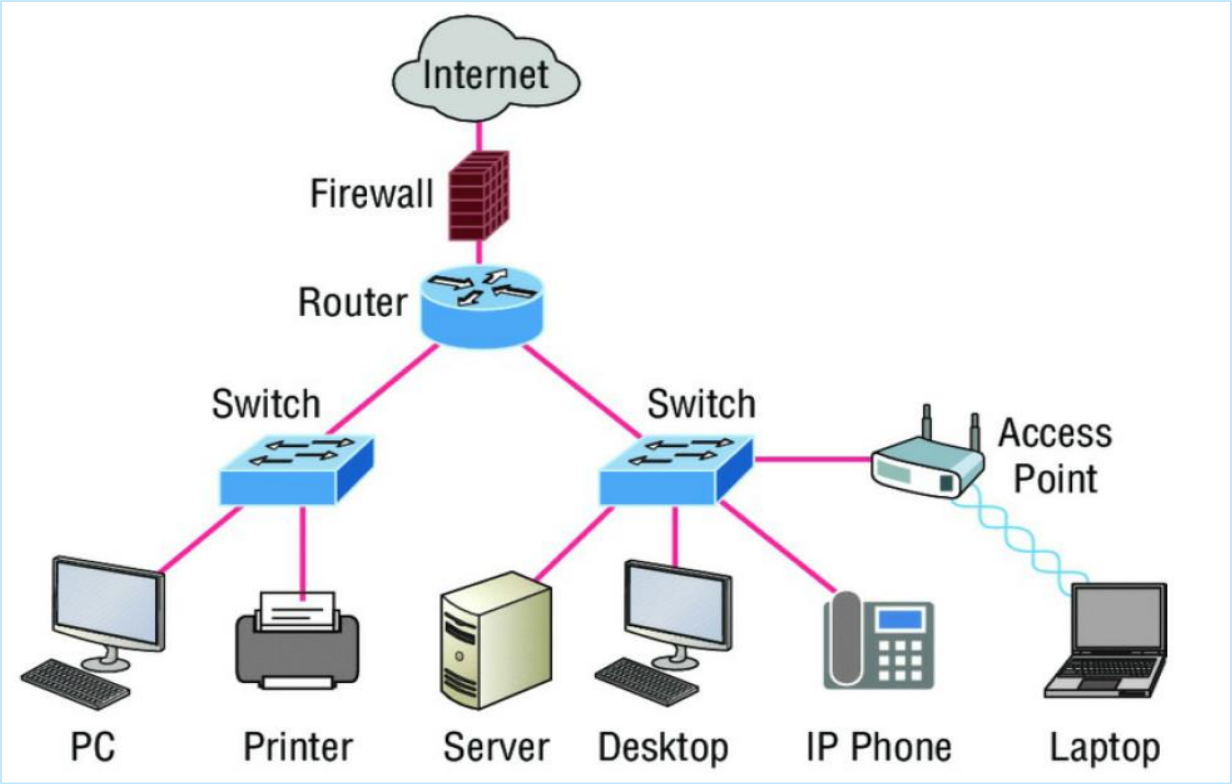
NETWORK & INFRASTRUCTURE SECURITY

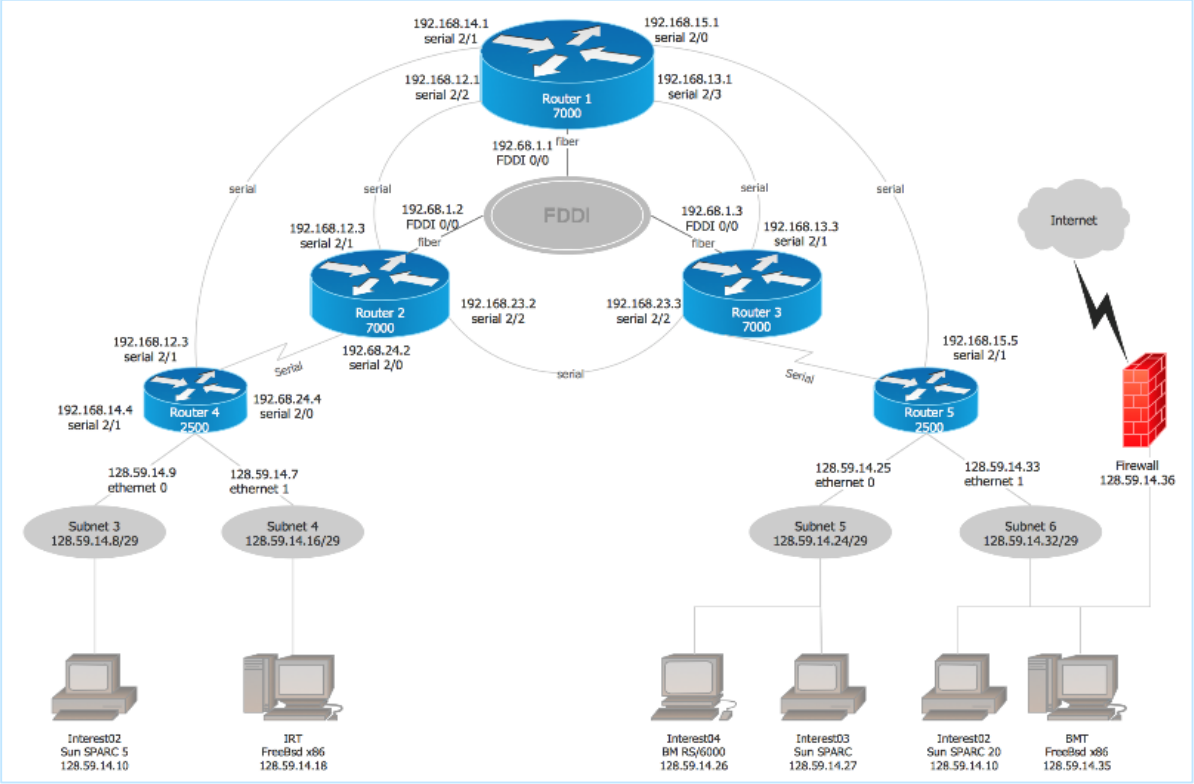
Topics

- Basic of Networks
- OSI Model & TCP IP Protocol Suite
- Introduction to network devices & functionality
- Network Security
- Perimeter Security
- Host & End Point Security
- Security challenges in the boundaryless Organization
- Mobile Security
- References

Basics of Networks

A network is a collection of computers / servers / network devices / peripherals or other devices connected to one another to allow the sharing of data.





Basics of Networks

❑ Local Area Network (LAN)

- ✓Is limited in size, typically spanning a few hundred meters, and no more than a mile
- ✓Is fast, with speeds from 10 Mbps to 10 Gbps
- ✓Requires little wiring, typically a single cable connecting to each device or Wireless Connection.

❑ Metropolitan Area Network (MAN)

- ✓Acts a high speed network to allow sharing of regional resources.
- ✓Typically covers an area of between 5 and 50 km diameter.
- ✓Example: Telephone company network that provides a high speed DSL to customers.

