies these principles to software development, combined with CI/CD automation, to radically increase productivity, business agility, and cost savings.

Cloud native architectures consist of cloud services such as containers, serverless security, platform as a service (PaaS), and microservices. These services are loosely coupled, meaning they are not hardwired to any infrastructure components, which allows developers to make changes frequently all across technology boundaries such as public, private, and multicloud deployments without affecting other pieces of the application or other team members' projects.

"Cloud native" refers to a methodology of software development essentially designed for cloud delivery, one that exemplifies all the benefits of the cloud by nature.

As more organizations have adopted DevOps and developer teams have begun to update their application development pipelines, security teams quickly realized their tools did not suffice for the developer-driven, API-centric, infrastructure-agnostic patterns of cloud native security. As a result, cloud native security point products began to appear on the market. These products were each engineered to address one part of the problem or one segment of the software stack, but on their own could not collect enough information to accurately understand or report on the risks across cloud native environments. This situation forced security teams to juggle multiple tools and vendors, which increased cost, complexity, and risk in addition to creating blind spots where the tools overlapped but didn't integrate.

Key Idea

- "Cloud native" refers to a methodology of software development that essentially is designed for cloud delivery and by nature exemplifies all the benefits of the cloud.

The solution to this problem requires a unified platform approach that can envelop the entire CI/CD lifecycle and integrate with the DevOps workflow. Just as cloud native approaches have fundamentally changed how organizations utilize the cloud, CNSPs are fundamentally restructuring how to secure the cloud.

CNSPs share context about infrastructure, PaaS, users, development platforms, data, and application workloads across platform components to enhance security. CNSPs also:

- Provide unified visibility for SecOps and DevOps teams
- Deliver an integrated set of capabilities to respond to threats and protect cloud native applications
- Automate the remediation of vulnerabilities and misconfigurations consistently across the entire build-deploy-run lifecycle

In the past, organizations that wanted to embrace new compute options were stifled by the need to buy more security products to support those options. Stitching together disparate solutions in an attempt to enforce consistent policies across technology boundaries became more of a problem than a solution. However, CNSPs offer coverage across the application development lifecycle, multicloud, and the continuum of compute alternatives. This coverage allows organizations to choose the correct compute options for any given workload, thus granting them freedom without worry over how to integrate solutions for security. CNSPs epitomize the benefits of a cloud native strategy by enabling agility, flexibility, and digital transformation.

The Palo Alto Networks CNSP includes the following solutions to secure the cloud: Prisma Cloud, Prisma Access, and Prisma SaaS.

Prisma Cloud is the most comprehensive cloud native security platform, designed to protect all aspects of cloud use with the industry's leading technology. Prisma Cloud provides broad security and compliance coverage for the entire cloud native technology stack as well as applications and data throughout the entire application lifecycle across multicloud and hybrid cloud environments. Prisma Cloud takes an integrated approach that enables SecOps and DevOps teams to accelerate cloud native application deployment by implementing security early in the development cycle.

3.17 Identify the four pillars of Prisma Cloud application security

Prisma Cloud comprises four pillars:

- **Visibility, governance, and compliance.** Gain deep visibility into the security posture of multicloud environments. Track all deployments with an automated asset inventory and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.
- **Compute security.** Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your *integrated development environment* (IDE), *software configuration management* (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.
- **Network protection.** Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.
- **Identity security.** Monitor and leverage *user and entity behavior analytics (UEBA)* across your environments to detect and block malicious actions. Gain visibility into and enforce governance policies on user activities and manage the permissions of both users and workloads.

Key Terms

- An **integrated development environment (IDE)** is a software application that provides comprehensive tools such as a source code editor, build automation tools, and a debugger for application developers.
- **Software configuration management (SCM)** is the task of tracking and controlling changes in software.

3.18 Describe the concept of SASE

With increasing numbers of mobile users, branch offices, data, and services located outside the protections of traditional network security appliances, organizations are struggling to keep pace and ensure the security, privacy, and integrity of their networks and their customers' data.

Many of the technologies on the market are built on architectures not designed to handle all types of traffic and security threats. This forces organizations to adopt multiple point products to handle different requirements, such as secure web gateways, firewalls, secure VPN remote access, and SD-WAN. For every product there is an architecture to deploy, a set of policies to configure, and an interface to manage, each with its own set of logs. This situation creates an administrative burden that introduces cost, complexity, and gaps in security posture.

To address these challenges, Secure Access Service Edge (SASE) has emerged. By design, SASE (pronounced "sassy") helps organizations adopt cloud and mobility by providing network and network security services from a common cloud-delivered architecture. A SASE solution must provide consistent security services and access to all types of cloud applications (public cloud, private cloud, and SaaS) delivered through a common framework. Organizations can remove multiple point products and adopt a single cloud-delivered SASE solution to reduce complexity while saving significant technical, human, and financial resources.

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following:

- **Networking**
  - Software-defined wide-area networks (SD-WANs)
  - Virtual private networks (VPNs)
  - Zero Trust network access (ZTNA)
  - Quality of Service (QoS)
- **Security**
  - Firewall as a service (FWaaS)
  - Domain Name System (DNS) security
  - Threat prevention
  - Secure web gateway (SWG)
  - Data loss prevention (DLP)
  - Cloud access security broker (CASB)

Key Terms

- A **secure web gateway (SWG)** is a security platform or service designed to maintain visibility in web traffic. Additional functionality may include web content filtering.
- A **cloud access security broker (CASB)** software monitors activity and enforces security policies on traffic between an organization's users and cloud-based applications and services.

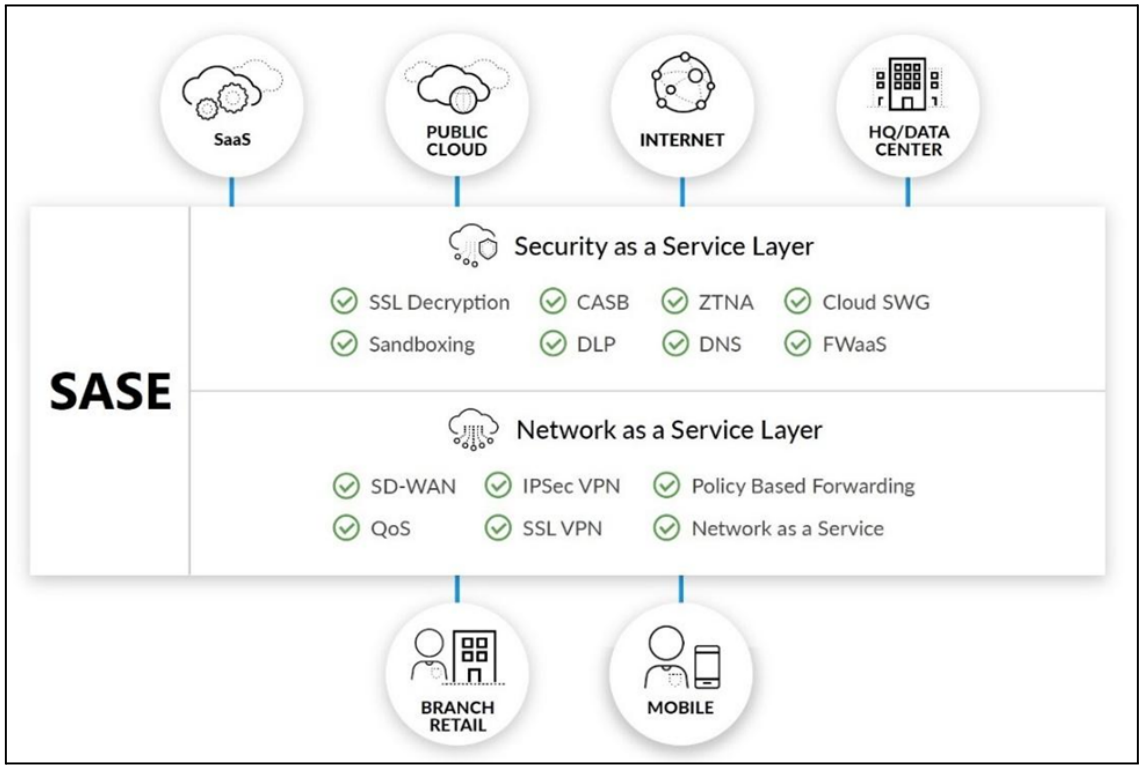


Figure: SASE: advanced network and security capabilities in a converged, cloud-delivered solution

Prisma Access delivers globally distributed networking and security to all your users and applications. Whether your users work at branch offices or home offices, they connect to Prisma Access to safely access cloud and data center applications and the internet.

Prisma Access consistently protects all traffic, on all ports and from all applications, thus enabling your organization to:

- **Prevent successful cyberattacks** with proven security philosophies and threat intelligence for deep visibility and precise control that extends across your organization
- **Fully inspect all application traffic** bidirectionally, including SSL/TLS-encrypted traffic, on all ports, whether communicating with the internet, with the cloud, or between branches
- **Benefit from comprehensive threat intelligence** powered by automated threat data from Palo Alto Networks and hundreds of third-party feeds

3.19 Describe the SASE layer

The Prisma Access SASE architecture consists of a network-as-a-service layer, a security-as-a-service layer, and a common management platform to secure branch/retail and mobile users across SaaS, public cloud, internet, and headquarters/data center environments (see Figure 3-13).

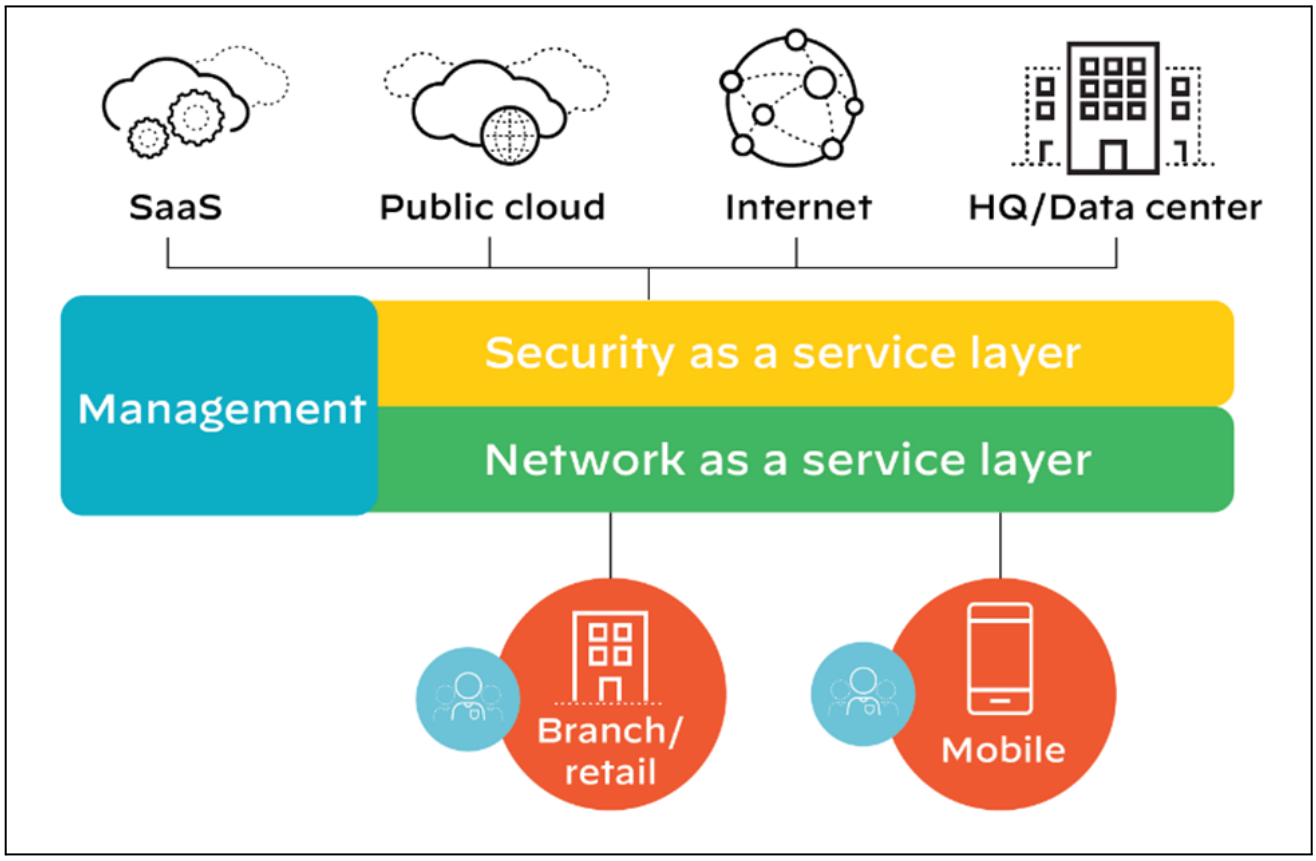


Figure: The Prisma Access architecture

Network-as-a-service layer

The network-as-a-service layer in Prisma Access delivers important SASE capabilities, including:

- Software-defined wide-area network (SD-WAN)
- Virtual private network (VPN)
- Zero Trust network access (ZTNA)
- Quality of service (QoS)

SD-WAN

Companies are adopting software-defined wide-area networks (SD-WAN) to connect branch offices to the corporate network and provide local internet breakout as an alternative to costly multiprotocol label switching (MPLS) connections. The challenge with SD-WAN, however, is how to combine security with the SD-WAN fabric, which leads to the need for multiple overlays.

In a SASE solution, SD-WAN edge devices can connect to a cloud-based infrastructure rather than to physical SD-WAN hubs located in data center or colocation facilities. This approach enables the interconnectivity between branch offices without the complexity of deploying and managing physical SD-WAN hubs.

You already should consider or have adopted SD-WAN into your organization's network infrastructure as a way to securely connect and control access to branch offices and remote employees. SASE creates a unified framework for SD-WAN services and other solutions to connect to, thus providing a single point of view and simplified management solution to protect your network.

Prisma Access connects branch offices over a standard IPsec VPN tunnel using common IPsec-compatible devices, such as your existing branch router, SD-WAN edge device, or a third-party firewall. It uses Border Gateway Protocol (BGP) or static routes for routing from the branch and equal-cost multi-path (ECMP) routing for faster performance and better redundancy across multiple links.

Virtual private network

Organizations rely on virtual private networks (VPNs) to provide a secure encrypted connection for mobile users and branch offices to access corporate data, applications, and internet access. There are many types of VPN services from IPsec VPN to SSL VPN, clientless VPN, and remote access VPN, all of which require a connection to a VPN gateway. VPNs are not optimized for access to the cloud, which results in no security or access control when users disconnect to reach cloud apps or services.

A SASE solution encompasses VPN services and enhances the capabilities to operate in a cloud-based infrastructure to securely route traffic to the public cloud, SaaS, internet, or private-cloud apps. In an IPsec VPN example, you can create a site-to-site connection to a cloud-based infrastructure from any IPsec-compatible device located at a branch or retail location via a branch router, wireless access point, SD-WAN edge device, or firewall. Mobile users employ an always-on IPsec or SSL VPN connection between their endpoint or mobile device, and a SASE solution ensures consistent traffic encryption and threat prevention.

Regardless of which type of VPN service you use in your organization, a SASE solution provides a unified cloud infrastructure to connect to, instead of requiring you to backhaul to a VPN gateway at corporate headquarters. This solution dramatically simplifies the management and policy control needed to enforce least-privileged access rules.

Prisma Access (formerly GlobalProtect cloud service) provides cloud-delivered security infrastructure that enables your organization to connect users to a nearby cloud gateway, enable secure access to all applications, and maintain full visibility and inspection of traffic across all ports and protocols.

For managed mobile devices:

- Users with managed devices have the GlobalProtect app installed on their laptop, mobile phone, or tablet. The GlobalProtect app connects to Prisma Access automatically whenever internet access is available, without requiring any user interaction.
- Users can access all of their applications, whether in the cloud or the data center. The connectivity layer connects applications in different locations, thus enabling secure access (based on App-ID and User-ID policies) to public cloud, SaaS, and data center applications.
- Prisma Access delivers protection through the security service layer, such as protections against known and unknown malware, exploits, C2 traffic, and credential-based attacks.

For unmanaged/BYOD devices:

- Your organization can deploy Prisma Access in conjunction with mobile device management (MDM) integration to support bring-your-own-device (BYOD) policies. The integration enables capabilities such as per-app VPN.
- Users such as contractors and employees with BYOD devices with unmanaged devices can access applications without an app installed by using Prisma Access with Clientless VPN.
- Clientless VPN also enables secure access to SaaS applications from unmanaged devices with inline protections by using Security Assertion Markup Language (SAML) proxy integration. This functionality works in conjunction with Prisma SaaS.

Zero Trust network access

Zero Trust network access (ZTNA) is an important part of the Zero Trust philosophy of "never trust, always verify," developed by Forrester to identify the need to protect data. ZTNA requires users who want to connect to the cloud to authenticate through a gateway before gaining access to the applications they need. This requirement provides an IT admin the ability to identify users and create policies to restrict access, minimize data loss, and quickly mitigate any issues or threats that may arise.

Many ZTNA products are based on software-defined perimeter (SDP) architectures, which do not provide content inspection, thus creating a discrepancy in the types of protection available for each application. For consistent protection, the organization must build additional controls on top of the ZTNA model and establish inspection for all traffic across all applications.

SASE builds on the ZTNA key principles and applies them across all the other services within a SASE solution. SASE identifies users, devices, and applications, regardless of where they connect from, thus simplifying policy creation and management. SASE removes the complexity of connecting to a gateway by incorporating the networking services into a single unified cloud infrastructure.

Key Idea

- Zero Trust Network Access (ZTNA) is an important part of the Zero Trust philosophy of "never trust, always verify" developed by Forrester.

A SASE solution should incorporate ZTNA concepts for protecting applications and apply other security services to consistently enforce DLP and threat prevention policies. Access controls establish who a person is, but other security controls are also necessary to make sure that the person's behaviors and actions are not harmful to the organization. The same controls need to be applied across access to all applications.