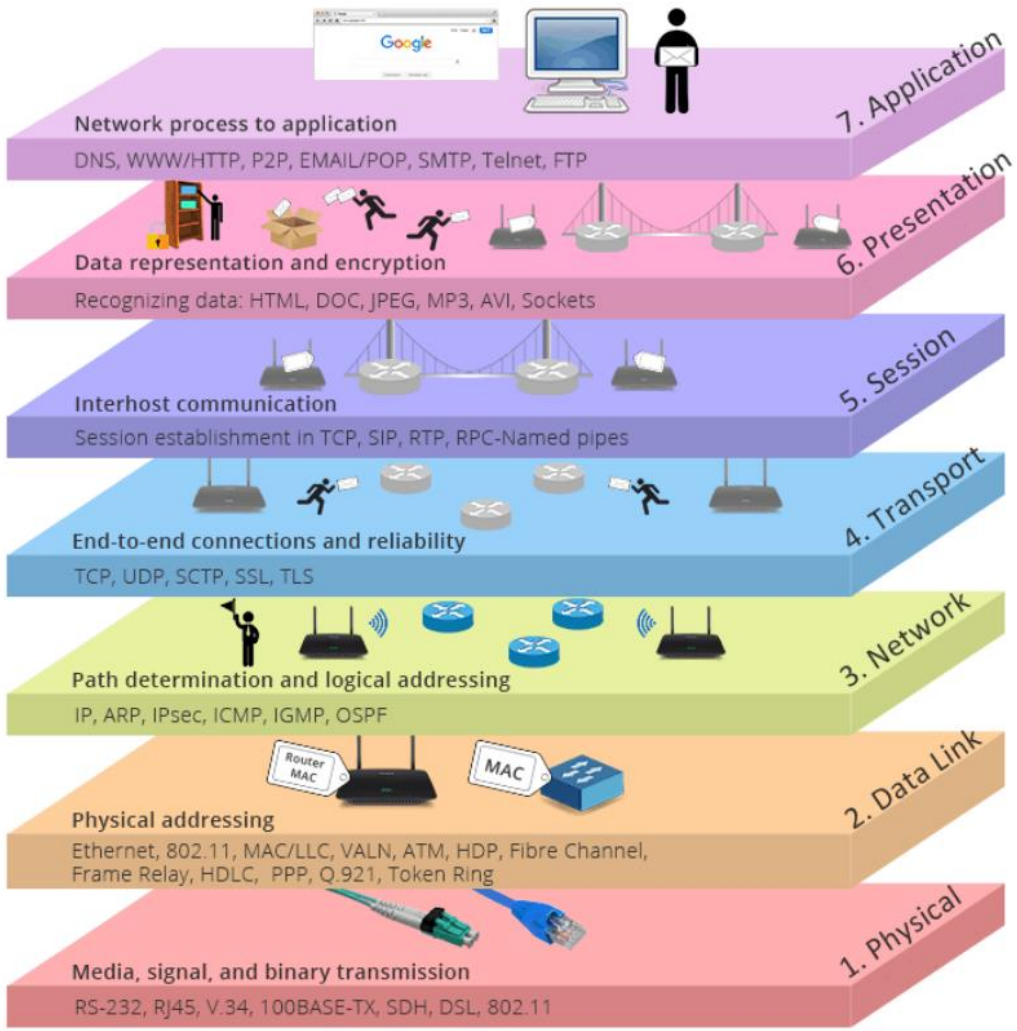
❑ Wide Area Network (WAN)

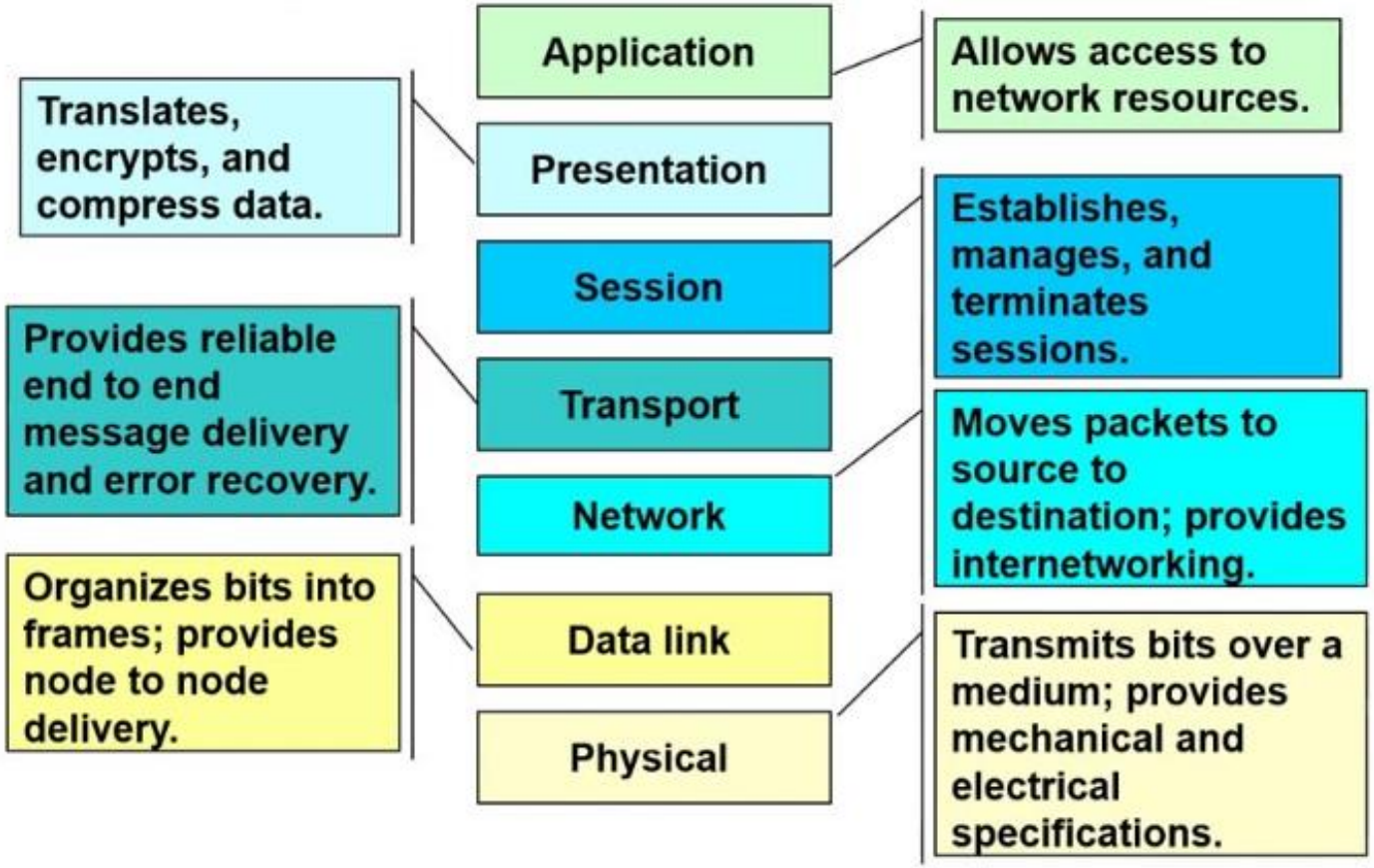
- ✓Covers a large geographic area such as country, continent or even whole of the world.
- ✓Example: ISP Networks

❑ Personal Area Network (PAN)

- ✓A network that is used for communicating among computers and computer devices (including telephones) in close proximity of around a few meters within a room.