Quality of Service

Organizations that transition from MPLS to SD-WAN using broadband services are finding that the service quality varies. Quality of Service (QoS) establishes bandwidth allocation assigned to particular apps and services. Businesses rely on QoS to ensure that their critical apps and services perform adequately (for example, medical equipment or credit card processing services). If these systems were to slow down due to lack of bandwidth, business operations and sales would be severely impacted. QoS prioritizes business-critical apps, based on a ranking system, so you can choose which apps and services take precedence over others.

QoS is an important step when you begin migrating from MPLS. A SASE solution incorporates QoS services in the cloud, thus allowing you to easily mark sensitive applications (such as VoIP) as higher priority than general internet browsing and entertainment apps.

QoS is immensely important for businesses of any size. Management of QoS traffic and allocation doesn't need to be difficult. SASE enables you to dynamically shape traffic based on the policies that prioritize critical application requirements. Make sure that your SASE solution contains QoS capabilities.

Security-as-a-service layer

The security-as-a-service layer in Prisma Access delivers important SASE capabilities, including:

- DNS security
- Firewall as a service (FWaaS)
- Threat prevention
- Secure web gateway (SWG)
- Data loss prevention (DLP)
- Cloud access security broker (CASB)

DNS security

Every organization uses DNS to translate a domain name into an IP address. DNS is an open service, and by default it cannot detect DNS-based threats. As a result, malicious activity within DNS can be used to propagate an attack.

DNS security protects your users by predicting and blocking malicious domains while neutralizing threats. A SASE solution adopts DNS security features by providing consistent security across the network and users, regardless of their location.

Your SASE solution should contain DNS protections delivered within the cloud environment as part of the network access. DNS security should be built into the solution that your branch offices and mobile users use to connect to the internet. The DNS security provided in your SASE solution should leverage a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic.

Prisma Access delivers the Palo Alto Networks DNS Security service, which provides a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic. Organizations can block known malicious domains, predict new malicious domains, and stop DNS tunneling.

Firewall as a service

Firewall as a service (FWaaS) is a deployment method for delivering a firewall as a cloud-based service. FWaaS possesses the same features as a next-generation firewall, but is implemented in the cloud. Organizations that move the firewall to the cloud can benefit from cost savings by eliminating the need to install or maintain security hardware at branch and retail locations.

A SASE solution incorporates FWaaS into its unified platform. Organizations that include the FWaaS service model within a SASE framework can easily manage their deployments from a single platform.

A SASE solution should enable FWaaS capabilities to provide the protection of a next-generation firewall by implementing Network Security policy in the cloud. You must ensure that your SASE solution does not provide only basic port blocking or minimal firewall protections. You need the same features that a next-generation firewall embodies and the features that cloud-based security offers, such as threat prevention services and DNS security.

Prisma Access provides FWaaS, which protects branch offices from threats while providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, and sandboxing.

Threat prevention

In today's world of small- and large-scale breaches, where ransomware attacks occur daily, threat prevention is important for protecting your organization's data and employees. A variety of threat prevention tools are available, from anti-malware and intrusion prevention to SSL decryption and file blocking, thus providing organizations ways to block threats. However, these point products require separate solutions, thus making management and integration difficult.

Within a SASE solution, a single cloud platform integrates all these point products and services. This integration provides simplified management and oversight of all threats and vulnerabilities across your network and cloud environments.

You need the latest threat intelligence to stop exploits and malware in order to protect your data. Your SASE solution should incorporate threat prevention tools into its framework so you can react quickly and swiftly to remediate threats. Be sure to check the quality of threat intelligence that is being provided by the vendor. The vendor should gather and share data from various sources, including customers, other vendors, and other related industry leaders, to provide continuous protection from unknown threats.

The use of Prisma Access for threat prevention combines the proven technologies in the Palo Alto Networks platform with global sources of threat intelligence and automation to stop previously known or unknown attacks.

Secure web gateway

Organizations rely on secure web gateway (SWG) to prevent employees and devices from accessing malicious websites. SWG can be used to block inappropriate content (such as pornography and gambling) or websites that businesses don't want users accessing while at work, such as streaming services such as Netflix. SWG also can be used to enforce an acceptable use policy (AUP) before internet access is granted.

SWG is one of the many security services that a SASE solution must provide. As organizations grow and add ever greater numbers of remote users, coverage and protection become more difficult. A SASE solution moves SWG into the cloud, thus providing protection in the cloud through a unified platform for complete visibility and control over the entire network.

A SASE solution includes the same security services in an SWG, allowing organizations to control access to the web and enforce security policies that protect users from hostile websites. Other security services such as FWaaS, DNS security, threat prevention, DLP, and CASB also should be included.

Prisma Access for SWG functionality is designed to maintain visibility into all types of traffic while stopping evasions that can mask threats. The Palo Alto Networks web filtering capabilities also drive its credential theft prevention technology, which can stop corporate credentials from being sent to previously unknown sites.

Data loss prevention

Data loss prevention (DLP) tools protect sensitive data and ensure that it is not lost, stolen, or misused. DLP is a composite solution that monitors data within the environments where it is deployed (such as networks, endpoints, and clouds) and through their egress points. It also alerts important stakeholders when policies are violated. Due to compliance requirements such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR), DLP is a crucial solution for data security and compliance. Legacy DLPs rely on old core technology initially designed for on-premises perimeters and subsequently extended and adapted to cloud applications. DLPs are loaded with features, disjointed policies, configurations, and workarounds, and have become very complex, difficult to deploy at scale, and expensive. Digital transformation and new data use models demand a fresh approach to data protection.

Through the SASE approach, DLP becomes one cloud-delivered solution centralized around the data itself, everywhere. The same policies are consistently applied to sensitive data, whether at rest, in motion, or in use, and regardless of its location. In the SASE architecture, DLP is no longer a standalone solution anymore, but embedded in the organization's existing control points, thus eliminating the need to deploy and maintain multiple tools. With SASE, organizations can finally enable a comprehensive data protection solution that relies on a scalable and simple architecture and allows effective machine learning by leveraging access to global traffic.

DLP is a necessary tool to protect sensitive data and ensure compliance throughout the organizations. Consequently, the SASE solution must include this core capability. With SASE, DLP is an embedded, cloud-delivered service used to accurately and consistently identify, monitor, and protect sensitive data everywhere across networks, clouds, and users.

Prisma Access combines integration with DLP controls that are API-driven (through Prisma SaaS) and inline (through Prisma Access). These DLP policies allow organizations to categorize data and establish policies that prevent data loss.

Cloud access security broker

Many organizations depend on cloud access security brokers (CASBs) to provide visibility into SaaS application use, understand where their sensitive data resides, enforce company policies for user access, and protect their data from hackers. CASBs are cloud-based security policy enforcement points that provide a gateway for your SaaS provider and your employees.

CASB should be another security feature within your SASE solution, creating a single platform for stakeholders to manage security controls. A SASE solution helps you understand which SaaS apps are being used and where data is going, regardless of where users are located.

Your SASE solution should incorporate both inline and API-based SaaS controls for governance, access controls, and data protection. The combination of inline and API-based CASB capabilities is called a multimode CASB and provides superior visibility, management, security, and zero-day protection against emerging threats.

Prisma Access and Prisma SaaS implement security controls that combine inline security API security and contextual controls, acting as a CASB to determine access to sensitive information.

These controls are implemented in an integrated manner and applied throughout all cloud application policies.

Key Idea

- The combination of inline and API-based CASB capabilities is called a multimode CASB

3.19.1 Describe sanctioned, tolerated, and unsanctioned SaaS applications

To safely enable SaaS use in your organization, start by clearly defining the SaaS applications that should be used and which behaviors within those applications are allowed. This step requires a clear definition of which applications are:

- **Sanctioned** (allowed and provided by IT)
- **Tolerated** (allowed because of a legitimate business need, with restrictions, but not provided by IT)
- **Unsanctioned**

Sanctioned SaaS applications provide business benefits and are fast to deploy, require minimal cost, and are infinitely scalable. Tolerated SaaS applications fulfill a legitimate business need, but certain use restrictions may be necessary to reduce risk. Unsanctioned SaaS applications either clearly provide no business benefits or the security risks of the application outweigh the business benefits. For example, an unsanctioned SaaS application may violate regulatory compliance mandates, create an unacceptable risk of loss of corporate intellectual property or other sensitive data, or enable malware distribution.

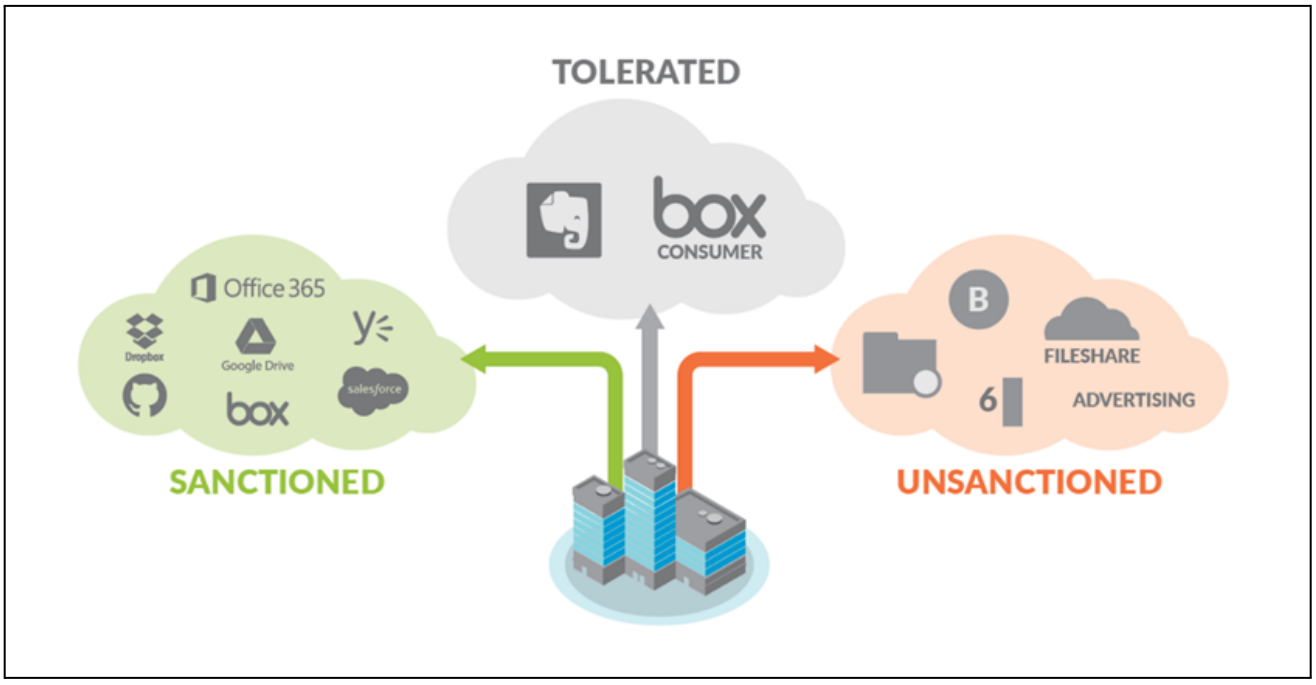


Figure: Sanctioned and unsanctioned SaaS applications

SaaS threat prevention
WildFire threat cloud integration with Prisma SaaS provides cyberthreat prevention to block known malware and to identify and block unknown malware. This integration extends the existing integration of WildFire to prevent threats from spreading through the sanctioned SaaS applications, which in turn prevents a new insertion point for malware. When new malware is discovered by Prisma SaaS, the threat information is shared with the rest of the product portfolio, even if it is not deployed inline with the SaaS applications.

Data exposure visibility

Prisma SaaS provides complete visibility across all user, folder, and file activity, which provides detailed analysis that helps you transition from a position of speculation to one of exact knowledge regarding occurrences within the SaaS environment at any given point. Because you can view deep analytics into day-to-day use, you can quickly pinpoint any data risks or compliance-related policy violations. This detailed analysis of user and data activity allows for granular data governance and forensics.

Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

Contextual data exposure control
Prisma SaaS enables you to define granular, context-aware policy control that provides you with the ability to drive enforcement and quarantine users and data as soon as a violation occurs. This control allows you to quickly and easily satisfy data risk compliance requirements such as PCI and PII while still maintaining the benefits of cloud-based applications.

Prisma SaaS prevents data exposure in unstructured (hosted files) and structured (application entries such as Salesforce.com) data. Both data types are a common source of improper data shares.

Advanced document classification
Prisma SaaS inspects documents for common sensitive data strings (such as credit card numbers, SSH keys, and Social Security numbers) and flags them as risks if they are improperly shared. Unique to Prisma SaaS is the ability to identify documents by type, through advanced document classification regardless of the data that is contained in the document itself. Prisma SaaS has been designed to automatically identify sensitive documents, such as those related to medical, tax, and legal issues.

Retroactive policy
A traditional network security solution can see only inline data and apply security policies to data accessed inline, after the policy is created. This approach doesn't effectively prevent SaaS data exposure, however, because SaaS data may have been shared long before the policy was created. This data may not be accessed inline for many months or years, thus potentially leaving sensitive data exposed indefinitely to malware infection and unauthorized access.

Prisma SaaS retroactively applies security policies to all users and data from the beginning of the SaaS account's creation, rather than the policy's creation, to identify any potential vulnerabilities or policy violations. Prisma SaaS does not wait for someone to access the data inline to apply policies and resolve any vulnerabilities or violations; SaaS data and shares are proactively discovered, protected, and resolved, regardless of when they were created.

Policies are context-driven to allow for granular definitions of data exposure risks. This granularity is necessary to enable SaaS use while still preventing accidental data exposure. Policies take several factors in context to create an overall data exposure risk profile. One or two factors may not provide enough insight into the potential risk of the share. The overall risk of exposure is determined only after reaching a comprehensive understanding of the full context of the share.

Risks are calculated by user type, document type, sensitive data contained, how the data is shared, and whether malware is present. This capability provides the ability to control the exposure at a granular level based on several important factors. For example, a financial team may be able to share financial data with other people on its team, but not beyond that. Even though the original share is allowed, the team cannot share data that is infected with malware. The financial team may, however, be allowed to share non-sensitive data company-wide or, in some cases, with external vendors. The key to enabling this level of granularity is the ability to look at the share in the context of all the factors.

3.19.2 List how to control sanctioned SaaS usage

To control sanctioned SaaS use, an enterprise security solution must provide the following:

- **Threat prevention:** SaaS applications introduce new threat risks that need to be understood and controlled. Many SaaS applications automatically sync files with users, and users often share data in SaaS applications with third parties that are out of an organization's control. These two aspects of SaaS environments create a new insertion point for malware that not only can get in from external shares but also can automatically sync those infected files across the organization without any user intervention. To address SaaS-based malware threats, a security solution must be able to prevent known and unknown malware from residing in sanctioned SaaS applications, regardless of the source.
- **Visibility and data exposure control:** After sanctioned SaaS use is defined and controlled with a granular policy, data residing in those SaaS applications no longer is visible to the organization's perimeter firewalls. This loss of visibility creates a blind spot for IT. Additional data exposure controls are needed to specifically address the unique risks associated with SaaS environments, with a focus on data protection. Visibility of data stored and used in SaaS applications is critical to ensuring a deep understanding of users, the data they have shared, and how they have shared it.
- **Risk prevention, not just risk response:** An organization's users commonly use certain SaaS applications long before the organization officially sanctions those applications. Even after a SaaS application is sanctioned, data often is shared with third parties that don't necessarily have next-generation security solutions to effectively safeguard SaaS data from malware threats and data exposure risks. Threat prevention and data exposure control in a SaaS-based environment require visibility and control not just from the time that a SaaS application is sanctioned going forward. You need visibility and control of *all* your data, including data that was being stored and shared before the SaaS application was sanctioned.

Data residing within enterprise-enabled SaaS applications is not visible to an organization's network perimeter. Prisma SaaS connects directly to sanctioned SaaS applications to provide data classification, sharing/permission visibility, and threat detection within the application. This capability yields unparalleled visibility, which allows organizations to inspect content for data exposure violations and control access to shared data via a contextual policy.

Prisma SaaS builds on the existing SaaS visibility and granular control capabilities of the product portfolio provided through App-ID, with detailed SaaS-based reporting and granular control of SaaS use. The figure below shows an example of the granular controls for SaaS applications supported by App-ID.

APPLICATION	CONTROL	FEATURE
Box	Box- Personal	App-ID
	Box- Corporate	App-ID
	Upload control	File Blocking
	Download control	File Blocking
	Malware detection	WildFire & protection profile
	User-based control	User-ID

Figure: Example of granular controls supported by App-ID

Prisma SaaS is a completely cloud-based, end-to-end security solution that provides visibility and control within SaaS applications, without the need for any proxies, agents, software, additional hardware, or network changes. Prisma SaaS isn't an inline service, so it doesn't impact latency, bandwidth, or end-user experience. Prisma SaaS communicates directly with the SaaS applications themselves and looks at data from any source, regardless of the device or location from which the data was sent.

3.20 Describe the network-as-a-service layer

The network-as-a-service layer in Prisma Access delivers important SASE capabilities, including:

- Software-defined wide-area network (SD-WAN)
- Virtual private network (VPN)
- Zero Trust network access (ZTNA)
- Quality of service (QoS)

Refer section 3.19 for more details.

3.21 Describe how Prisma Access provides traffic protection

Cloud Managed Prisma Access – using the Prisma Access app – gives you a simplified way to interact with and manage Prisma Access. In the Prisma Access app, you'll find what you need to manage your Prisma Access with the Prisma Access app. If you're using Panorama to manage Prisma Access, visit here instead.