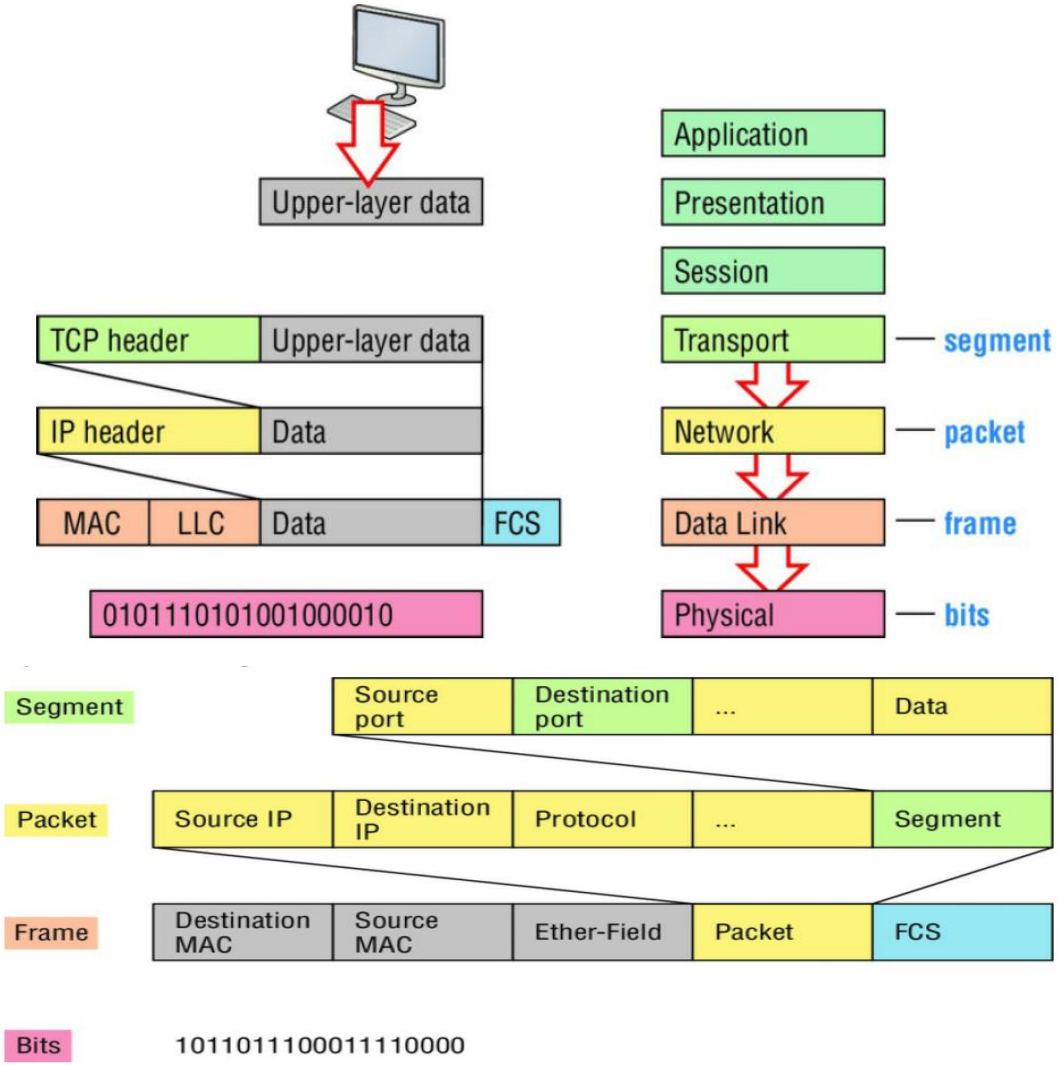
OSI Model


Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
Router MAC
MAC
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11


Translates, encrypts, and compress data.
Provides reliable end to end message delivery and error recovery.
Organizes bits into frames; provides node to node delivery.
Application
Presentation
Session
Transport
Network
Data link
Physical
Allows access to network resources.
Establishes, manages, and terminates sessions.
Moves packets to source to destination; provides internetworking.
Transmits bits over a medium; provides mechanical and electrical specifications.

Basics of Networks

PDU and layer addressing



Protocols at OSI Layers

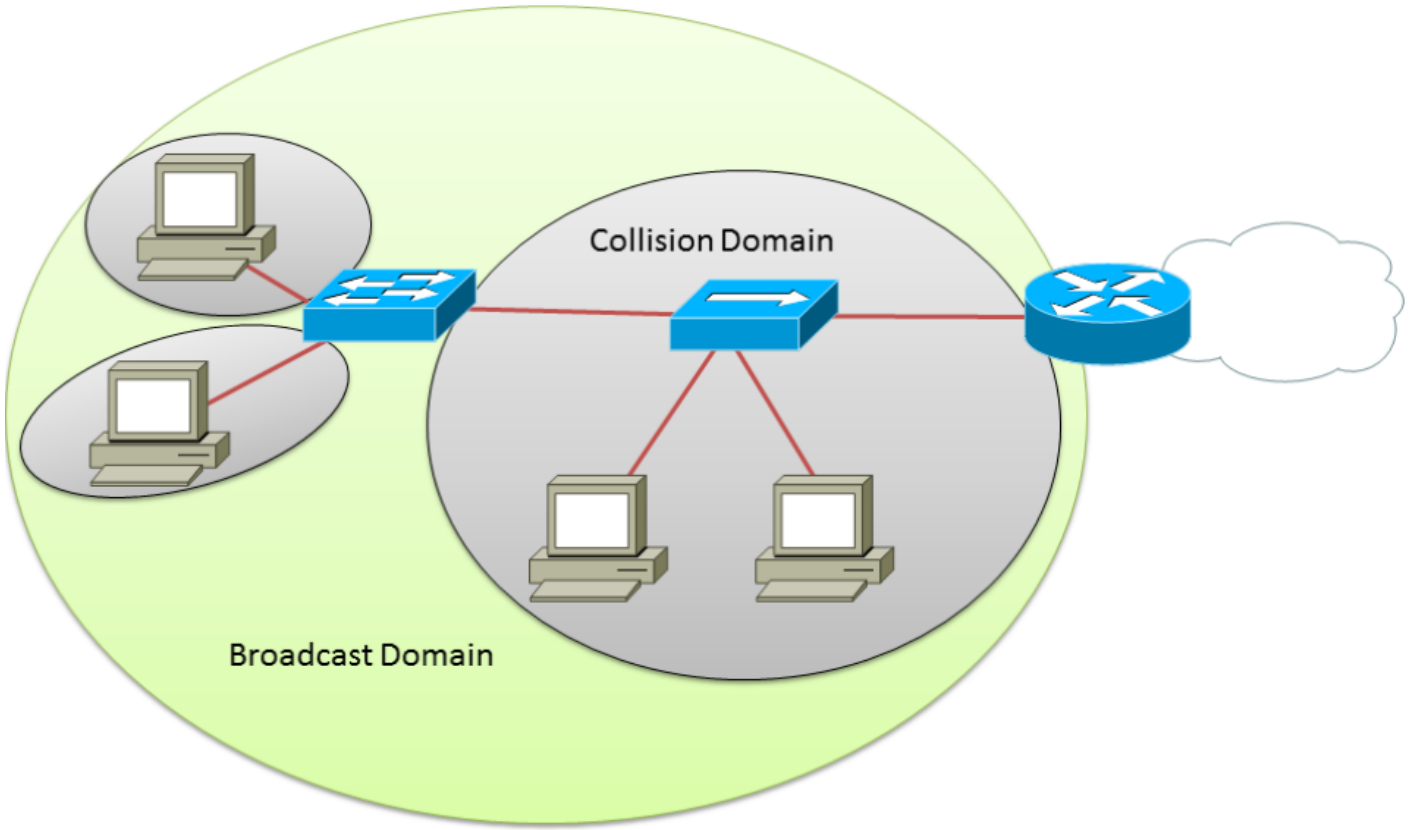
OSI Model	Protocols
Application Layer	DNS, DHCP, FTP, HTTPS, IMAP, LDAP, NTP, POP3, RTP, RTSP, SSH, SIP, SMTP, SNMP, Telnet, TFTP
Presentation Layer	JPEG, MIDI, MPEG, PICT, TIFF
Session Layer	NetBIOS, NFS, PAP, SCP, SQL, ZIP
Transport Layer	TCP, UDP
Network Layer	ICMP, IGMP, IPsec, IPv4, IPv6, IPX, RIP
Data Link Layer	ARP, ATM, CDP, FDDI, Frame Relay, HDLC, MPLS, PPP, STP, Token Ring
Physical Layer	Bluetooth, Ethernet, DSL, ISDN, 802.11 Wi-Fi

Collision domains:

A collision domain is a section of a network connected by a shared medium or through repeaters where data packets can collide with one another when being sent, particularly when using early versions of Ethernet.