Prisma Access helps you deliver consistent security to your remote networks and mobile users. All your users – at headquarters, office branches, and on the road – connect to Prisma Access to safely use the internet and cloud and data center applications. You get protection at scale with global coverage, so you don't have to worry about things like sizing and deploying firewalls at your branches or building out and managing appliances in colocation facilities.

The Prisma Access app is one of two management interfaces for Prisma Access (you can also use Panorama). You'll need to decide how you want to manage Prisma Access before you begin, as you cannot change management interfaces once you get started.

3.21 Reference

- Prisma Access Administrator's Guide (Cloud Managed) (paloaltonetworks.com). https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin

3.22 Describe Prisma Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) Leverages data from public service providers to deliver continuous visibility, security policy compliance and threat detection across cloud resources, users, data, and applications. This includes APIs that enable you to add cloud accounts, monitor cloud security posture, enable data classification and malware scanning on public cloud storage, detect and respond to threats, and maintain compliance. It includes the Visibility, Compliance, and Governance APIs, Data Security API, and Identity and Access Management (IAM) API.

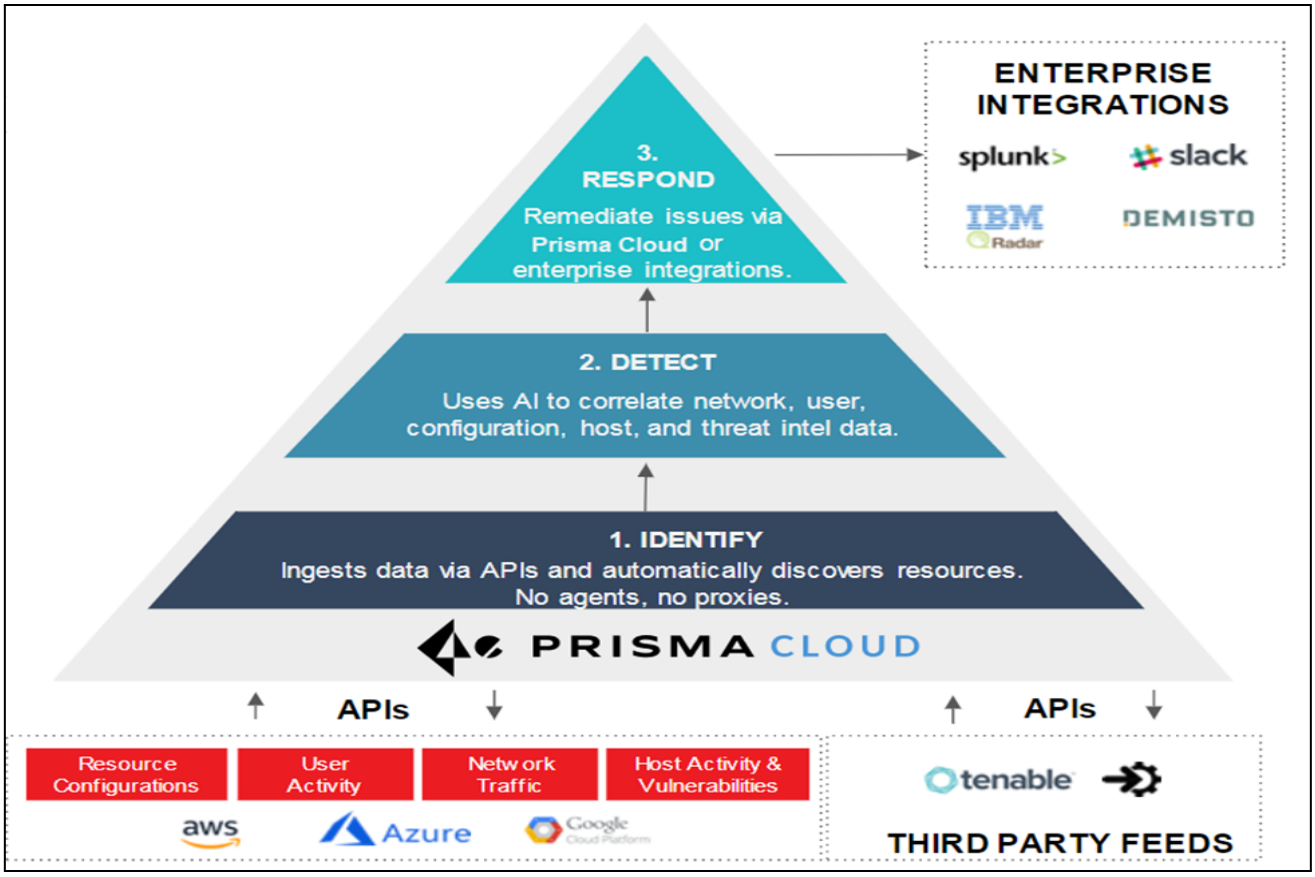
Cloud Security Posture Management with Prisma Cloud

The API-based service enables granular visibility into your resources deployed on public cloud platforms and into the network traffic flows to these resources from the internet and between instances. Prisma Cloud also provides threat detection and response for resource misconfigurations and workload vulnerabilities and visibility into user activity within each cloud environment. Tracking user activity helps to identify account compromises, the escalation of privileges with privileged accounts, and insider threats from malicious users, unauthorized activity, and inadvertent errors. Prisma Cloud continuously monitors your cloud environments to help ensure that your cloud infrastructure is protected from these security threats.

In addition to providing visibility and reducing risks, Prisma Cloud facilitates Security Operations Center (SOC) enablement and adherence to compliance standards. As the service automatically discovers and monitors compliance for new resources that are deployed in your cloud environment, it enables you to implement policy guardrails to ensure that resource configurations adhere to industry standards; it also helps you integrate configuration change alerts into DevSecOps workflows that automatically resolve issues as they are discovered. This capability streamlines the process of identifying issues and detecting and responding to a list of prioritized risks to maintain an agile development process and operational efficiency.

Key Idea

- Prisma Cloud continuously monitors your cloud environments to ensure that your cloud infrastructure is protected from security threats.



Here are some highlights of Prisma Cloud:

- **Comprehensive Visibility**—Enables you to view your resources – deployed on multiple cloud infrastructure platforms – from a single console. In addition to providing a consolidated view of the resources across the cloud platforms, Prisma Cloud integrates with threat intelligence feeds, vulnerability scanners, and Security Information and Event Management (SIEM) solutions to help you build a contextual view of your cloud deployments.
- **Policy Monitoring**—Enables you to use Prisma Cloud, which includes Security policies based on industry standards, to continuously monitor for violations. Because cloud platforms enable agility and your users can create, modify, and destroy resources on-demand, these user actions often occur without any security oversight. Prisma Cloud provides hundreds of out-of-the-box policies for common security and compliance standards, such as GDPR, PCI, CIS, and HIPAA. You can also create custom policy rules to address specific needs or to customize the default policy rules.
- **Anomaly Detection**—Automatically detects suspicious user and network behavior using machine learning. Prisma Cloud consumes data about your AWS resources from AWS CloudTrail, AWS Inspector, and Amazon GuardDuty to detect account compromises and insider threats. This service uses machine learning to score the risk level for each cloud resource based on the severity of business impact, policy violations, and anomalous behavior. Risk scores are then aggregated so that you can prioritize your alerts and benchmark risk postures across your entire environment.

- **Contextual Alerting**—Leverages highly contextual alerts for prioritization and rapid response. Because Prisma Cloud also integrates with external vulnerability services such as AWS Inspector, Tenable.io, and Qualys to continuously scan your environment, it gains additional context to identify unexpected and potentially unauthorized and malicious activity. For example, the service scans for unpatched hosts, escalation of privileges, and use of exposed credentials, and also scans communication for malicious IP addresses, URLs, and domains.
- **Cloud Forensics**—Enables you to go back to any point in time and investigate an issue within seconds. To help you identify security blind spots and investigate issues, Prisma Cloud monitors network traffic from sources such as AWS VPC flow logs, Azure flow logs, GCP flow logs, Amazon GuardDuty, and user activity from AWS CloudTrail and Azure.
- **Compliance Reporting**—Reports your risk posture to your management team, to your board of directors, and to auditors.
- **Data Security**—Scans data stored on AWS S3 buckets and provides visibility on the scan results directly on the Prisma Cloud dashboard. The data security capabilities include predefined data policies and associated data classification profiles such as PII, Financial, or Healthcare & Intellectual Property that scan your objects stored in the S3 bucket to identify exposure – how sensitive information is kept private, or exposed or shared externally, or allows unauthorized access. It also integrates the industry-leading WildFire service to detect known and unknown malware that may have infiltrated any Amazon Web Service Simple Storage Service (AWS S3) buckets.

3.22 Reference

- Cloud Security Posture Management. https://prisma.pan.dev/docs/cloud
- Cloud Security Posture Management with Prisma Cloud. https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin/get-started-with-prisma-cloud/prisma-cloud

3.23 Summary of key ideas

- The U.S. National Institute of Standards and Technology (NIST) defines cloud computing in Special Publication (SP) 800-145 as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.”
- Integrate security into your IDE, SCM and CI workflows to detect and prevent issues as early as possible.
- Virtual machines provide the greatest levels of isolation, compatibility, and control in the continuum and are suitable for running nearly any type of workload.
- In the DevOps model, developers frequently deliver small amounts of code for continuous testing.
- Cloud resources and SaaS applications must be correctly configured and adhere to your organization’s security standards from day one to prevent successful attacks.
- “Cloud native” refers to a methodology of software development essentially designed for cloud delivery and exemplifies all the benefits of the cloud by nature.
- Zero Trust Network Access (ZTNA) is an important part of the Zero Trust philosophy of “never trust, always verify” developed by Forrester.
- The combination of inline and API-based CASB capabilities is called a multimode CASB
- Prisma Cloud continuously monitors your cloud environments to ensure that your cloud infrastructure is protected from security threats.

Domain 4: Elements of Security Operations

4.1 Describe the main elements included in the development of SOC business objectives

Security operations centers can go by many names, including Cyber Defense Center or Security Intelligence Center. A security operations center, or SOC, is typically thought of as a physical room or area in an organization's office where cybersecurity analysts work to monitor enterprise systems. Security operations can be defined more broadly as a function that identifies, investigates, and mitigates threats. If there is a person in an organization responsible for looking at security logs, that fits the role of security operations. Continuous improvement is also a key activity of a security operations organization.

Mission

Developing, documenting, and socializing the mission statement for your security operations is one of the most important elements of the organization. It will define to you, and to the business, the purpose of the SOC. This should include the objectives of the security operations organization and the goals the organization expects to achieve for the business.

Socializing the mission statement and getting buy-in from executives provides clear expectations and scope of the security operations team's responsibilities. Some mission statements include defending an organization, protecting assets, or enabling the business. Some, like service providers, are customer-focused. Others provide openness, as university systems do. Each mission statement is unique; however, they do have some common properties. The mission statement should define what actions will be taken, how those actions will be executed, and what the results are to the business.

Key Idea

- Palo Alto Networks Security Operations Center Mission Statement:
  Defend our information and technology resources, intellectual property, and ability to operate by disrupting our adversaries' abilities to conduct their operations and achieve their desired outcomes.

Governance

Governance measures performance against the defined and socialized mission statement. It defines the rules and processes put in place to ensure proper operation of the organization. It can include principles, mandates, standards, enforcement criteria, and SLAs. Additionally, it defines how the security operations team will be managed and who is responsible for ensuring the team continually meets the mission of the business. This should include actions performed to ensure the mission objectives are met.

Planning
Planning includes details on how the security operations organization will achieve its goals. Main business drivers must be identified and documented. Other inclusions consist of vision, strategy, service scope, deliverables, responsibilities, accountability, operational hours, stakeholders and a statement of success.

Planning ought to include a three-year vision, ensuring the continuation of operations – even in times of rotating executives that may have execution variances – to provide the expected value to the business. Planning also ought to incorporate an investment strategy. This not only includes technology purchases but automation goals and investment in people. It should tightly align to the business. If there is a large M&A strategy or digital transformation to the cloud, for example, the investment plan should align to those initiatives.

4.1.1 Reference

- Elements of Security Operations, https://www.paloaltonetworks.com/resources/ebooks/elements-of-soc

4.2 Describe the components of SOC business management and operations

Case Management
An SOC's necessary capability includes a clear protocol for documenting and escalating incidents. Case management is a collaborative process that involves documenting, monitoring, tracking and notifying the entire organization of security incidents and their current status. The minimum set of data points that should be captured in a case, as well as the tool users select for this function, should be capable of handling this data. Often, organizations will utilize multiple tools (ticketing, SOAR, email, etc.) for case management. However, this path is ill-advised, as it severs data continuity and incident handling efficiency takes a hit.
Case management should also include a definition of who will have access to the data and tools, how cases will be documented in a consistent manner, and how teams will collaborate to close out incidents. A case management system should also be encrypted with strict access controls enforced due to the highly sensitive data that it will contain.

Budget
A financial plan for the costs of running the SOC should begin with an agreement on the mission of the SOC. Then, the technology, staff, facility, training, and additional needs to achieve that mission are identified. From there, a budget can be established to meet the minimum requirements of the team.

Often, a SOC budget is set from the top-down or assigned a percentage of an IT budget. This approach is not business focused and will result in frustration between capabilities and expectations from the business.

Once the budget is established, it should be followed by a regular review to identify additional needs or surplus. The timeline for regular budget requests and approval should be documented to avoid surprises or a last-minute rush to defend the organization's needs. Define the process needed to change the allocated budget, as well as a process for emergency budget relief.
A business-savvy budgeting resource can help the security operations organization navigate CapEx spending vs. OpEx spending and the expectations of the business. Be aware that government SOCs have additional considerations around the timing of elections and possible party-switching, which could result in dramatic budget shifts.

Metrics
If analysts spend time gathering metrics that cannot drive change, then this process will prove, at best, a waste of time. Worse, this method can drive the wrong behavior. Mean Time to Resolution (MTTR) provides a clear example of this danger. MTTR is a fine metric when used in an NOC (where uptime is key) but can be detrimental when used in an SOC. Holding analysts accountable for MTTR will result in rushed and incomplete analyses; analysts will rush to close incidents rather than do full investigations that can feed learning back into the controls to prevent future attacks. This will not produce better outcomes or reduced risk for the business.

Another poor metric is counting the number of firewall rules deployed. Organizations can put in place 10,000 firewall rules, but if the first is inaccurate, then the rest are useless. This is similar to measuring the number of data feeds into a SIEM. If there are 15 data feeds but only one use-case, then the data feeds aren't being properly utilized and are a potentially expensive waste.
Caution should be taken when measuring peoples' performance. Ranking top performers by number of incidents handled can have skewed results and may lead to analysts "cherry-picking" incidents that they know are fast to resolve. Additionally, evaluating individual performance in this way violates the law in various countries.

Reporting
Reporting ought to give an account of what analysts have observed, heard, done, or investigated. It should quantify activity and demonstrate the value the security operations team provides to the business or client organizations in the case of an MSSP. Reporting outcomes will not necessarily drive changes in behavior but can track current activity. Reports are typically generated daily, weekly and monthly.

Daily reports should include open incidents, with details centered on daily activity. Weekly reports should identify security trends to initiate threat-hunting activities, which includes the number of cases opened and closed and conclusions of the tickets (malicious, benign, false positives). Include such information as how many different security use cases were triggered and their severity, as well as how they were distributed through the hours of the day.
Monthly reports should focus on the overall effectiveness of the SecOps function. These reports should cover topics such as how long events are sitting in queue before being triaged, if the staffing in the SOC is appropriate (do more resources need to be added or reassigned), the efficacy of rule fires, and if rules that never fire or always fire result in a false-positive.

Business Liaisons
A growing trend is for security organizations to hire business liaisons. This role ties in to the different aspects of the business and helps to identify and explain the impact of security. This includes keeping up to date with new product launches and development schedules, onboarding new branch offices, and handling mergers and acquisitions where legacy networks/applications need to be brought into the main security program. This role can also assume responsibilities for partner, vendor, and team interface management.

Governance, Risk, and Compliance
The governance, risk, and compliance (GRC) function is responsible for creating the guidelines to meet business objectives, manage risk, and meet compliance requirements. Common compliance standards include PCI-DSS, HIPAA, GDPR, etc. These standards require different levels of protection/encryption and data storage. Those requirements are typically handled by other groups; however, the breach disclosure requirements directly involve the security operations team. The SOC team must interface with the GRC team to define escalation intervals, contacts, documentation and forensic requirements.

DevOps
The DevOps team's responsibilities include developing, implementing, and maintaining company-created applications. This role has evolved greatly with the adoption of cloud apps and agile development, where application upgrades are now rolled out within minutes, rather than the long cycles where we would see major releases only every six to 12 months. The DevOps team's main motivation is to push bug-free features out to users as rapidly as possible. Some groups work security protocols into their release cycles, but so far most do not.

Security operations will need to interface with the DevOps team to work protocol into the release procedures and to get ahead of the new development tools and features tested/used by DevOps. Additionally, the SecOps team will want to familiarize themselves with the DevOps processes and procedures in order to reduce friction between the teams.

4.3 List the six essential pillars of effective security operations

Security operations can be complex. However, by breaking them down into discrete elements, you can assess which of the elements are covered in a SOC and to what extent. Then use the element map to evolve security operations toward methods that provide better prevention and remediation faster.
The elements of security operations are broken down into six pillars. These pillars range from capabilities the business requires from the SOC to the operationalization of those capabilities.

The six pillars include:
1. Business (goals and outcomes)
2. People (who will perform the work)
3. Interfaces (external functions to help achieve goals)
4. Visibility (information needed to accomplish goals)
5. Technology (capabilities needed to provide visibility and enable people)
6. Processes (tactical steps required to execute on goals)
All elements must tie back to the business itself and the goals of the security operations organization.

1. Business

The Business pillar defines the business objectives and management strategies of the security operations team. Business questions that require an answer include:

- Mission: What are we doing?
- Planning: How are we going to do it?
- Governance: How are we going to manage what we are doing?
- Staffing: Who do we need to do this?
- Facility: Where are we going to do this?
- Budget: What will it cost to do this?
- Metrics: How will we know whether it works effectively?
- Reporting: How will we track activity and provide updates?
- Collaboration: How will we communicate and track issues with the rest of the business?

2. People

The People pillar defines the humans who will accomplish the goals of the security operations team and how to manage them. Questions to answer include:

- How will we find staff and train them to fulfill their roles?
- What will we do to retain them?
- How will we manage the workloads of the staff?
- How will we validate the efficacy of the actions of the staff?

3. Interfaces

The Interfaces pillar defines what functions to involve to achieve the stated goals. Security operations is not a silo and needs to work with many other functions of the business. We describe each of these interactions as "interfaces," and they should clearly define expectations between the groups. Each group will have different goals and motivations that, when understood, will help create positive team interactions. Identifying the scope of responsibility and separation of duties will also reduce friction within an organization. Questions to answer include:

- What other functions of the business impact security operations?
- What other functions of the business does security operations impact?
- How will the security operations team work alongside these other functions?
- Who has ownership of responsibilities and what, if any, service-level agreements (SLAs) need to be documented?
- At what interval will these interfaces be reviewed and updated?

4. Visibility

The Visibility pillar defines what information the SecOps function needs access to. This includes security and systems data, as well as knowledge management content and communications through collaboration tools. Questions to answer include:

- What primary security data does the SecOps team need access to?
- What contextual data is needed?
- How often does this data need to be refreshed?
- What knowledge base information needs to be accessed?
- How will the security operations team see activity in the SOC?
- How will external teams see activity in the SOC?

5. Technology
The Technology pillar defines the needs to achieve visibility into the necessary information in the security operations organization. It is important to note that each element should not be thought of as a different tool but rather a capability that should be achieved with the given technology stack. Technologies and capabilities change rapidly, so these are the most fluid elements of a security operations team.

A glut of siloed tools in the industry leads to a variety of issues, including extensive vendor management, limited feature use, duplicate functionality, and, sometimes, end-user degradation. PAN sees a shift, with organizations moving away from best-of-breed siloed tools toward platforms that provide capabilities needed in the SOC without the need for installation and maintenance of different tools. Questions to answer for the Technology pillar include:

- What capabilities are required to achieve the necessary visibility?
- What technology will provide these capabilities?
- Who will be responsible for the licensing, implementation, and maintenance of the technology?
- How will technology and content updates be requested and performed?
- What updates will be carried out automatically and at what interval?

6. Processes
The Processes pillar defines the processes and procedures executed by the security operations organization to achieve the determined mission. Questions to answer include:

- What processes need to be defined?
- Where will the processes and procedures be documented?
- How will this documentation be accessed and socialized?
- Who will have responsibility for keeping this documentation updated?
- How often will the processes need to be reviewed and updated?

4.3.1 References

- The Six Pillars of Effective Security Operations
  https://www.paloaltonetworks.com/blog/2020/01/cortex-security-operations/

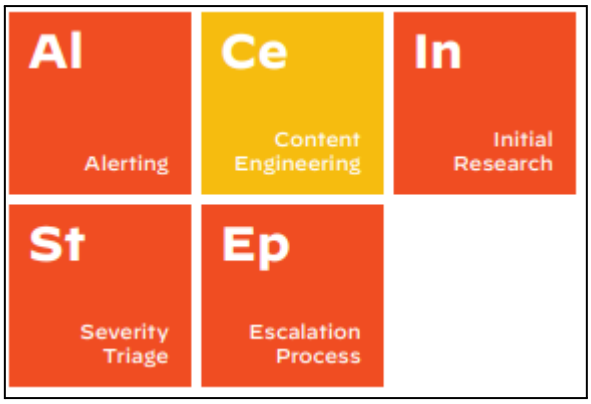
4.4 Describe the four SecOps functions

There are four main functions of security operations are:

1. Identify – Identify an alert as potentially malicious and open an incident.
2. Investigate – Investigate the root cause and impact of the incident.
3. Mitigate – Stop the attack.
4. Continuous Improvement – Adjust and improve operations to keep up with changing and emerging threats.

The majority of a Security Operations Analyst's time is spent in the identify phase due to false positives and low-fidelity alerts they must weed through. Correctly implemented prevention-based architectures and automated correlation help reduce the time needed for this phase. Analysts also spend a lot of time in the mitigation phase. The lack of automated remediation drives this trend, along with complex or lacking interfaces with teams outside of the security operations organization that need to be involved in halting the attack.

4.4.1 Identify



Alerting
An alert determines whether an event is important enough to become an actionable incident. The function has a high opportunity to utilize automation.

Content Engineering
The content engineering function builds the necessary alerting profiles to identify the alerts that will be forwarded for investigation. The content engineer and the security operations teams need feedback continuously flowing between them.

Initial Research
Initial research is a set of high-level processes utilized by an organization to begin an investigation into a suspicious alert. The results of the initial research provide context around an incident to help in gathering information to triage, escalate, and determine if further investigation is needed or if the alert is malicious or benign.

Severity Triage
Severity triage defines the event prioritization based on impact to the business to help guide the analyst's action through the Incident Response lifecycle. When utilizing automation to assign an initial severity, the analyst reviews that severity assignment and then validates it against the uniqueness of the organization. This verifies or modifies the severity and prioritization of the incident against other priorities.

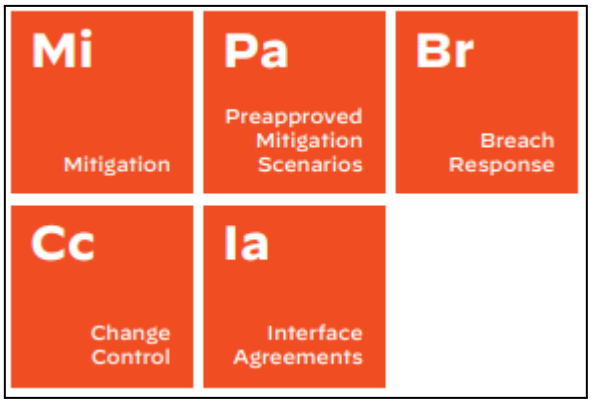
Escalation Process
Escalation guidelines enable the security operations team to increase the organization's awareness of a potential issue and receive the necessary support.

4.4.2 Investigate

Detailed Analysis
Detailed analysis encompasses a deeper investigation into an incident to determine if it is truly malicious, identify the scope of the attack, and document the observed impact. It involves a manual process to answer the questions: What? Where? When? Why? Who? and How? Additionally, a detailed analysis helps to confidently determine if an incident is a "true" incident. In the event of a false positive, feedback should be provided to the Content Engineer so they can tune alerts, or to the security engineering team so they may update controls.

Forensics and Telemetry
Forensics and telemetry provide the necessary data to perform the different types of investigation, from severity triage to detailed analysis and hunting. Telemetry is a broad range of activity gathered in real-time from a given source. It is inclusive rather than selective, and rarely collects the contents of an item. Examples of network telemetry would be session and packet headers rather than packet contents. Endpoint telemetry would include process execution details and file and memory reads and writes, but not their contents. Telemetry is consistently recorded, which makes it more useful than a "log" that collects prescribed information only when triggered by a specific event; it is also more accessible than forensics due to the wider coverage area and speed of collection.

4.4.3 Mitigate



Mitigation
Once an incident has been validated, a mitigation strategy must be executed. The mitigation strategy consists of a set of processes as well as interface agreements to contain the security incident. This typically includes documentation of any actions taken by the security team and temporary controls that can be implemented to quickly stop an attack, which should lead to permanent controls to prevent future attacks.

Preapproved Mitigation Scenarios
Some mitigation processes are easily automated for preapproved mitigation scenarios. These include a set of parameters that allow for the immediate containment or prevention of a security incident without further approvals. An example would be to block an infected laptop from the network to prevent the spread of malware.

Breach Response
A true breach requires a plan separate from standard mitigation. It defines how to effectively respond during a critical severity incident. The first piece of this plan is to identify the cross-functional stakeholders, including corporate communications, legal teams, and third-parties as appropriate. Then assign a timeline of when each stakeholder should become involved and how they will be initially notified.

Change Control
In cases of both manual and automated mitigation, a change control process must be in place to monitor, document, and control changes being made. A good change control process ensures alterations to the environment have a minimized impact to business and documentation in case a look-back review needs to be performed. The information required for this documentation should be identified and ideally contained in a formalized template. This process should have timelines for reviewing and rolling back temporary changes. Also included should be who can request changes, the steps needed to initiate change, and any prerequisites or change windows available for the modification.

Interface Agreements
Interface agreements define how the security operations team and surrounding teams will interact with each other. These agreements list the teams involved and detail the scope of work and responsibilities for each team. SLAs and change request processes and escalation should be referred to in cases where an interface agreement is not upheld. Communication paths and tools used between the teams should be identified. Regularly review all agreements. Additionally, set and clearly state the intervals of reviews.

4.4.4 Improve

Tuning
Tuning refers to adjustments made to the alerting procedures regarding security incidents based on the outcomes of security investigations. It is an important step in reducing false positives and low-fidelity alerts in the SOC. An analyst may determine, during the course of a security incident, that there is a better way to detect the incident to increase visibility at the SIEM. When this occurs, the analyst will engage the tuning process to improve that visibility for future incidents. General tuning should be based on metrics collected from systems in the SOC. This includes a process to retire alerts when they are stale or ineffective.
The tuning process should define:

- Who or what triggers tuning efforts
- The thresholds for those triggers
- A review process for existing alerts
- The steps to request modifications to existing alerts (to increase visibility of future security incidents based on the outcome of a security investigation)

PAN recommends that alerts be reviewed – at minimum – on a quarterly cadence with a monthly review of alert metrics.

Process Improvement
Adjustments must also be made to the incident response lifecycle based on the results of security incidents and new threats. New technologies introduced to the SOC and the business may also require IR process updates. The process should include information about who can update the IR processes (this person must be a qualified resource knowledgeable in IR). Changes need not be made daily, so IR process updates should define how often processes should be reviewed, which will vary by process. All improvements should be reviewed and then socialized with affected groups.

Capability Improvement
Capability improvement is rooted in revisiting prior incidents and asking how these incidents can be better prevented or mitigated in the future. This results in adjustments to the alerting profile, prevention posture, and automation techniques. Sometimes the goal is to prevent an attack, while other times it's to stop a breach faster or gather the appropriate information needed for quicker investigation. Ideally, this effort should be on-going and follow every investigation. In most cases that is not possible, so a monthly review of incidents should occur to identify opportunities for capability improvement.

Quality Review
As new tuning measures, processes, and capabilities are implemented, a thorough peer evaluation of the changes should be carried out to ensure effectiveness and value to the business. Additionally, incident workflows and documentation should also be reviewed to confirm consistency within the IR process, which will result in a higher level of capability from the security operations organization. Identifying the person responsible for reviewing changes and closed cases must be documented along with a cadence for the review process. That resource must be given time to perform these reviews outside of their normal duties. A process should be created to define what severity cases require review, what items in the case will be reviewed, how feedback will be provided, and what training opportunities arise from the reviews. The identified training must then be delivered to the security operations organization (and sometimes beyond the SecOps group) to improve the overall efficiency and efficacy of preventing breaches.

4.5 Describe SIEM

Originally designed as a tool to assist organizations with compliance and industry-specific regulations, security information and event management (SIEM) is a technology that has been around for almost two decades. It combines security information management (SIM) with security event management (SEM) and provides the foundation for cybersecurity threat detection capabilities. SIEM technology helps to manage security incidents through the collection and analysis of log data, security events, and other event or data sources.

Key Idea

- Security operations center (SOC) analysts use SIEM tools to manage security incidents, and detect and respond to potential threats quickly.

According to Gartner, businesses looking for SIEM today need the solution to collect security event logs and telemetry in real time for threat detection, incident response, and compliance use cases, with the ability to analyze the telemetry to detect attacks and other flagged activities. SIEMs also provide the ability to investigate incidents, report on activities, and store the relevant events and logs.

SIEM solutions help security teams to:

- Collect, enrich, and store data
- Apply correlation and analytics
- Investigate and mitigate threats
- Provide data insights and reporting

SIEM software brings together event and log data from end-user devices, servers, network infrastructure, security devices, and applications, and aggregates the data into a centralized platform for easy access. Data collected can then be sorted into designated actionable categories that can recognize deviations from normal activity. This makes it easier for incident response teams to identify threats and investigate security alerts and incidents. SIEM solutions can be deployed on-premises, hybrid, and more increasingly, cloud-based. Cloud-based SIEMs offer faster and simpler deployment, and can scale automatically to accommodate increases in data sources or data ingestion.

4.5.1 References

- What Is Security Information and Event Management (SIEM)? https://www.paloaltonetworks.com/cyberpedia/what-is-security-information-and-event-management

4.6 Describe the purpose of security orchestration, automation, and response (SOAR)

Companies and organizations find value in SOAR because it minimizes the impact of security incidents of all types while maximizing the value of existing security investments, and reduces the risk of legal liability and business downtime overall. SOAR helps companies address and overcome their security challenges by enabling them to:

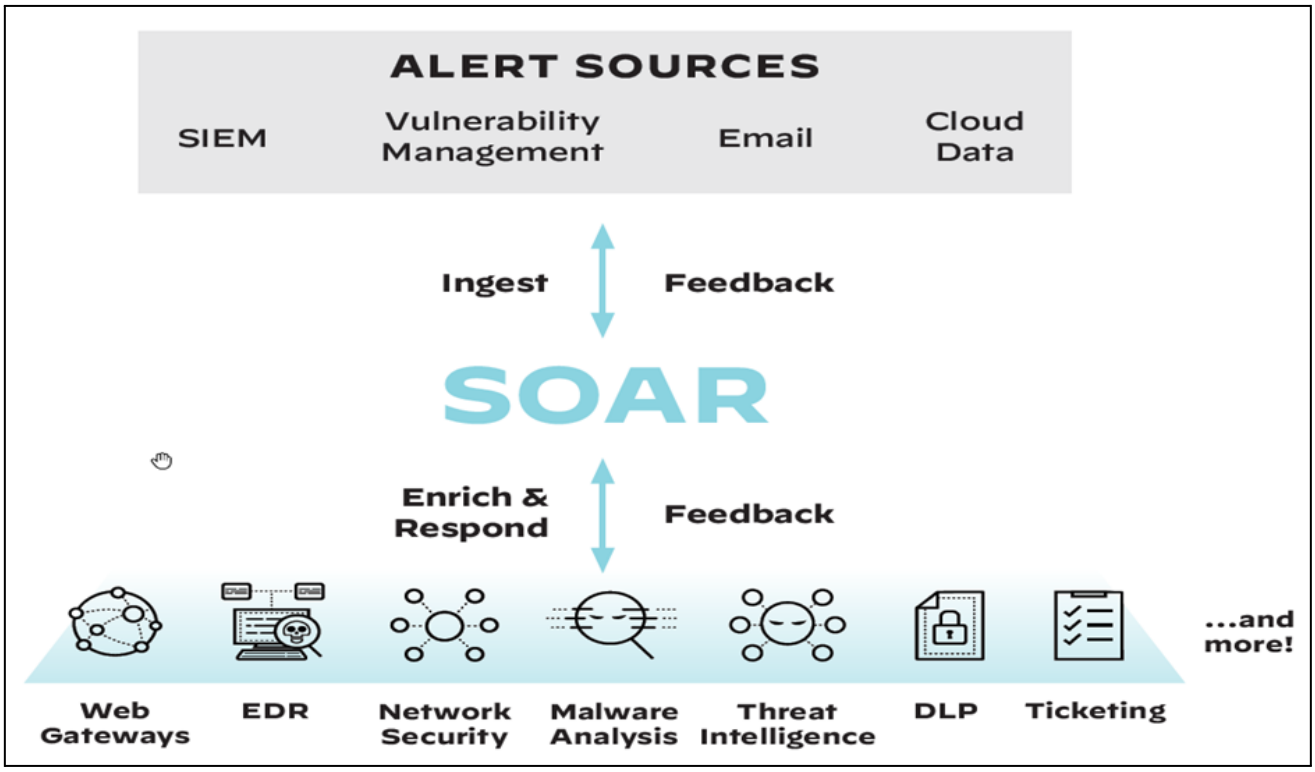
- **Unify their existing security systems and centralize data collection** to gain full visibility, thus greatly improving the company's security posture and operational efficiency and productivity.
- **Automate repetitive manual tasks** and manage all aspects of the security incident lifecycle, therefore increasing analyst productivity and freeing up analysts to focus on improving security instead of on performing manual tasks.
- **Define incident analysis and response procedures** as well as leverage security playbooks to prioritize, standardize, and scale response processes in a consistent, transparent, and documented way.
- **Engage in faster incident response as analysts** can quickly and accurately identify and assign incident severity levels to security alerts, reducing alerts, and alleviating alert fatigue.
- **Streamline processes and operations** to better identify and manage potential vulnerabilities both proactively and reactively.
- **Supports real-time collaboration and unstructured investigations** by routing each security incident to the analyst best suited to respond to it while providing functions that support easy communication and tracking between teams and team members.

SOAR systems allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows.

Key Idea

- SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

The playbooks coordinate across technologies, security teams, and external users for centralized data visibility and action. They help accelerate incident response times and increase analyst productivity. They standardize processes and thus provide consistency, which improves operational confidence in SOC capabilities.