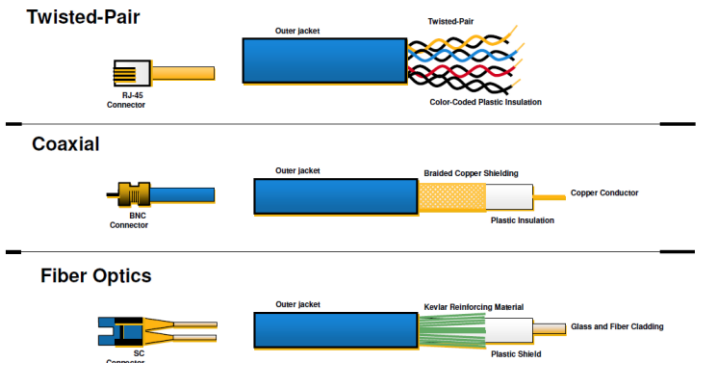
Broadcast domains:

A Broadcast Domain consists of all the devices that will receive any broadcast packet originating from any device within the network segment.



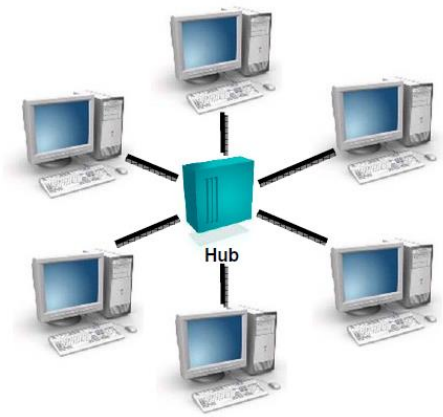
Basics of Networks

Physical Media Types



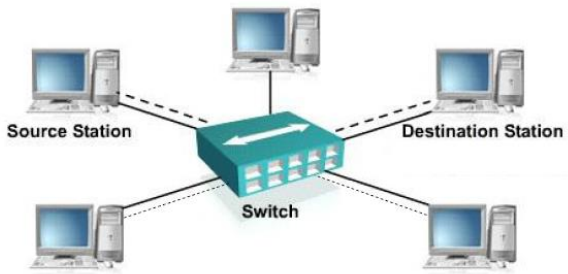
Hub

A hub (concentrator) is a device that repeats the signals it receives on one port to all other ports. It is a central connection point for several network devices.



Switch

When a switch receives data the switch examines the data link header for the MAC address of the destination station and forwards it to the correct port. This opens a path between ports that can use the full bandwidth of the topology.

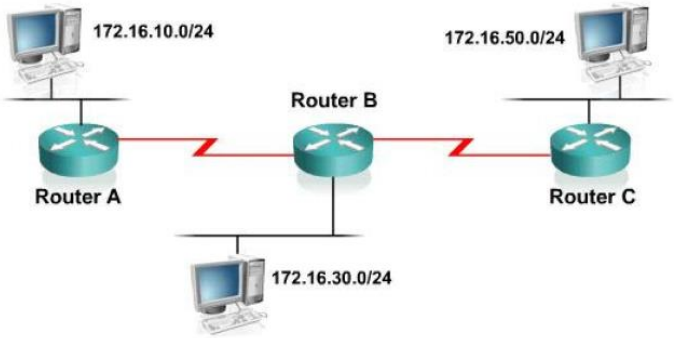


Router

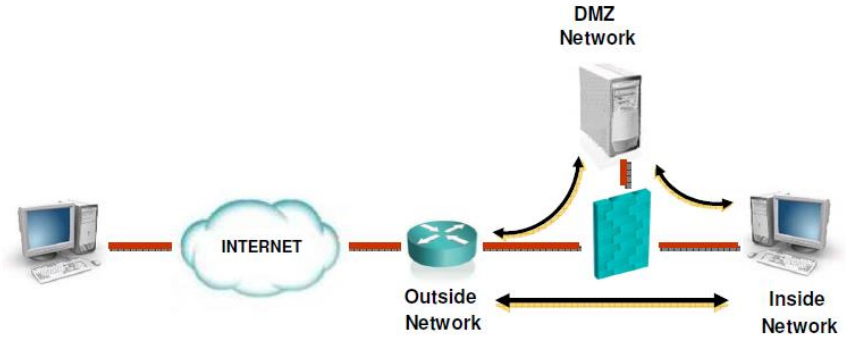
The devices that operate at the Network layer are routers and Layer 3 Switches