SOAR Use Cases

Use Case	What Orchestration Helps With (High-Level Overview)
Handling security alerts	Phishing enrichment and response – ingesting potential phishing emails; triggering a playbook; automating and executing repeatable tasks, such as triaging and engaging affected users; extracting and checking indicators; identifying false positives; and priming the SOC for a standardized response at scale. Endpoint malware infection – pulling in threat feed data from endpoint tools, enriching that data, cross-referencing retrieved files/hashes with a security information and event management (SIEM) solution, notifying analysts, cleaning endpoints, and updating the endpoint tool database. Failed user logins – after a predefined number of failed user login attempts, assessing whether a failed login is genuine or malicious by triggering a playbook, engaging users, analyzing their replies, expiring passwords, and closing the playbook. Logins from unusual locations – identifying potentially malicious virtual private network (VPN) access attempts by checking VPN and cloud access security broker (CASB) presence, cross-referencing IPs, confirming a breach with the user, issuing a block, and closing the playbook.
Managing security operations	Secure Sockets Layer (SSL) certificate management – checking endpoints to see which SSL certificates have expired or will soon expire, informing users, rechecking the status a few days later, escalating an issue to the appropriate people, and closing the playbook. Endpoint diagnostics and kickstart – checking connectivity and agent connectivity, enriching context, opening a ticket, kickstarting agents, and closing the playbook. Vulnerability management – ingesting vulnerability and asset information, enriching endpoint and common vulnerabilities and exposures (CVE) data, querying for vulnerability context, calculating severity, turning over control to security analysts for remediation and investigation, and closing the playbook.
Hunting for threats and responding to incidents	Indicators of compromise (IOC) hunting – taking in and extracting IOCs from attached files, hunting IOCs across threat intelligence tools, updating databases, and closing the playbook. Malware analysis – ingesting data from multiple sources, extracting and detonating malicious files, generating and displaying a report, checking for malice, updating the database, and closing the playbook. Cloud-aware incident response – consuming data from cloud-focused threat detection and event logging tools, unifying processes across cloud and on-premises security infrastructures, correlating with a SIEM, extracting and enriching indicators, checking for malice, turning over control to analysts and having them review the information, update the database, and close the playbook.
Automating data enrichment	IOC enrichment – ingesting data from multiple sources; extracting any indicators that need to be detonated; enriching URLs, IPS and hashes; checking for malice; updating the database; inviting analysts to review and investigate the information; and closing the playbook. Assigning incident severity – checking other products for a vulnerability score and to see whether existing indicators have been assigned a score, assigning severity, checking usernames and endpoints to see if they are on a critical list, assigning critical severity, and closing an incident.

4.6.1 References

- What Is SOAR? https://www.paloaltonetworks.com/cyberpedia/what-is-soar

4.7 Describe the analysis tools used to detect evidence of a security compromise

Analysis tools include advanced techniques, tools, and algorithms that provide the ability to detect evidence of security compromise within large volumes of data. Processes should be defined to explain how an analyst will determine whether an alert is malicious and the chosen tools should assist or automate this process. The tools also should provide access to gather context, preferably automated about the given event. Ownership, budget, and the support model for the tools need to be defined.

Analysis tools often are based on machine learning, deep learning, and artificial intelligence that provide either standalone, embedded, or add-on functionality to detect evidence of a security compromise. Security analytics can be performed on data either stored at rest or collected in motion, even at line speed on a massive network. This capability can be obtained by SecOps teams in a variety of different ways, with most security products and services including some sort of security analytics function.

4.8 Describe how to collect security data for analysis

> Analysis tools include advanced techniques, tools, and algorithms that provide the ability to detect evidence of security compromise within large volumes of data. Processes should be defined for how an analyst will determine whether an alert is malicious and the chosen tools should assist or automate this process. The tools also should provide access to gather context, preferably automated about the given event. Ownership, budget, and the support model for the tools need to be defined.

Analysis tools often are based on machine learning, deep learning, and artificial intelligence that provide either standalone, embedded, or add-on functionality to detect evidence of a security compromise. Security analytics can be performed on data that is either stored at rest or collected in motion, even at line speed on a massive network. This capability can be obtained by SecOps teams in a variety of different ways with most security products and services including some sort of security analytics function.

Endpoint Protection
Today's modern endpoint protection solutions help to secure endpoints by analyzing files before and after they execute to look for signs of suspicious activity or indicators of potential threats. This analysis is typically done via a single agent from the cloud to allow for speed and scalability with little if any impact on end-user device performance.

Administrators monitor and control endpoints through a centralized management console that can remotely connect to devices whether they are connected to the internet or not. Logs can often be forwarded from these centralized management points to a central collection point for security analysis.

Network Traffic Capture
Network traffic captures provide the ability to intercept and log traffic traversing network appliances. This can be accomplished with firewalls, IDS/IPS, proxies, routers, switches, and standalone traffic capture technologies. Logging of this traffic provides visibility to the security operations organization for detailed analysis and advanced investigations. Raw traffic logs should be accessible by analysts but not presented to them unless tied to an alert or as queried by the staff.

Firewall
Firewalls are an essential cybersecurity control to separate networks and enforce restrictions for communications between them. They can be physical devices in a datacenter or implemented virtually to protect assets in the cloud. Firewall functionality varies and can include URL Filtering, IPS/IDS, antivirus, SSL decryption, and VPNs, among other features to consolidate capabilities into a single tool. They can be set up to monitor boundary traffic as well as lateral traffic and used for network segmentation to further lock down a business's critical assets. They are a key tool for the team to gain visibility into network traffic through logs and alerts received from different points in the environment. The security operations team should define what information they require from the firewall, including additional context for investigation of alerts. Many firewalls are not configured out-of-the-box to provide this context, so the security operations team may have to drive that requirement with the network security team. Although firewalls provide the visibility that analysts need, they can also be a burden to the analysts if not continuously updated with new policies and/or if they are not tuned properly and provide overwhelming low-fidelity data to the SOC.

Intrusion Prevention/Detection Systems
Other tools used to gain visibility are Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and DNS sinkholing. These features may be integrated with a firewall or used as standalone tools. An IDS is considered a reactive control that generates alerts based on rules configured in the system, while an IPS has the added capability to mitigate or block malicious behavior; this makes it a proactive control. DNS sinkholing allows, alerts upon, or sinkholes known malicious traffic. Agreements must be in place between the group that maintains the IDS/IPS/DNS sinkholing technologies and the SOC, defining how OS upgrades, outages, and patching will be communicated to the SOC and how the SOC will request that additional signatures be added. The SOC should also be aware of basic architecture and configuration settings, such as coverage of the functionality and if they are configured to fail open. As with firewalls, additional logging may need to be turned on to generate the context needed by the security operations team to perform investigations.

Malware Sandbox
A malware sandbox is used as a safe place to simulate an end user's environment to test unknown applications that may contain viruses or other types of malicious code. A security team can "detonate" malicious code to observe the behavior and impact to systems and networks without impacting the whole of the environment. Malware sandbox features can include malicious file analysis, API call tracing, and memory analysis, along with other advanced capabilities. The sandbox should be set up to analyze the impact to all operating systems used in the environment and should produce ample logs from which to generate security controls. The security operations team is typically not responsible for using the malware sandbox but benefits from the information gathered during simulations.

Threat Intelligence Platform (TIP)
Threat Intelligence Platform (TIP) is a technology solution that collects, aggregates and organizes threat intel data from multiple sources and formats. A TIP provides security teams with information on known malware and other threats, powering efficient and accurate threat identification, investigation and response. It enables threat analysts to spend their time analyzing data and investigating potential security threats rather than spending their time collecting and managing data. Moreover, a TIP allows security and threat intelligence teams to easily share threat intelligence data with other stakeholders and security systems. A TIP can be deployed as either a software-as-a-service (SaaS) or as an on-premises solution.

4.9 Describe the use of analysis tools within a security operations environment

A number of SecOps tools exist to help security teams successfully run the SOC. These tools have grown in number as technology evolves and can present a complex mix of siloed tools to manage. Fortunately, consolidation of capabilities has begun across the industry to provide less tools with more functionality.

Tools that help SecOps teams build a proactive defense include:

- Security information and event management (SIEM)
- Network detection and response
- Endpoint detection and response
- User and entity behavior analytics (UEBA)
- Extended detection and response (XDR)
- Security orchestration, automation, and response (SOAR)

4.9.1 References

- Security Operations (SecOps), https://www.paloaltonetworks.com/cyberpedia/what-is-security-operations

4.10 Describe the responsibilities of a security operations engineering team

The SOC engineering team's responsibilities encompass the implementation and ongoing maintenance of the security operation team's tools, including the SIEM and analysis tools. This team's responsibilities must be clearly defined. Will they be responsible for licensing, maintenance and updating tools? Will they manage the underlying architecture (CPU, RAM, storage, cloud implementation) or will that be handled by another team? Use the team's SLAs to cut down friction between teams as well as to establish clear communication plans.

4.11 Describe the Cortex platform in a security operations environment and the purpose of Cortex XDR for various endpoints

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can:

- Identify hidden, stealthy, and sophisticated threats proactively and quickly
- Track threats across any source or location within the organization
- Increase the productivity of the people operating the technology
- Get more out of their security investments
- Conclude investigations more efficiently

From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes. This, in turn, lets them better serve users and accelerate digital transformation initiatives – because when users, data, and applications are protected, companies can focus on strategic priorities.

XDR Benefits

- **Block known and unknown attacks with endpoint protection**: Block malware, exploits, and fileless attacks with integrated AI-driven antivirus and threat intelligence.
- **Gain visibility across all your data**: Collect and correlate data from any source to detect, triage, investigate, hunt, and respond to threats.
- **Automatically detect sophisticated attacks 24/7**: Use out-of-the-box analytics and custom rules to detect advanced persistent threats and other covert attacks.
- **Avoid alert fatigue**: Simplify investigations with automated root cause analysis and a unified incident engine, reducing the number of alerts your team needs to review and lowering the skill required for triage.
- **Increase SOC productivity**: Consolidate endpoint security policy management and monitoring, investigation, and response across your network, endpoint, and cloud environments in one console, thereby increasing SOC efficiency.
- **Root out adversaries without disrupting your users**: Stop attacks while avoiding user or system downtime.
- **Shut down advanced threats**: Protect your network against insider abuse, external attacks, ransomware, fileless and memory-only attacks, and advanced zero-day malware.
- **Force multiply your security team**: Stop every stage of an attack by detecting indicators of compromise (IOCs) and anomalous behavior as well as prioritizing analysis with incident scoring.
- **Restore hosts after a compromise**: Quickly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys by using remediation suggestions.
- **Extend detection and response to third-party data sources**: Enable behavioral analytics on logs collected from third-party firewalls while integrating third-party alerts into a unified incident view and root cause analysis for faster investigations.

What is EDR Security?

Endpoint detection and response refers to a category of tools used to find and investigate threats on endpoint devices. EDR tools typically provide detection, analysis, investigation, and response capabilities. Compared to these security solutions, XDR takes a wider view by integrating data from endpoint, cloud, identity, and other solutions.

EDR products monitor events generated by endpoint agents to look for suspicious activity, and the alerts they create help SecOps analysts identify, investigate, and remediate issues. These solutions also collect telemetry data on suspicious activity and may enrich that data with other contextual information from correlated events. However, they lack key capabilities that slow down incident response.

Key Idea

- EDR solutions do not offer integrations with other tools and data sources for full visibility, so they cannot provide holistic protection.

4.11.1 References

- What is endpoint detection and response (EDR)?
  https://www.paloaltonetworks.com/cyberpedia/what-is-endpoint-detection-and-response-edr
- What is XDR?
  https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

4.12 Describe how Cortex XSOAR improves security operations efficiency

Security teams lack the people and scalable processes to keep pace with an overwhelming volume of alerts and endless security tasks. Analysts waste time pivoting across consoles for data collection, determining false positives, and performing manual, repetitive tasks throughout the lifecycle of an incident.

Cortex XSOAR enhances Security Operations Center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case, resulting in up to 90 percent faster response times and as much as a 95 percent reduction in alerts requiring human intervention.

4.13 Describe how Cortex Data Lake improves security operations visibility

Palo Alto Networks Cortex Data Lake provides cloud-based logging for our security products, including our next-generation firewalls, Prisma Access, and Cortex XDR. Cortex Data Lake lets you collect ever-expanding volumes of data without needing to plan for local compute and storage, and is ready to scale from the start.

Cortex Data Lake enables AI-based innovations for cybersecurity with the industry's only approach to normalizing and stitching together your enterprise's data. Get public cloud scale and locations with assurance of the security and privacy of your data. Significantly improve the accuracy of security outcomes with trillions of multi-source artifacts for analytics. Cortex Data Lake can:

- Radically simplify your security operations by collecting, integrating, and normalizing your enterprise's security data.
- Effortlessly run advanced AI and machine learning with cloud-scale data and compute.
- Constantly learns from new data sources to evolve your defenses

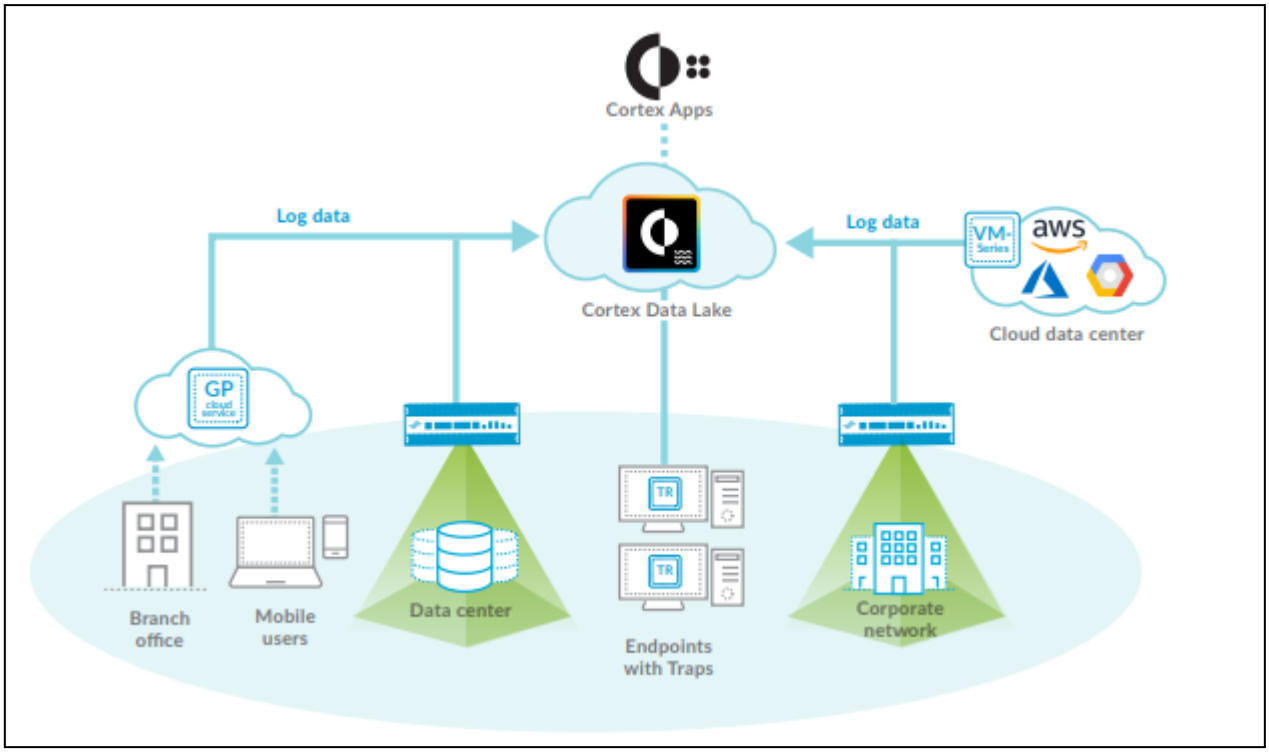


Figure: Cortex Data Lake Integration

Organizations often lack the visibility they need to stop attacks. Data is typically locked in silos across cloud, endpoint, and network assets, preventing tools from effectively finding, investigating, or automating threat response. Cortex Data Lake is the industry's only approach to normalizing and stitching together your enterprise's data. It automatically collects, integrates and normalizes data across your security infrastructure. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Tight sensor integration allows new data sources and types to be continually added to evolve your defenses.

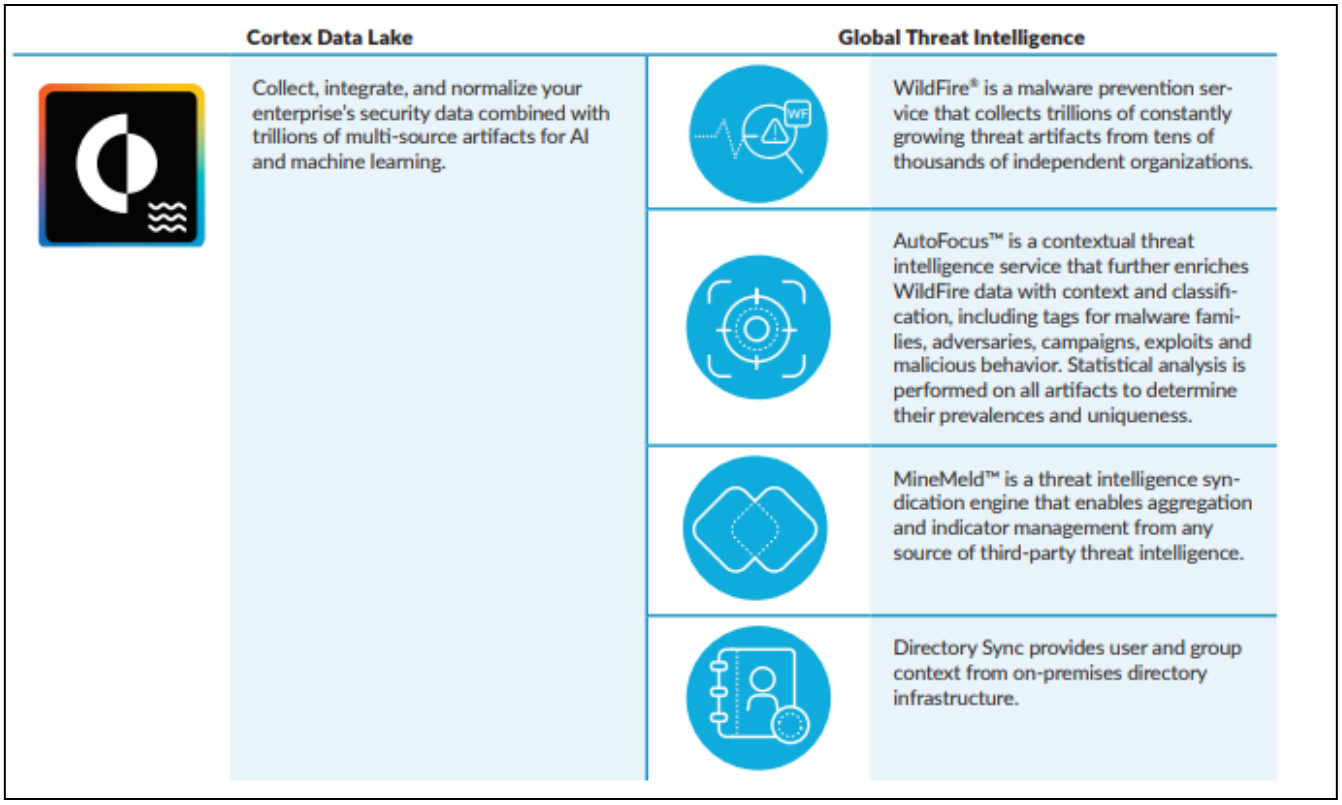


Figure: Cortex Data Lake data sources

4.14 Describe how XSIAM can be used to accelerate SOC threat response

The SIEM category has served security operations for many years as a way to aggregate and analyze alerts and logs, albeit with incremental improvement in security outcomes. As a result, security operations teams continued to bolt on new tools that promised to solve point problems, resulting in a fragmented and ineffective security architecture. As compute and data storage have improved exponentially, it is essential to radically reimagine how we can deliver real-time security that can match pervasive, AI-powered cyberattacks. XSIAM is the revolutionary approach that collects granular data — not just logs and alerts — to drive machine learning for natively autonomous response actions, such as cross-correlation of alerts and data, detection of highly sophisticated, emerging threats, and automated remediation based on native threat intelligence and attack surface data.

Specifically, Cortex XSIAM will transform security operations by enabling organizations to:

- **Build an intelligent data foundation while reducing costs.**
  Cortex XSIAM can natively ingest, normalize, and integrate granular data across the security infrastructure at nearly half the list cost of legacy security products attempting to solve the problem.
- **Respond in minutes rather than days.**
  By providing multiple layers of AI-driven analytics based on the data foundation, Cortex XSIAM detects emerging threats across the entire security infrastructure, automates correlation of alerts and data into incidents, and leverages a self-learning recommendation engine to determine response next-steps.

- **Proactively outpace threats.**
  Cortex XSIAM enables continuous discovery of vulnerabilities through native attack surface management and automated response based integrated threat intelligence from tens of thousands of Palo Alto Networks customers.

4.14.1 References

- Cortex Data Lake.
  https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-cortex-data-lake/overview
- What is endpoint detection and response (EDR)?
  https://www.paloaltonetworks.com/company/press/2022/palo-alto-networks-introduces-the-autonomous-security-platform--cortex-xsiam--to-reimagine-siem-and-soc-analytics

4.15 Summary of key ideas

- Palo Alto Networks Security Operations Center Mission Statement:
  Defend our information and technology resources, intellectual property, and ability to operate by disrupting our adversaries ability to conduct their operations and achieve their desired outcomes.
- Security operations center (SOC) analysts use SIEM tools to manage security incidents, and detect and respond to potential threats quickly.
- SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.
- EDR solutions do not offer integrations with other tools and data sources for full visibility, so they cannot provide holistic protection.

Appendix: Glossary

- **Address Resolution Protocol (ARP):** A protocol that translates a logical address, such as an IP address, to a physical MAC address. RARP translates a physical MAC address to a logical address. See also *IP address*, *media access control (MAC) address*, and *Reverse Address Resolution Protocol (RARP)*.
- **Advanced Encryption Standard (AES):** A symmetric block cipher based on the Rijndael cipher.
- **AES:** See *Advanced Encryption Standard (AES)*.
- **AI:** See *artificial intelligence (AI)*.
- **American Standard Code for Information Interchange (ASCII):** A character-encoding scheme based on the English alphabet, consisting of 128 characters.
- **Android Packet Kit (APK):** An app created for the Android mobile operating system.
- **API:** See *application programming interface (API)*.
- **APK:** See *Android Package Kit (APK)*.
- **APP:** See *Australian Privacy Principles (APP)*.
- **Application programming interface (API):** A set of routines, protocols, and tools for building software applications and integrations.
- **AR:** See *augmented reality (AR)*.

- **ARP:** See *Address Resolution Protocol (ARP)*.
- **Artificial intelligence (AI):** The ability of a system or application to interact with and learn from its environment and automatically perform actions accordingly, without requiring explicit programming.
- **AS:** See *autonomous system (AS)*.
- **ASCII:** See *American Standard Code for Information Interchange (ASCII)*.
- **Attack vector:** A path or tool that an attacker uses to target a network. Also known as a threat vector.
- **Augmented reality (AR):** Augmented reality enhances a real-world environment with virtual objects.
- **Australian Privacy Principles (APP):** The Privacy Act 1988 establishes standards for collecting and handling personal information, referred to as the Australian Privacy Principles (APP).
- **Authoritative DNS server:** The system of record for a given domain. See also *Domain Name System (DNS)*.
- **Autonomous system (AS):** A group of contiguous IP address ranges under the control of a single internet entity. Individual autonomous systems are assigned a 16-bit or 32-bit AS number (ASN) that uniquely identifies the network on the internet. ASNs are assigned by the Internet Assigned Numbers Authority (IANA). See also *Internet Protocol (IP) address* and *Internet Assigned Numbers Authority (IANA)*.
- **Bare-metal hypervisor:** See *native hypervisor*.
- **BES:** See *bulk electric system (BES)*.
- **Blockchain:** A data structure containing transactional records (stored as blocks) that ensures security and transparency through a vast, decentralized peer-to-peer network with no single controlling authority. Cryptocurrency is an internet-based financial instrument that uses blockchain technology. See also *cryptocurrency*.
- **Boolean:** A system of algebraic notation used to represent logical propositions.
- **Boot sector:** Contains machine code loaded into an endpoint's memory by firmware during the startup process, before the operating system is loaded.
- **Boot sector virus:** Targets the boot sector or master boot record (MBR) of an endpoint's storage drive or other removable storage media. See also *boot sector* and *master boot record (MBR)*.
- **Bot:** Individual endpoints that are infected with advanced malware that enables an attacker to take control of the compromised endpoint. Also known as a zombie. See also *botnet* and *malware*.
- **Botnet:** A network of bots (often tens of thousands or more) working together under the control of attackers using numerous command-and-control (C2) servers. See also *bot*.
- **Bridge:** A wired or wireless network device that extends a network or joins separate network segments.
- **Bring your own access (BYOA):** A remote access policy in which remote users are allowed to connect to the corporate network using personal wireless service (for example, cellular service for a personal smartphone) from a wireless network operator.
- **Bring your own device (BYOD):** A policy trend in which organizations permit end users to use their own personal devices, primarily smartphones and tablets, for work-related purposes. BYOD relieves organizations from the cost of providing equipment to employees, but creates a management challenge because of the vast number and type of devices that must be supported.
- **Broadband cable:** A type of high-speed internet access that delivers different upload and download data speeds over a shared network medium. The overall speed varies depending on the network traffic load from all the subscribers on the network segment.

- **Broadcast domain:** The portion of a network that receives broadcast packets sent from a node in the domain.
- **Bulk electric system (BES):** The large interconnected electrical system, consisting of generation and transmission facilities (among others), that comprises the "power grid."
- **Bus topology:** A LAN topology in which all nodes are connected to a single cable (the backbone) that is terminated on both ends. In the past, bus networks were commonly used for very small networks because they were inexpensive and relatively easy to install, but today bus topologies are rarely used. The cable media has physical limitations (the cable length), the backbone is a single point of failure (a break anywhere on the network affects the entire network), and tracing a fault in a large network can be extremely difficult. See also *local-area network (LAN)*.
- **BYOA:** See *bring your own access (BYOA)*.
- **BYOD:** See *bring your own device (BYOD)*.
- **California Consumer Privacy Act (CCPA):** A privacy rights and consumer protection statute enacted in 2018 for residents of California. It became effective on January 1, 2020.
- **CASB:** See *cloud access security broker (CASB)*.
- **CCPA:** See *California Consumer Privacy Act (CCPA)*.
- **CD:** See *continuous delivery (CD)*.
- **CDN:** See *content delivery network (CDN)*.
- **Child process:** In multitasking operating systems, a subprocess created by a parent process currently running on the system.
- **CI:** See *continuous integration (CI)*.
- **CIDR:** See *classless inter-domain routing (CIDR)*.
- **CIP:** See *Critical Infrastructure Protection (CIP)*.
- **Circuit-switched network:** A network in which a dedicated physical circuit path is established, maintained, and terminated between the sender and receiver across a network for each communications session.
- **Classless inter-domain routing (CIDR):** A method for allocating IP addresses and IP routing that replaces classful IP addressing (for example, Class A, B, and C networks) with classless IP addressing. See also *Internet Protocol (IP) address*.
- **Cloud access security broker (CASB):** Software that monitors activity and enforces security policies on traffic between an organization's users and cloud-based applications and services.
- **Collision domain:** A network segment on which data packets may collide with each other during transmission.
- **Consumerization:** A computing trend describing the process that occurs as end users increasingly find personal technology and apps that are more powerful or capable, more convenient, less expensive, quicker to install, and easier to use than enterprise IT solutions.
- **Container:** A standardized, executable, and lightweight software code package that contains all the necessary components to run a given application or applications, including code, runtime, system tools and libraries, and configuration settings in an isolated and virtualized environment to enable agility and portability of the application workload(s).
- **Content delivery network (CDN):** A network of distributed servers that distributes cached web pages and other static content to a user from the geographic location physically closest to the user.
- **Continuous deployment:** An automated CI pipeline that requires the code to pass automated testing before it is automatically deployed, giving customers instant access to new features. See also *continuous integration (CI)*.

- **Continuous integration (CI):** A development process that requires developers to integrate code into a repository several times per day for automated testing. Each check-in is verified by an automated build, allowing teams to detect problems early.
- **Continuous delivery (CD):** An automated CI pipeline that requires the code to go through manual technical checks before it is implemented into production. See also *continuous integration (CI)*.
- **Convergence:** The time required for all routers in a network to update their routing tables with the most current routing information about the network.
- **Covered entity:** Defined by HIPAA as a healthcare provider that electronically transmits PHI (such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies), a health plan (such as a health insurance company, health maintenance organization, company health plan, or government program, including Medicare, Medicaid, military and veterans' healthcare), or a healthcare clearinghouse. See also *Health Insurance Portability and Accountability Act (HIPAA)* and *protected health information (PHI)*.
- **CRC:** See *cyclic redundancy check (CRC)*.
- **Critical Infrastructure Protection (CIP):** Cybersecurity standards defined by NERC to protect the physical and cyber assets necessary to operate the bulk electric system (BES). See also *bulk electric system (BES)* and *North American Electric Reliability Corporation (NERC)*.
- **Cryptocurrency:** A form of digital currency, such as Bitcoin, that uses encryption to control the creation of currency and verify the transfer of funds independent of a central bank or authority.
- **Cybersecurity Enhancement Act of 2014:** A U.S. regulation that provides an ongoing, voluntary public-private partnership to improve cybersecurity and to strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness.
- **Cybersecurity Information Sharing Act (CISA):** A U.S. regulation that enhances information sharing about cybersecurity threats by allowing internet traffic information to be shared between the U.S. government and technology and manufacturing companies.
- **Cyclic redundancy check (CRC):** A checksum used to create a message profile. The CRC is recalculated by the receiving device. If the recalculated CRC doesn't match the received CRC, the packet is dropped and a request to resend the packet is transmitted back to the device sending the packet.
- **DAAS:** Data, assets, applications, and services.
- **Data encapsulation:** A process in which protocol information from the OSI or TCP/IP layer immediately above is wrapped in the data section of the OSI or TCP/IP layer immediately below. Also referred to as data hiding. See also *Open Systems Interconnection (OSI) model* and *Transmission Control Protocol/Internet Protocol (TCP/IP) model*.
- **Data hiding:** See *data encapsulation*.
- **Data mining:** Enables patterns to be discovered in large datasets using machine learning, statistical analysis, and database technologies. See also *machine learning*.
- **DDOS:** See *distributed denial-of-service (DDOS)*.
- **Default gateway:** A network device, such as a router or switch, to which an endpoint sends network traffic when a specific destination IP address is not specified by an application or service, or when the endpoint does not know how to reach a specified destination. See also *router* and *switch*.
- **DevOps:** The culture and practice of improved collaboration between application development and IT operations teams.
- **DGA:** See *domain generation algorithm (DGA)*.
- **DHCP:** See *Dynamic Host Configuration Protocol (DHCP)*.

- **Digital subscriber line (DSL):** A type of high-speed internet access that delivers different upload and download data speeds. The overall speed depends on the distance from the home or business location to the provider's central office (CO).
- **Distributed denial-of-service (DDOS):** A type of cyberattack in which extremely high volumes of network traffic such as packets, data, or transactions are sent to the target victim's network to make their network and systems (such as an e-commerce website or other web application) unavailable or unusable.
- **DLL:** See *dynamic-link library (DLL)*.
- **DNS:** See *Domain Name System (DNS)*.
- **DNS over HTTPS (DoH):** DNS traffic that is encrypted using the HTTPS protocol. See also *Domain Name System* (DNS) and *Hypertext Transfer Protocol Secure (HTTPS)*.
- **DoH:** See *DNS over HTTPS (DOH)*.
- **Domain generation algorithm (DGA):** A program designed to generate domain names in a particular fashion. Attackers developed DGAs so that malware can quickly generate a list of domains that it can use for command and control (C2).
- **Domain name registrar:** An organization that is accredited by a TLD registry to manage domain name registrations. See also *top-level domain (TLD)*.
- **Domain Name System (DNS):** A hierarchical distributed database that maps the FQDN for computers, services, or any resource connected to the internet or a private network to an IP address. See also *fully qualified domain name (FQDN)*.
- **Drive-by download:** A software download, typically malware, that occurs without a user's knowledge or permission.
- **DSL:** See *digital subscriber line (DSL)*.
- **Dynamic Host Configuration Protocol (DHCP):** A network management protocol that dynamically assigns (leases) IP addresses and other network configuration parameters (such as default gateway and DNS information) to devices on a network. See also *default gateway* and *Domain Name System (DNS)*.
- **Dynamic-link library (DLL):** A type of file used in Microsoft operating systems that enables multiple programs to simultaneously share programming instructions contained in a single file to perform specific functions.
- **EAP:** See *Extensible Authentication Protocol (EAP)*.
- **EAP-TLS:** See *Extensible Authentication Protocol Transport Layer Security (EAP-TLS)*.
- **EBCDIC:** See *Extended Binary-Coded Decimal Interchange Code (EBCDIC)*.
- **EHR:** See *electronic health record (EHR)*.
- **Electronic health record (EHR):** As defined by HealthIT.gov, an EHR "goes beyond the data collected in the provider's office and include[s] a more comprehensive patient history. EHR data can be created, managed, and consulted by authorized providers and staff from across more than one healthcare organization."
- **Electronic medical record (EMR):** As defined by HealthIT.gov, an EMR "contains the standard medical and clinical data gathered in one provider's office."
- **EMR:** See *electronic medical record (EMR)*.
- **Endpoint:** A computing device such as a desktop or laptop computer, handheld scanner, IoT device or sensor (such as an autonomous vehicle, smart appliance, smart meter, smart TV, or wearable device), point-of-sale (POS) terminal, printer, satellite radio, security or videoconferencing camera, self-service kiosk, smartphone, tablet, or VoIP phone. Although endpoints can include servers and network equipment, the term is generally used to describe end-user devices. See also *internet of things (IoT)* and *Voice over Internet Protocol (VoIP)*.

- **Enterprise 2.0:** A term introduced by Andrew McAfee and defined as "the use of emergent social software platforms within companies, or between companies and their partners or customers." See also *Web 2.0*.
- **Exclusive or (XOR):** A Boolean operator in which the output is true only when the inputs are different (for example, TRUE and TRUE equals FALSE, but TRUE and FALSE equals TRUE). See also *Boolean*.
- **Exploit:** A small piece of software code, part of a malformed data file, or a sequence (string) of commands, that leverages a vulnerability in a system or software, thereby causing unintended or unanticipated behavior in the system or software.
- **Extended Binary-Coded Decimal Interchange Code (EBCDIC):** An 8-bit character-encoding scheme largely used on mainframe and mid-range computers.
- **Extended reality (XR):** Broadly covers the spectrum from physical to virtual reality with various degrees of partial sensory to fully immersive experiences.
- **Extensible Authentication Protocol (EAP):** A widely used authentication framework that includes about 40 different authentication methods.
- **Extensible Authentication Protocol Transport Layer Security (EAP-TLS):** An Internet Engineering Task Force (IETF) open standard that uses the Transport Layer Security (TLS) protocol in Wi-Fi networks and PPP connections. See also *Internet Engineering Task Force (IETF)*, *Point-to-Point Protocol (PPP)*, and *Transport Layer Security (TLS)*.
- **Extensible Markup Language (XML):** A programming language specification that defines a set of rules for encoding documents in a human-readable and machine-readable format.
- **FaaS:** See *function as a service (FaaS)*.
- **False negative:** In anti-malware, this refers to malware that is incorrectly identified as a legitimate file or application. In intrusion detection, a false negative is a threat incorrectly identified as legitimate traffic. See also *false positive*.
- **False positive:** In anti-malware, this refers to a legitimate file or application that is incorrectly identified as malware. In intrusion detection, a false positive refers to legitimate traffic that is incorrectly identified as a threat. See also *false negative*.
- **Favicon ("favorite icon"):** A small file containing one or more small icons associated with a particular website or webpage.
- **Federal Exchange Data Breach Notification Act of 2015:** A U.S. regulation that further strengthens HIPAA by requiring health insurance exchanges to notify individuals whose personal information has been compromised as the result of a data breach as soon as possible, but no later than 60 days after breach discovery. See also *Health Insurance Portability and Accountability Act (HIPAA)*.
- **Federal Information Security Management Act (FISMA):** See *Federal Information Security Modernization Act (FISMA)*.
- **Federal Information Security Modernization Act (FISMA):** A U.S. law that implements a comprehensive framework to protect information systems used in U.S. federal government agencies. Known as the Federal Information Security Management Act prior to 2014.
- **Fiber optic:** Technology that converts electrical data signals to light and delivers constant data speeds in the upload and download directions over a dedicated fiber optic cable medium. Fiber optic technology is much faster and more secure than other types of network technology.
- **File Transfer Protocol (FTP):** A program used to copy files from one system to another over a network.
- **FISMA:** See *Federal Information Security Modernization Act (FISMA)*.
- **Floppy disk:** A removable magnetic storage medium commonly used from the mid-1970s until about 2007, when it was largely replaced by removable USB storage devices.