Router

Layer 3 Switch



Firewall

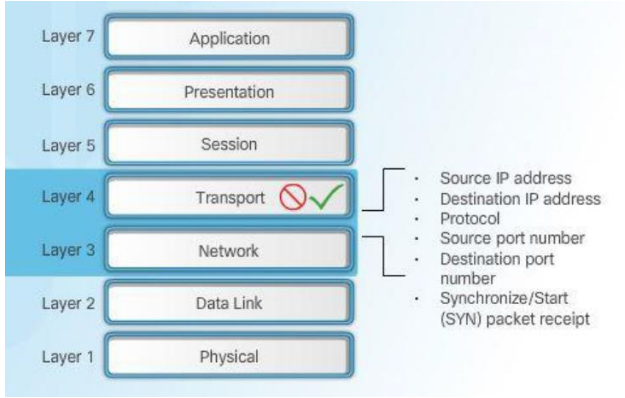


Recap and Questions

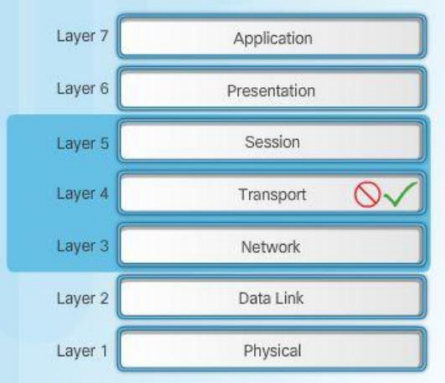
NETWORK SECURITY - FIREWALLS

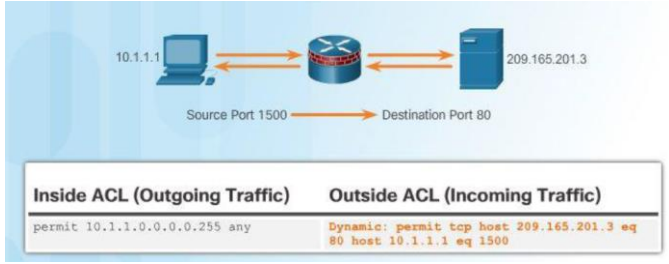
Firewalls

Packet Filtering

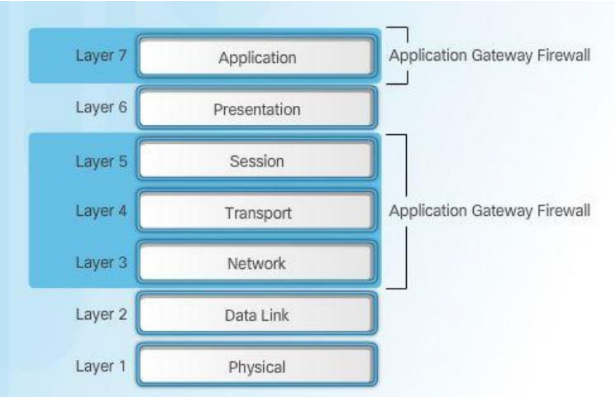


Stateful Firewalls

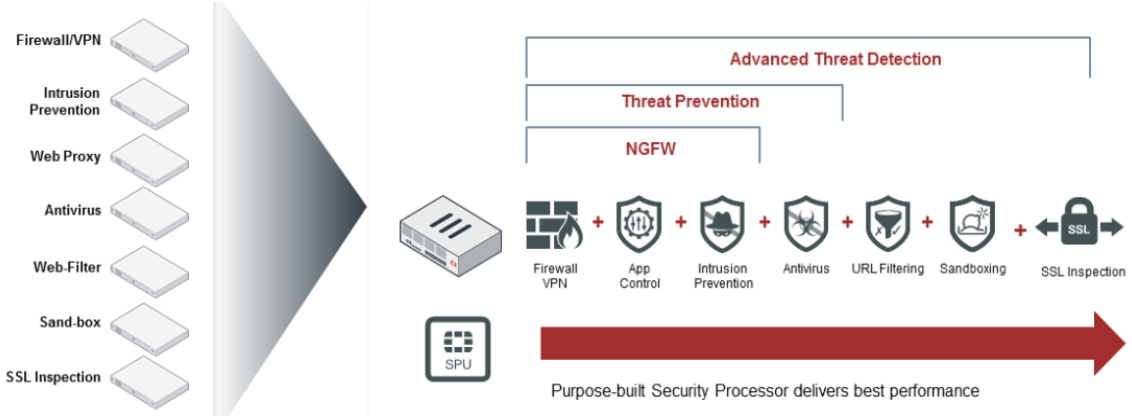




Application Gateways



Next –Gen Firewalls , UTM



Traditional Firewall - Shortcomings

- Legacy firewalls were built on the assumption that an application would respect its protocol which would respect the port.

  For example, Port 80 must mean HTTP and that must mean Web browsing.
  Port 25 must mean SMTP and that must mean e-mail.

- Modern applications are deliver content using a wide range / random ports.

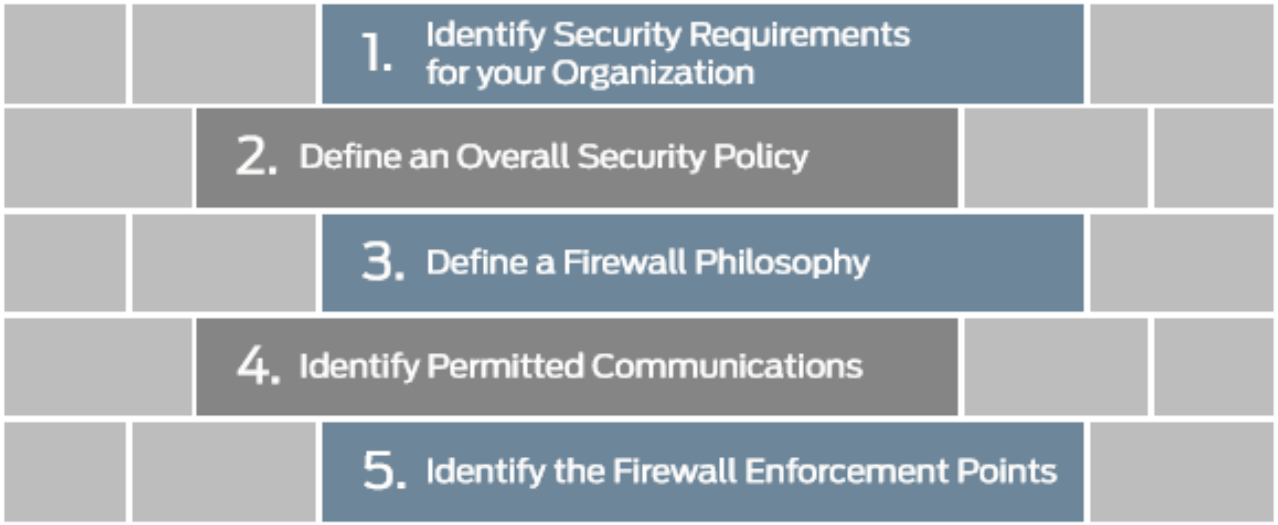
- Its easy to mimic an application and tunnel harmful content.

- Lacked intelligence to distinguish different kinds of web traffic.

- Operation was limited to Data Link and Transport layers of network operation. As a result, firewall software could identify and control traffic (moving data) but not analyze it.