- **Flow control:** A technique used to monitor the flow of data between devices to ensure that a receiving device, which may not necessarily be operating at the same speed as the transmitting device, doesn't drop packets.
- **FQDN:** See *fully qualified domain name (FQDN)*.
- **FTP:** See *File Transfer Protocol (FTP)*.
- **Fully qualified domain name (FQDN):** The complete domain name for a specific computer, service, or resource connected to the internet or a private network.
- **Function as a service (FAAS):** A cloud computing service that provides a platform for customers to develop, run, and manage their application functions without having to build and maintain the infrastructure normally required to develop and launch an application.
- **GDPR:** See *General Data Protection Regulation (GDPR)*.
- **General Data Protection Regulation (GDPR):** A European Union (EU) regulation that applies to any organization that does business with EU residents. It strengthens data protection for EU residents and addresses the export of personal data outside the EU.
- **Generic Routing Encapsulation (GRE):** A tunneling protocol developed by Cisco Systems that can encapsulate various Network layer protocols inside virtual point-to-point links.
- **GIF:** See *Graphics Interchange Format (GIF)*.
- **GLBA:** See *Gramm-Leach-Bliley Act (GLBA)*.
- **Gramm-Leach-Bliley Act (GLBA):** A U.S. law that requires financial institutions to implement privacy and information security policies to safeguard the non-public personal information of clients and consumers.
- **Graphics Interchange Format (GIF):** A bitmap image format that allows up to 256 colors and is suitable for images or logos (but not photographs).
- **GRE:** See *Generic Routing Encapsulation (GRE)*.
- **Hacker:** Term originally used to refer to anyone with highly specialized computing skills, without connoting good or bad purposes. However, common misuse of the term has redefined a hacker as someone that circumvents computer security with malicious intent, such as a cybercriminal, cyberterrorist, or hacktivist.
- **Hash signature:** A cryptographic representation of an entire file or program's source code.
- **Health Insurance Portability and Accountability Act (HIPAA):** A U.S. law that defines data privacy and security requirements to protect individuals' medical records and other personal health information. See also *covered entity* and *protected health information (PHI)*.
- **Heap spray:** A technique used to facilitate arbitrary code execution by injecting a certain sequence of bytes into the memory of a target process.
- **Hextet:** A group of four 4-bit hexadecimal digits in a 128-bit IPv6 address. See also *Internet Protocol (IP) address*.
- **High-order bits:** The first four bits in a 32-bit IPv4 address octet. See also *Internet Protocol (IP) address*, *octet*, and *low-order bits*.
- **HIPAA:** See *Health Insurance Portability and Accountability Act (HIPAA)*.
- **Hop count:** The number of router nodes that a packet must pass through to reach its destination.
- **Hosted hypervisor:** A hypervisor that runs within an operating system environment. Also known as a Type 2 hypervisor. See also *hypervisor* and *native hypervisor*.
- **HTTP:** See *Hypertext Transfer Protocol (HTTP)*.
- **HTTPS:** See *Hypertext Transfer Protocol Secure (HTTPS)*.
- **Hub:** A device used to connect multiple networked devices together on a local-area network (LAN). Also known as a concentrator.

- **Hypertext Transfer Protocol (HTTP):** An application protocol used to transfer data between web servers and web browsers.
- **Hypertext Transfer Protocol Secure (HTTPS):** A secure version of HTTP that uses SSL or TLS encryption. See also *Secure Sockets Layer (SSL)* and *Transport Layer Security (TLS)*.
- **Hypervisor:** Technology that allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer.
- **IaaS:** See *Infrastructure as a service (IaaS)*.
- **IaC:** See *infrastructure as code (IaC)*.
- **IAM:** See *Identity and Access Management (IAM)*.
- **IANA:** See *Internet Assigned Numbers Authority (IANA)*.
- **ICMP:** See *Internet Control Message Protocol (ICMP)*.
- **IDE:** See *integrated development environment (IDE)*.
- **Identity and Access Management (IAM):** A framework of business processes, policies, and technologies that facilitates the management of electronic or digital identities.
- **IETF:** See *Internet Engineering Task Force (IETF)*.
- **IMAP:** See *Internet Message Access Protocol (IMAP)*.
- **Indicator of compromise (IoC):** A network or operating system (OS) artifact that provides a high level of confidence that a computer security incident has occurred.
- **Infrastructure as a service (IaaS).** A cloud computing service model in which customers can provision processing, storage, networks, and other computing resources and deploy and run operating systems and applications. However, the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over operating systems, storage, and deployed applications, along with some networking components (for example, host firewalls). The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.
- **Infrastructure as code (IaC):** A DevOps process in which developers or IT operations teams can programmatically provision and manage the infrastructure stack (such as virtual machines, networks, and connectivity) for an application in software. See also *DevOps*.
- **Initialization vector (IV):** A random number used only once in a session, in conjunction with an encryption key, to protect data confidentiality. Also known as a nonce.
- **Integrated development environment (IDE):** A software application that provides comprehensive tools, such as a source code editor, build automation tools, and a debugger for application developers.
- **Inter-process communication (IPC):** A mechanism in an operating system that makes it possible to concurrently coordinate activities and manage shared data between different program processes.
- **Internet Assigned Numbers Authority (IANA):** A private, nonprofit U.S. corporation that oversees global IP address allocation, autonomous system (AS) number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and internet numbers. See also *autonomous system (AS)* and *Domain Name System (DNS)*.
- **Internet Control Message Protocol (ICMP):** An internet protocol used to transmit diagnostic messages.
- **Internet Engineering Task Force (IETF):** An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet.
- **Internet Message Access Protocol (IMAP):** A store-and-forward email protocol that allows an email client to access, manage, and synchronize email on a remote server.

- **Internet of things (IoT):** The IoT refers to the network of physical smart, connected objects that are embedded with electronics, software, sensors, and network connectivity.
- **Internet Protocol (IP) address:** A 32-bit or 128-bit identifier assigned to a networked device for communications at the Network layer of the OSI model or the Internet layer of the TCP/IP model. See also *Open Systems Interconnection (OSI) model* and *Transmission Control Protocol/Internet Protocol (TCP/IP) model*.
- **Intranet:** A private network that provides information and resources such as a company directory, human resources policies and forms, department or team files, and other internal information to an organization's users. Like the internet, an intranet uses the HTTP and/or HTTPS protocols, but access to an intranet typically is restricted to an organization's internal users. Microsoft SharePoint is a popular example of intranet software. See also *Hypertext Transfer Protocol (HTTP)* and *Hypertext Transfer Protocol Secure (HTTPS)*.
- **IoC:** See *indicator of compromise (IoC)*.
- **IoT:** See *internet of things (IoT)*.
- **IP address:** See *Internet Protocol (IP) address*.
- **IP telephony:** See *Voice over Internet Protocol (VoIP)*.
- **IPC:** See *inter-process communication (IPC)*.
- **IV:** See *initialization vector (IV)*.
- **Jailbreaking:** Hacking an Apple iOS device to gain root-level access to the device. This hacking is sometimes done by end users to allow them to download and install mobile apps without paying for them, from sources, other than the App Store, that are not sanctioned and/or controlled by Apple. Jailbreaking bypasses the security features of the device by replacing the firmware's operating system with a similar, albeit counterfeit version, which makes the device vulnerable to malware and exploits. See also *rooting*.
- **Joint Photographic Experts Group (JPEG):** A photographic compression method used to store and transmit photographs.
- **JPEG:** See *Joint Photographic Experts Group (JPEG)*.
- **Kerberos:** An authentication protocol in which tickets are used to identify network users.
- **LAN:** See *local-area network (LAN)*.
- **Least privilege:** A network security principle in which only the permission or access rights necessary to perform an authorized task are granted.
- **Least significant bit:** The last bit in a 32-bit IPv4 address octet. See also *Internet Protocol (IP) address*, *octet*, and *most significant bit*.
- **Linear bus topology:** See *bus topology*.
- **LLC:** See *Logical Link Control (LLC)*.
- **Local-area network (LAN):** A computer network that connects laptop and desktop computers, servers, printers, and other devices so that applications, databases, files and file storage, and other networked resources can be shared across a relatively small geographic area such as a floor, a building, or a group of buildings.
- **Logical Link Control (LLC):** A sublayer of the OSI model Data Link layer that manages the control, sequencing, and acknowledgement of frames and manages timing and flow control. See also *Open Systems Interconnection (OSI) model* and *flow control*.
- **Long-Term Evolution (LTE):** A type of 4G cellular connection that provides fast connectivity, primarily for mobile internet use.
- **Low-order bits:** The last four bits in a 32-bit IPv4 address octet. See also *Internet Protocol (IP) address*, *octet*, and *high-order bits*.
- **LTE:** See *Long-Term Evolution (LTE)*.
- **M2M:** See *machine to machine (M2M)*.
- **MAC address:** See *media access control (MAC) address*.

- **Machine learning:** A subset of AI that applies algorithms to large datasets to discover common patterns in the data that then can be used to improve the performance of the system. See also *artificial intelligence (AI)*.
- **Machine to machine (M2M):** M2M devices are networked devices which exchange data and can perform actions without manual human interaction.
- **Malware:** Malicious software or code that typically damages, takes control of, or collects information from an infected endpoint. Malware broadly includes viruses, worms, trojan horses (including remote access trojans, or RATs), anti-AV, logic bombs, back doors, root kits, boot kits, spyware, and (to a lesser extent) adware.
- **Master boot record (MBR):** The first sector on a computer hard drive, containing information about how the logical partitions (or file systems) are organized on the storage media, and an executable boot loader that starts up the installed operating system.
- **MBR:** See *master boot record (MBR)*.
- **MEC:** See *multi-access edge computing (MEC)*.
- **Media access control (MAC) address:** A unique 48-bit or 64-bit identifier assigned to a network interface card (NIC) for communications at the Data Link layer of the OSI model. See also *Open Systems Interconnection (OSI) model*.
- **Metamorphism:** A programming technique used to alter malware code with every iteration, to avoid detection by signature-based anti-malware software. Although the malware payload changes with each iteration, for example, by using a different code structure or sequence, or inserting garbage code to change the file size, the fundamental behavior of the malware payload remains unchanged. Metamorphism uses more advanced techniques than polymorphism. See also *polymorphism*.
- **MFA:** See *multi-factor authentication* (MFA).
- **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP):** A protocol used to authenticate Microsoft Windows-based workstations using a challenge-response mechanism to authenticate PPTP connections without sending passwords. See also *Point-to-Point Tunneling Protocol (PPTP)*.
- **Mixed reality (MR):** Includes technologies such as VR, AR, and XR that deliver an immersive and interactive physical and digital sensory experience in real time. See also *augmented reality (AR)*, *extended reality (XR)*, and *virtual reality (VR)*.
- **Most significant bit:** The first bit in a 32-bit IPv4 address octet. See also *Internet Protocol (IP) address*, *octet*, and *least significant bit*.
- **Motion Picture Experts Group (MPEG):** An audio and video compression method used to store and transmit audio and video files.
- **MPEG:** See *Motion Picture Experts Group (MPEG)*.
- **MPLS:** See *multiprotocol label switching (MPLS)*.
- **MR:** See *mixed reality (MR)*.
- **MS-CHAP:** See *Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)*.
- **Multi-access edge computing (MEC):** MEC is defined by the European Telecommunications Standards Institute (ETSI) as an environment "characterized by ultra-low latency and high bandwidth as well as real-time access to radio network information that can be leveraged by applications".
- **Multicloud:** An enterprise cloud environment (or strategy) consisting of two or more public and/or private clouds.
- **Multi-factor authentication (MFA):** Any authentication mechanism that requires two or more of the following factors: something you know, something you have, something you are.

- **Multiprotocol label switching (MPLS):** MPLS is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide-area networks.
- **Mutex:** A program object that allows multiple program threads to share the same resource, such as file access, but not simultaneously.
- **NAT:** See *network address translation (NAT)*.
- **National Cybersecurity Protection Advancement Act of 2015:** A U.S. regulation that amends the Homeland Security Act of 2002 to enhance multidirectional sharing of information related to cybersecurity risks and strengthens privacy and civil liberties protections.
- **Native hypervisor:** A hypervisor that runs directly on the host computer hardware. Also known as a Type 1 or bare-metal hypervisor. See also *hypervisor* and *hosted hypervisor*.
- **Natural language search:** The ability to understand human spoken language and context, rather than a Boolean search, for example, to find information. See also *Boolean*.
- **NERC:** See *North American Electric Reliability Corporation (NERC)*.
- **Network address translation (NAT):** A technique used to virtualize IP addresses by mapping private, non-routable IP addresses assigned to internal network devices to public IP addresses.
- **Network and Information Security (NIS) Directive:** A European Union (EU) directive that imposes network and information security requirements for banks, energy companies, healthcare providers and digital service providers, among others.
- **NIS Directive:** See *Network and Information Security (NIS) Directive*.
- **Nonce:** See *initialization vector (IV)*.
- **North American Electric Reliability Corporation (NERC):** A not-for-profit international regulatory authority responsible for ensuring the reliability of the bulk electric system (BES) in the continental United States, Canada, and the northern portion of Baja California, Mexico. See also *bulk electric system (BES)* and *Critical Infrastructure Protection (CIP)*.
- **Obfuscation:** A programming technique used to render code unreadable. It can be implemented using a simple substitution cipher, such as an XOR operation, or more sophisticated encryption algorithms, such as AES. See also *Advanced Encryption Standard (AES)*, *exclusive or (XOR)*, and *packer*.
- **Octet:** A group of 8 bits in a 32-bit IPv4 address. See *Internet Protocol (IP) address*.
- **One-way hash function:** A mathematical function that creates a unique representation (a hash value) of a larger set of data in a manner that is easy to compute in one direction (input to output), but not in the reverse direction (output to input). The hash function can't recover the original text from the hash value. However, an attacker could attempt to guess what the original text was and see if it produces a matching hash value.
- **Open Systems Interconnection (OSI) model:** A seven-layer networking model consisting of the Application (Layer 7 or L7), Presentation (Layer 6 or L6), Session (Layer 5 or L5), Transport (Layer 4 or L4), Network (Layer 3 or L3), Data Link (Layer 2 or L2), and Physical (Layer 1 or L1) layers. Defines standard protocols for communication and interoperability using a layered approach in which data is passed from the highest layer (application) downward through each layer to the lowest layer (physical), then transmitted across the network to its destination, then passed upward from the lowest layer to the highest layer. See also *data encapsulation*.
- **Optical carrier:** A standard specification for the transmission bandwidth of digital signals on SONET fiber optic networks. Optical carrier transmission rates are designated by the integer value of the multiple of the base rate (51.84Mbps). For example, OC-3 designates a 155.52Mbps

(3 x 51.84) network and OC-192 designates a 9953.28Mbps (192 x 51.84) network. See also *synchronous optical networking (SONET)*.

- **OSI model:** See *Open Systems Interconnection (OSI) model*.
- **PaaS:** See *platform as a service (PaaS)*.
- **Packer:** A software tool that can be used to obfuscate code by compressing a malware program for delivery, then decompressing it in memory at runtime. See also *obfuscation*.
- **Packet capture (pcap):** A traffic intercept of data packets that can be used for analysis.
- **Packet-switched network:** A network in which devices share bandwidth on communications links to transport packets between a sender and receiver across a network.
- **PAP:** See *Password Authentication Protocol (PAP)*.
- **Password Authentication Protocol (PAP):** An authentication protocol used by PPP to validate users with an unencrypted password. See also *Point-to-Point Protocol (PPP)*.
- **Payment Card Industry Data Security Standards (PCI DSS):** A proprietary information security standard mandated and administered by the PCI Security Standards Council (SSC), and applicable to any organization that transmits, processes, or stores payment card (such as debit and credit cards) information. See also *PCI Security Standards Council (SSC)*.
- **pcap:** See *packet capture (pcap)*.
- **PCI:** See *Payment Card Industry Data Security Standards (PCI DSS)*.
- **PCI DSS:** See *Payment Card Industry Data Security Standards (PCI DSS)*.
- **PCI Security Standards Council (SSC):** A group comprising Visa, MasterCard, American Express, Discover, and JCB that maintains, evolves, and promotes PCI DSS. See also *Payment Card Industry Data Security Standards (PCI DSS)*.
- **PDU:** See *protocol data unit (PDU)*.
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** A Canadian privacy law that defines individual rights with respect to the privacy of their personal information, and governs how private sector organizations collect, use, and disclose personal information in the course of business.
- **Personally identifiable information (PII):** Defined by the U.S. National Institute of Standards and Technology (NIST) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity... and (2) any other information that is linked or linkable to an individual...."
- **Pharming:** A type of attack that redirects a legitimate website's traffic to a fake site.
- **PHI:** See *protected health information (PHI)*.
- **PII:** See *personally identifiable information (PII)*.
- **PIPEDA:** See *Personal Information Protection and Electronic Documents Act (PIPEDA)*.
- **PKI:** See *public key infrastructure (PKI)*.
- **Platform as a service (PaaS):** A cloud computing service model in which customers can deploy supported applications onto the provider's cloud infrastructure, but the customer has no knowledge of, and does not manage or control, the underlying cloud infrastructure. The customer has control over the deployed applications and limited configuration settings for the application-hosting environment. The company owns the deployed applications and data, and it is therefore responsible for the security of those applications and data.
- **Playbooks:** Task-based graphic workflows that help visualize processes across security products. Playbooks can be fully automated, fully manual, or anywhere in between. Also known as runbooks.
- **PoE:** See *Power over Ethernet (PoE)*.
- **Point-to-Point Protocol (PPP):** A Layer 2 (Data Link) protocol layer used to establish a direct connection between two nodes.

- **Point-to-Point Tunneling Protocol (PPTP):** An obsolete method for implementing virtual private networks, with many known security issues, that uses a TCP control channel and a GRE tunnel to encapsulate PPP packets. See also *Transmission Control Protocol (TCP)*, *Generic Routing Encapsulation (GRE)*, and *Point-to-Point Protocol (PPP)*.
- **Polymorphism:** A programming technique used to alter a part of malware code with every iteration, to avoid detection by signature-based anti-malware software. For example, an encryption key or decryption routine may change with every iteration, but the malware payload remains unchanged. See also *metamorphism*.
- **POP3:** See *Post Office Protocol Version 3 (POP3)*.
- **Post Office Protocol Version 3 (POP3):** An email retrieval protocol that allows an email client to access emails on a remote email server.
- **Power over Ethernet (PoE):** A network standard that provides electrical power to certain network devices over Ethernet cables.
- **PPP:** See *Point-to-Point Protocol (PPP)*.
- **PPTP:** See *Point-to-Point Tunneling Protocol (PPTP)*.
- **Pre-shared key (PSK):** A shared secret, used in symmetric key cryptography that has been exchanged between two parties communicating over an encrypted channel.
- **Private cloud:** A cloud computing model that consists of a cloud infrastructure that is used exclusively by a single organization.
- **Product integrations (or apps):** Mechanisms through which SOAR platforms communicate with other products. These integrations can be executed through REST APIs, webhooks, and other techniques. An integration can be unidirectional or bidirectional, with the latter allowing both products to execute cross-console actions. See also *security orchestration, automation, and response (SOAR)*, *representational state transfer (REST)*, and *application programming interface (API)*.
- **Protect surface:** In a Zero Trust architecture, the protect surface consists of the most critical and valuable data, assets, application, and services (DAAS) on a network.
- **Protected health information (PHI):** Defined by HIPAA as information about an individual's health status, provision of healthcare, or payment for healthcare that includes identifiers such as names, geographic identifiers (smaller than a state), dates, phone and fax numbers, email addresses, Social Security numbers, medical record numbers, or photographs. See also *Health Insurance Portability and Accountability Act (HIPAA)*.
- **Protocol data unit (PDU):** A self-contained unit of data (consisting of user data or control information and network addressing).
- **PSK:** See *pre-shared key (PSK)*.
- **Public cloud:** A cloud computing deployment model that consists of a cloud infrastructure that is open to use by the general public.
- **Public key infrastructure (PKI):** A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public key encryption.
- **QoS:** See *quality of service (QoS)*.
- **Quality of service (QoS):** The overall performance of specific applications or services on a network including error rate, bit rate, throughput, transmission delay, availability, jitter, etc. QoS policies can be configured on certain network and security devices to prioritize certain traffic, such as voice or video, over other, less performance-intensive traffic, such as file transfers.
- **RADIUS:** See *Remote Authentication Dial-In User Service (RADIUS)*.
- **Rainbow table:** A precomputed table used to find the original value of a cryptographic hash function.

- **RARP:** See *Reverse Address Resolution Protocol (RARP)*.
- **RASP:** See *runtime application self-protection (RASP)*.
- **RBAC:** See *role-based access control (RBAC)*.
- **Recursive DNS query:** A DNS query that is performed (if the DNS server allows recursive queries) when a DNS server is not authoritative for a destination domain. The non-authoritative DNS server obtains the IP address of the authoritative DNS server for the destination domain and sends the original DNS request to that server to be resolved. See also *Domain Name System (DNS)* and *authoritative DNS server*.
- **Remote Authentication Dial-In User Service (RADIUS):** A client-server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize access to a system or service.
- **Remote Procedure Call (RPC):** An inter-process communication (IPC) protocol that enables an application to be run on a different computer or network, rather than on the local computer on which it is installed.
- **Repeater:** A network device that boosts or retransmits a signal to physically extend the range of a wired or wireless network.
- **Representational state transfer (REST):** An architectural programming style that typically runs over HTTP and is commonly used for mobile apps, social networking websites, and mashup tools. See also *Hypertext Transfer Protocol (HTTP)*.
- **REST:** See *representational state transfer (REST)*.
- **Reverse Address Resolution Protocol (RARP):** A protocol that translates a physical MAC address to a logical address. See also *media access control (MAC) address*.
- **Ring topology:** A LAN topology in which all nodes are connected in a closed loop that forms a continuous ring. In a ring topology, all communication travels in a single direction around the ring. Ring topologies were common in token ring networks. See also *local-area network (LAN)*.
- **Role-based access control (RBAC):** A method for implementing discretionary access controls in which access decisions are based on group membership according to organizational or functional roles.
- **Rooting:** The Google Android equivalent of jailbreaking. See *jailbreaking*.
- **Router:** A network device that sends data packets to a destination network along a network path.
- **RPC:** See *remote procedure call (RPC)***.**
- **Runtime application self-protection (RASP):** Technology that detects attacks against an application in real time. RASP continuously monitors an app's behavior and the context of behavior to immediately identify and prevent malicious activity.
- **SaaS:** See *software as a service (SaaS)*.
- **Salt:** Randomly generated data that is used as an additional input to a one-way hash function that hashes a password or passphrase. The same original text hashed with different salts results in different hash values. See also *one-way hash function*.
- **Sarbanes-Oxley (SOX) Act:** A U.S. law that increases financial governance and accountability in publicly traded companies.
- **SASE:** See *Secure Access Service Edge (SASE)*.
- **SCM:** See *software configuration management (SCM)*.
- **Script kiddie:** Someone with limited hacking and/or programming skills that uses malicious programs (malware) written by others to attack a computer or network. See also *malware*.
- **SCTP:** See *Stream Control Transmission Protocol (SCTP)*.
- **SD-WAN:** See *software-defined wide-area network (SD-WAN)*.

- **Secure Access Service Edge (SASE):** An integrated solution that provides consistent networking and security services and access to cloud applications delivered through a common framework.
- **Secure Shell (SSH):** A more secure alternative to Telnet for remote access. SSH establishes an encrypted tunnel between the client and the server and can also authenticate the client to the server. See also *telnet*.
- **Secure Sockets Layer (SSL):** A cryptographic protocol for managing authentication and encrypted communication between a client and server to protect the confidentiality and integrity of data exchanged in the session.
- **Secure web gateway (SWG):** A security platform or service that is designed to maintain visibility in web traffic. Additional functionality may include web content filtering.
- **Security orchestration, automation, and response (SOAR):** Technology that helps coordinate, execute, and automate tasks between various people and tools, allowing companies to respond quickly to cybersecurity attacks and improve their overall security posture. SOAR tools use playbooks to automate and coordinate workflows that may include any number of disparate security tools and human tasks. See also *playbook*.
- **Serverless:** Generally refers to an operational model in cloud computing in which applications rely on managed services that abstract away the need to manage, patch, and secure infrastructure and virtual machines. Serverless applications rely on a combination of managed cloud services and FaaS offerings. See also *function as a service (FaaS)*.
- **Service set identifier (SSID):** A case sensitive, 32-character alphanumeric identifier that uniquely identifies a Wi-Fi network.
- **Session Initiation Protocol (SIP):** An open signaling protocol standard for establishing, managing, and terminating real-time communications such as voice, video, and text over large IP-based networks.
- **Simple Mail Transfer Protocol (SMTP):** A protocol used to send and receive email across the internet.
- **Simple Network Management Protocol (SNMP):** A protocol used to collect information by polling stations and sending traps (or alerts) to a management station.
- **SIP:** See *Session Initiation Protocol (SIP)*.
- **SMTP:** See *Simple Mail Transfer Protocol (SMTP)*.
- **SNMP:** See *Simple Network Management Protocol (SNMP)*.
- **SOAR:** See *security orchestration, automation, and response (SOAR)*.
- **Software as a service (SaaS):** A category of cloud computing services in which the customer is provided access to a hosted application maintained by the service provider.
- **Software-defined wide-area network (SD-WAN):** A virtualized service that separates the network control and management processes from the underlying hardware in a wide-area network, and makes them available as software.
- **Software configuration management (SCM):** The task of tracking and controlling changes in software.
- **SONET:** See *synchronous optical networking (SONET)*.
- **SOX:** See *Sarbanes-Oxley (SOX) Act*.
- **Spear phishing:** A highly targeted phishing attack that uses specific information about the target to make the phishing attempt appear legitimate.
- **SSH:** See *Secure Shell (SSH)*.
- **SSID:** See *service set identifier (SSID)*.
- **SSL:** See *Secure Sockets Layer (SSL)*.
- **STIX:** See *Structured Threat Information Expression (STIX)*.

- **Stream Control Transmission Protocol (SCTP):** A message-oriented protocol (similar to UDP) that ensures reliable, in-sequence transport with congestion control (similar to TCP). See also *User Datagram Protocol (UDP)* and *Transmission Control Protocol (TCP)*.
- **Structured Threat Information Expression (STIX):** An XML format for conveying data about cybersecurity threats in a standardized format. See also *Extensible Markup Language (XML)*.
- **Subnet mask:** A number that hides the network portion of an IPv4 address, leaving only the host portion of the IP address. See also *Internet Protocol (IP) address*.
- **Subnetting:** A technique used to divide a large network into smaller, multiple subnetworks.
- **Supernetting:** A technique used to aggregate multiple contiguous smaller networks into a larger network to enable more efficient internet routing.
- **SWG:** See *secure web gateway (SWG)*.
- **Switch:** An intelligent hub that forwards data packets only to the port associated with the destination device on a network.
- **Synchronous optical networking (SONET):** A protocol that transfers multiple digital bit streams synchronously over optical fiber.
- **T-carrier:** A full-duplex digital transmission system that uses multiple pairs of copper wire to transmit electrical signals over a network. For example, a T-1 circuit consists of two pairs of copper wire – one pair transmits, the other pair receives – that are multiplexed to provide a total of 24 channels, each delivering 64Kbps of data, for a total bandwidth of 1.544Mbps.
- **TCP:** See *Transmission Control Protocol (TCP)*.
- **TCP segment:** A PDU defined at the Transport layer of the OSI model. See also *protocol data unit (PDU)* and *Open Systems Interconnection (OSI) model*.
- **TCP/IP model:** See *Transmission Control Protocol/Internet Protocol (TCP/IP) model*.
- **Technical debt:** A software development concept, which has also been applied more generally to IT, in which additional future costs are anticipated for rework due to an earlier decision or course of action that was necessary for agility, but not necessarily the most optimal or appropriate decision or course of action.
- **Telnet:** A terminal emulator used to provide remote access to a system.
- **Three-way handshake:** A sequence used to establish a TCP connection. For example, a PC initiates a connection with a server by sending a TCP SYN (Synchronize) packet. The server replies with a SYN ACK packet (Synchronize Acknowledgment). Finally, the PC sends an ACK or SYN-ACK-ACK packet, acknowledging the server's acknowledgement, and data communication commences. See also *Transmission Control Protocol (TCP)*.
- **Threat vector:** See *attack vector*.
- **TLD:** See *top-level domain (TLD)*.
- **TLS:** See *Transport Layer Security (TLS)*.
- **Top-level domain (TLD):** The highest-level domain in DNS, represented by the last part of a FQDN (for example, .com or .edu). The most commonly used TLDs are generic top-level domains (gTLD) such as .com, edu, .net, and .org, and country-code top-level domains (ccTLD) such as .ca and .us. See also *Domain Name System (DNS)*.
- **Transmission Control Protocol (TCP):** A connection-oriented (a direct connection between network devices is established before data segments are transferred) protocol that provides reliable delivery (received segments are acknowledged and retransmission of missing or corrupted segments is requested) of data.
- **Transmission Control Protocol/Internet Protocol (TCP/IP) model:** A four-layer networking model consisting of the Application (Layer 4 or L4), Transport (Layer 3 or L3), Internet (Layer 2 or L2), and Network Access (Layer 1 or L1) layers.
- **Transport Layer Security (TLS):** The successor to SSL (although it still is commonly referred to as SSL). See also *Secure Sockets Layer (SSL)*.

- **Type 1 hypervisor:** See *native hypervisor*.
- **Type 2 hypervisor:** See *hosted hypervisor*.
- **UDP:** See *User Datagram Protocol (UDP)*.
- **UDP datagram:** A PDU defined at the Transport layer of the OSI model. See also *protocol data unit* (PDU), *User Datagram Protocol (UDP)*, and *Open Systems Interconnection (OSI) model*.
- **UEBA:** See *user and entity behavior analytics (UEBA)*.
- **User and entity behavior analytics (UEBA):** A type of cybersecurity solution or feature that discovers threats by identifying activity that deviates from a normal baseline.
- **Uniform resource identifier (URI):** A string of characters that uniquely identifies a resource, using a predefined syntax in a hierarchical naming scheme.
- **Uniform resource locator (URL):** A unique reference (or address) to an internet resource, such as a web page.
- **URI:** See *uniform resource identifier (URI)*.
- **URL:** See *uniform resource locator (URL)*.
- **User Datagram Protocol (UDP):** A connectionless (a direct connection between network devices is not established before datagrams are transferred) protocol that provides best-effort delivery (received datagrams are not acknowledged and missing or corrupted datagrams are not requested) of data.
- **Variable-length subnet masking (VLSM):** A technique that enables IP address spaces to be divided into different sizes. See also *Internet Protocol (IP) address*.
- **Virtual local-area network (VLAN):** A logical network that is created within a physical local-area network.
- **Virtual machine (VM):** An emulation of a physical (hardware) computer system, including CPU, memory, disk, operating system, network interfaces, etc.
- **Virtual reality (VR):** A simulated digital experience.
- **VLAN:** See *virtual local-area network (VLAN)*.
- **VLSM:** See *variable-length subnet masking (VLSM)*.
- **VM:** See *virtual machine (VM)*.
- **Voice over Internet Protocol (VoIP):** Technology that provides voice communication over an Internet Protocol (IP)-based network. Also known as IP telephony.
- **VoIP:** See *Voice over Internet Protocol (VoIP)*.
- **VR:** See *virtual reality (VR)*.
- **Vulnerability:** A bug or flaw that exists in a system or software and creates a security risk.
- **WAN:** See *wide-area network (WAN)*.
- **Watering hole:** An attack that compromises websites that are likely to be visited by a targeted victim to deliver malware via a drive-by download. See also *drive-by download*.
- **Web 2.0:** A term popularized by Tim O'Reilly and Dale Dougherty unofficially referring to a new era of the World Wide Web, which is characterized by dynamic or user-generated content, interaction, and collaboration, and the growth of social media. See also *Enterprise 2.0*.
- **Web 3.0:** As defined on ExpertSystem.com, Web 3.0 is characterized by the following five characteristics: semantic web, artificial intelligence, 3D graphics, connectivity, and ubiquity.
- **Whaling:** A type of spear phishing attack that is specifically directed at senior executives or other high-profile targets within an organization. See also *spear phishing*.
- **Wide-area network (WAN):** A computer network that connects multiple LANs or other WANs across a relatively large geographic area, such as a small city, a region or country, a

global enterprise network, or the entire planet (for example, the internet). See also *local-area network (LAN)*.

- **Wireless repeater:** A device that rebroadcasts the wireless signal from a wireless router or AP to extend the range of a Wi-Fi network.
- **XML:** See *Extensible Markup Language (XML)*.
- **XOR:** See *exclusive or (XOR)*.
- **XR:** See *extended reality (XR)*.
- **Zero-day threat:** The window of vulnerability that exists from the time a new (unknown) threat is released until security vendors release a signature file or security patch for the threat.
- **Zombie:** See *bot*.

Continuing Your Learning Journey with Palo Alto Networks

Training from Palo Alto Networks and our Authorized Training Partners delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications give you the Palo Alto Networks product portfolio knowledge necessary to prevent successful cyberattacks and to safely enable applications.

Digital Learning

For those of you who want to keep up to date on our technology, a learning library of *free* digital learning is available. These on-demand, self-paced digital-learning classes are a helpful way to reinforce the key information for those who have been to the formal hands-on classes. They also serve as a useful overview and introduction to working with our technology for those unable to attend a hands-on, instructor-led class.

Simply register in Beacon and you will be given access to our digital-learning portfolio. These online classes cover foundational material and contain narrated slides, knowledge checks, and, where applicable, demos for you to access.

New courses are being added often, so check back to see new curriculum available.

Instructor-Led Training

Looking for a hands-on, instructor-led course in your area?

Palo Alto Networks Authorized Training Partners (ATPs) are located globally and offer a breadth of solutions from onsite training to public, open-environment classes. About 42 authorized training centers are delivering online courses in 14 languages and at convenient times for most major markets worldwide. For class schedule, location, and training offerings, see https://www.paloaltonetworks.com/services/education/atc-locations.

Learning Through the Community

You also can learn from peers and other experts in the field. Check out our communities site at https://live.paloaltonetworks.com, where you can:

- Discover reference material
- Learn best practices
- Learn what is trending

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com