Firewalls

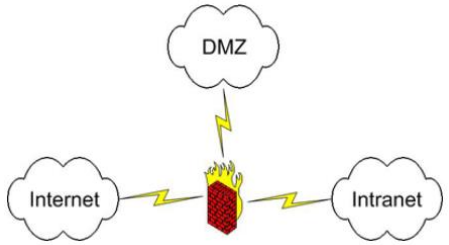
Best Practices for Firewall Design



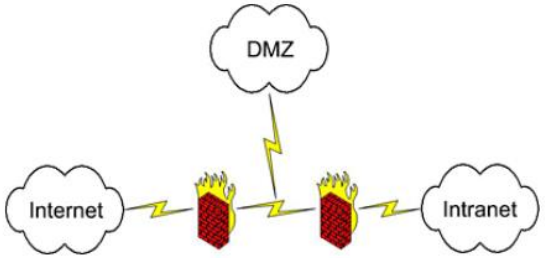
General Deployment Modes

Bastion Host

Screened Subnet

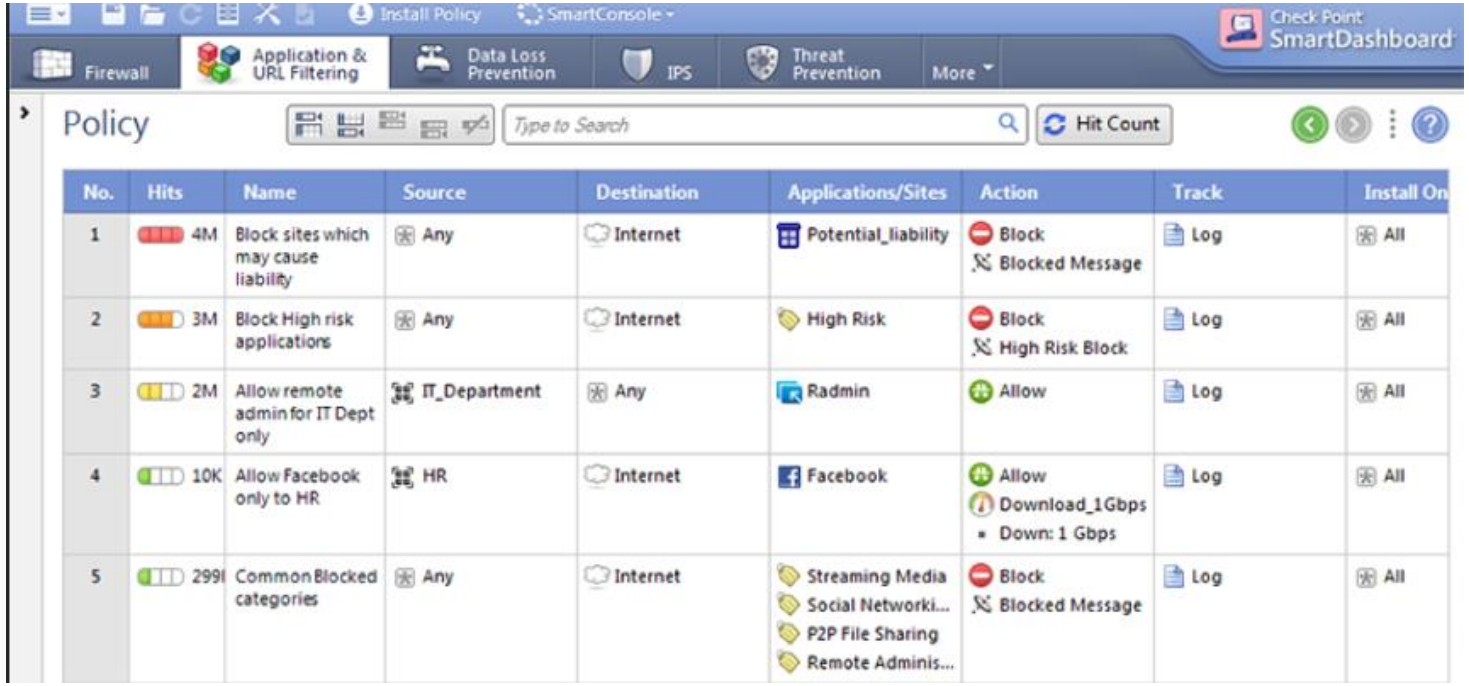


Multi-homed firewall



Policy Samples - NGFWs

			Source				Destination						
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Addr...	Application	Service	Action	Profile	Options
1	Rule B	none	Trust	192.168.1.3	any	any	Untrust	any	dns ftp web-browsing	application-default		none	
2	Rule C	none	Trust	192.168.1.3	any	any	Untrust	any	any	any		none	
3	Rule A	none	Trust	any	any	any	Untrust	any	any	any		none	
4	Rule D	none	Untrust	any	any	any	any	any	any	any		none	



Policy Samples - NGFWs

Overview | Analysis | **Policies** | Devices | Health | System | Help | jlamar

Intrusion | **Access Control** | Network Discovery | Custom Applications | Users | Correlation | Actions

Interesting Use Cases

Enter a description

Save | Cancel | Save and Apply | Add Category | Add Rule | Search Rules

Device Targets: 0 devices

#	Name	Source Zones	Dest Zones	Sou... Net...	Dest Net...	VLA...	U...	Applications	Services	URLs	Action			
Administrator Rules														
This category is empty.														
Standard Rules														
1	Mobile Security 1	Intern	any	any	Ten	any	any	Android browser Blackberry browser Mobile Safari	any	any	Block		1	
2	Read Only Facebook	Intern	Exter	any	any	any	any	Facebook Status Update Facebook Send Email Facebook Comment Facebook Chat Tags: Facebook game; Fill	any	any	Block		0	
3	Web Block List	Intern	Exter	any	any	any	any	any	any	Adult and Pornography (Any Reputation) Bot Nets (Any Reputation) Confirmed SPAM Sources (Any Reputati Gambling (Any Reputation) (13 more...)	Block		0	
4	Block All P2P	Intern	Exter	any	any	any	any	Categories: peer to peer	any	any	Block		0	
5	Inbound Email	Exter	Intern	any	any	any	any	SMTP	SMTP	any	Allow		0	
6	Outbound Web Browsing	Exter	Intern	any	any	any	any	HTTP	any	any	Allow		0	
Root Rules														
This category is empty.														
Default Action										Access Control: Block All Traffic				

1 Row Selected

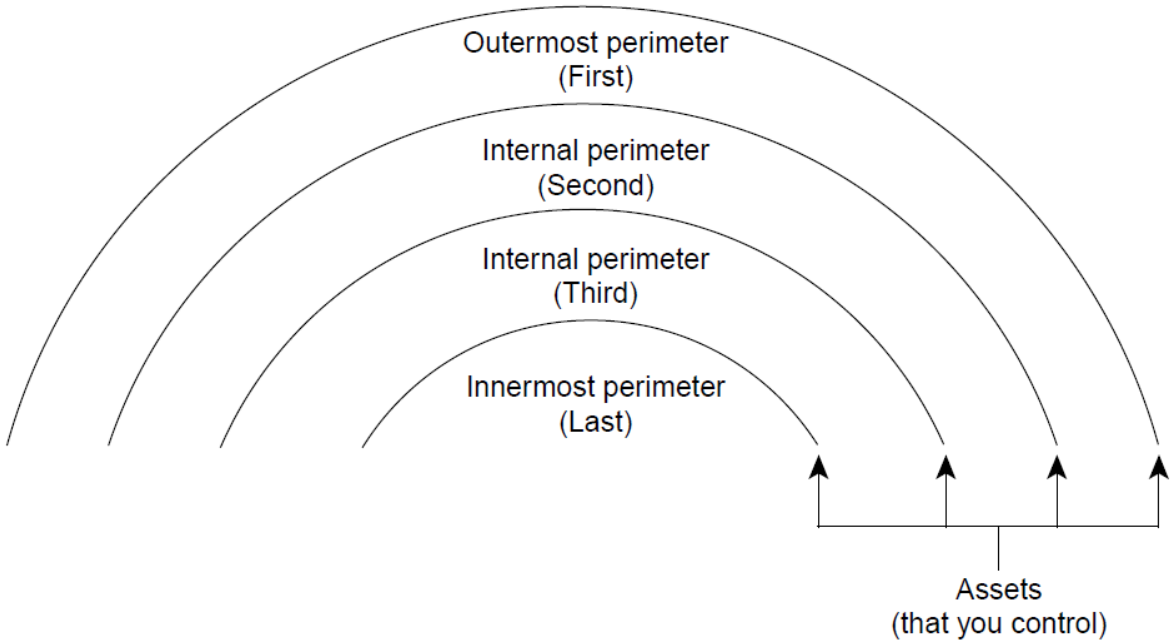
Displaying 1 - 6 of 6 rules | Page 1 of 1

Recap and Questions

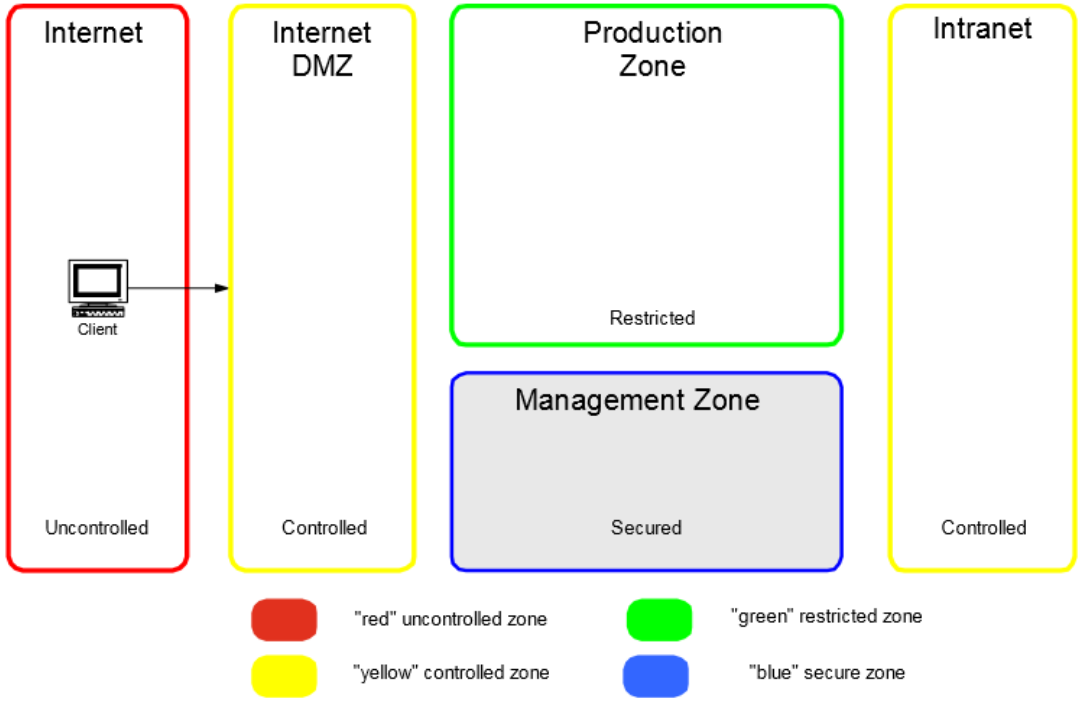
PERIMETER SECURITY

Perimeter Security

Traditional Perimeters



Typical Network Zones



Perimeter Protection Technologies

- ❑ Firewalls
- ❑ Intrusion Detection and Prevention Systems (IDS/IDPS)
- ❑ DLP – Data Loss Prevention

Perimeter Security

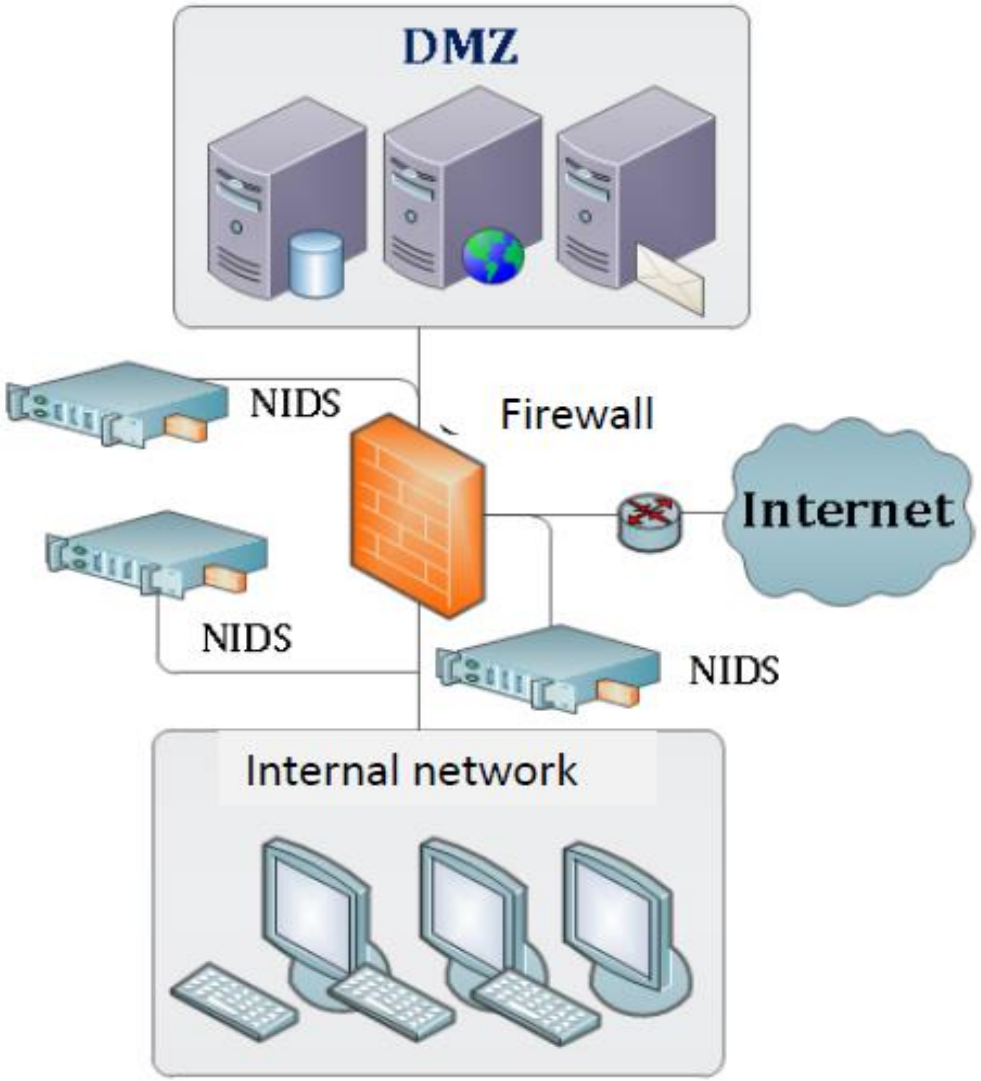
Intrusion Detection and Prevention Systems (IDS/IDPS)

Two types of IDS:

- ❑ HIDS: Host IDS, monitor changes in the operating system and software
- ❑ NIDS: Network IDS, monitor network traffic

Two common detection methods:

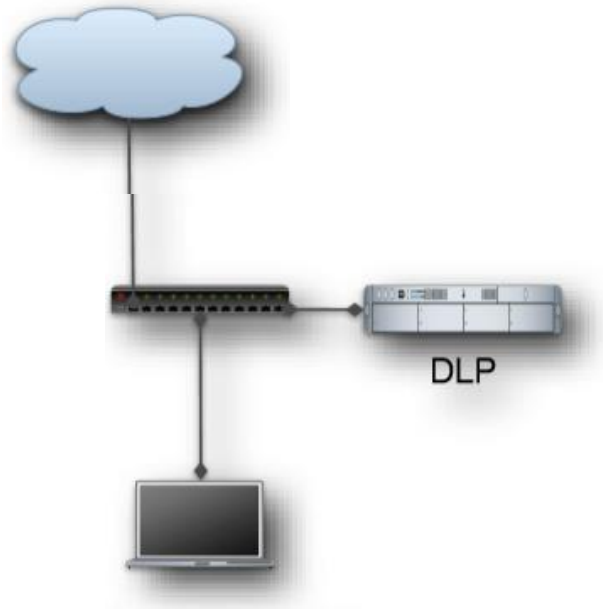
- ❑ Signatures
- ❑ Behavior patterns



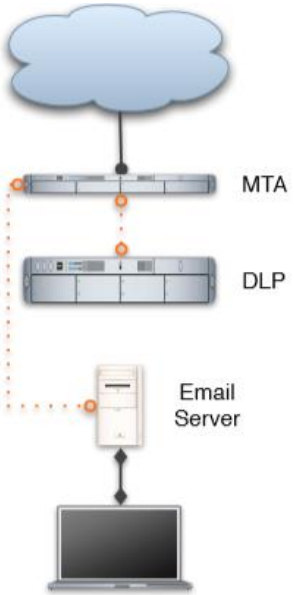
Data Loss Prevention- DLP

- ❑ To accurately identify sensitive data in its many forms
- ❑ To prevent the loss of that data.

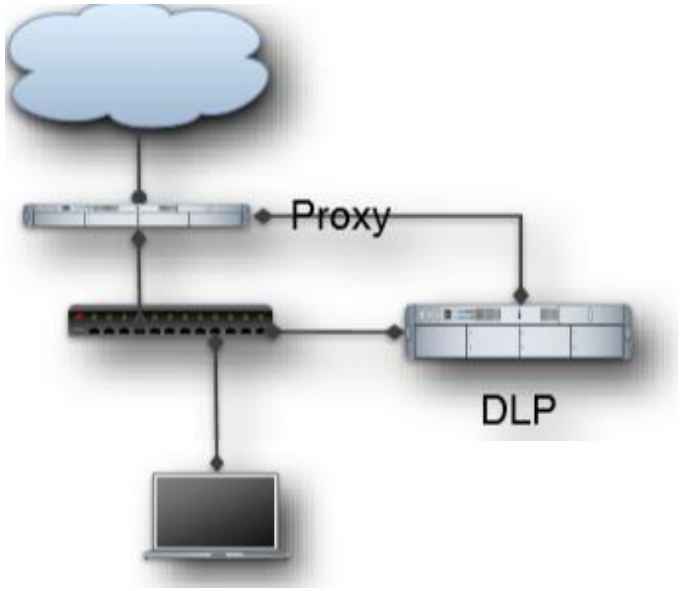
Network Monitor



Email Monitor



Proxy

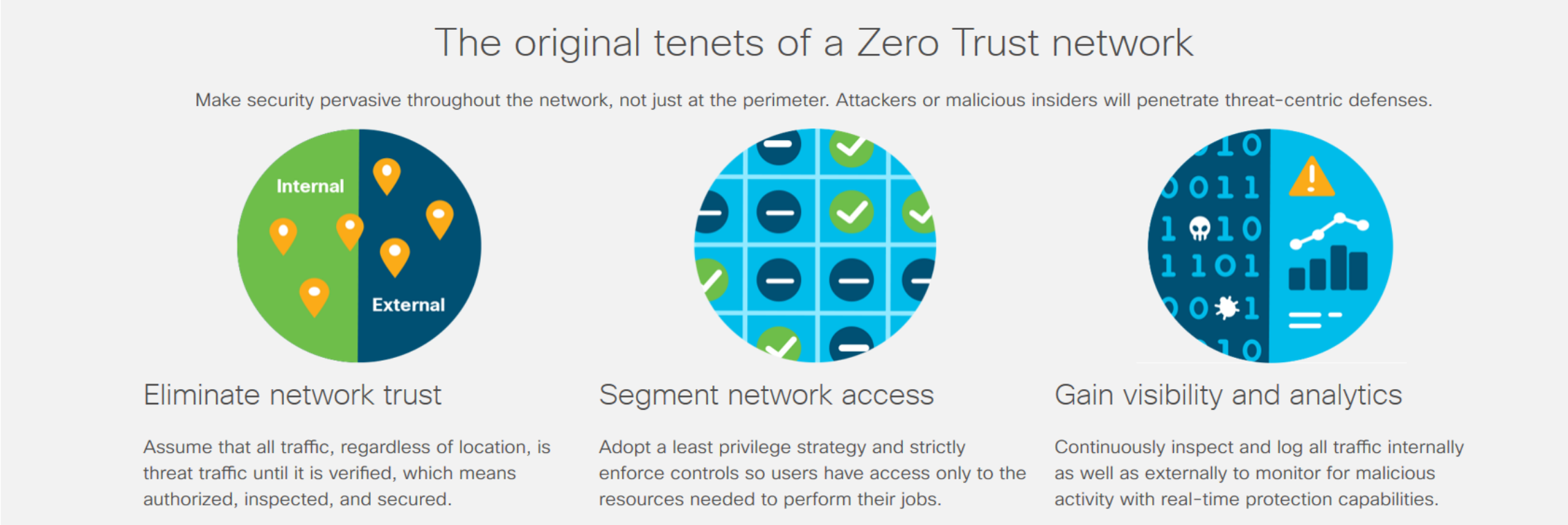


Perimeter Security

Legacy Perimeter defense –Assumptions :

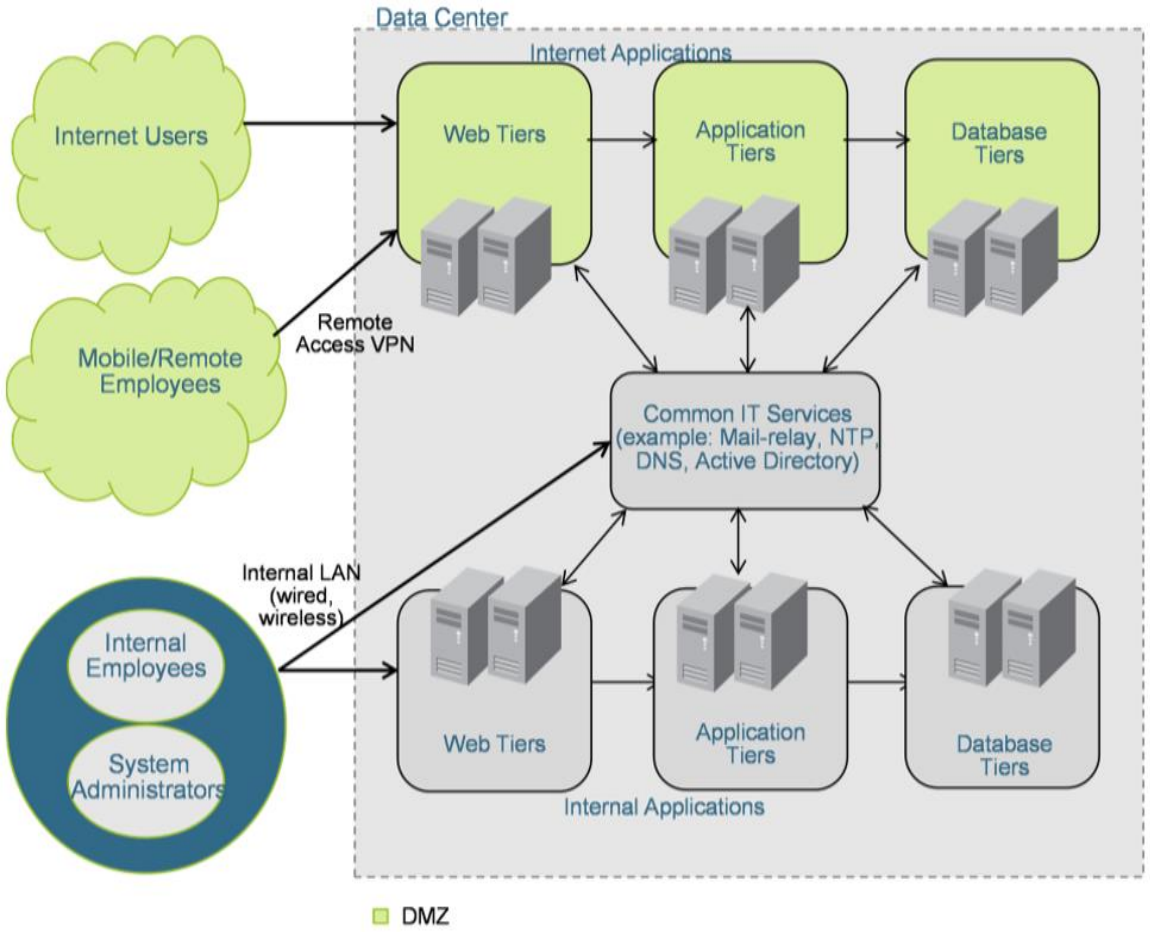
- ❑ Everything on the inside of an organization's network can be trusted.
- ❑ Threat always originate from untrusted zone towards Trusted Zone via the Perimeter.
- ❑ Lateral movement of attacks posed low Risk.

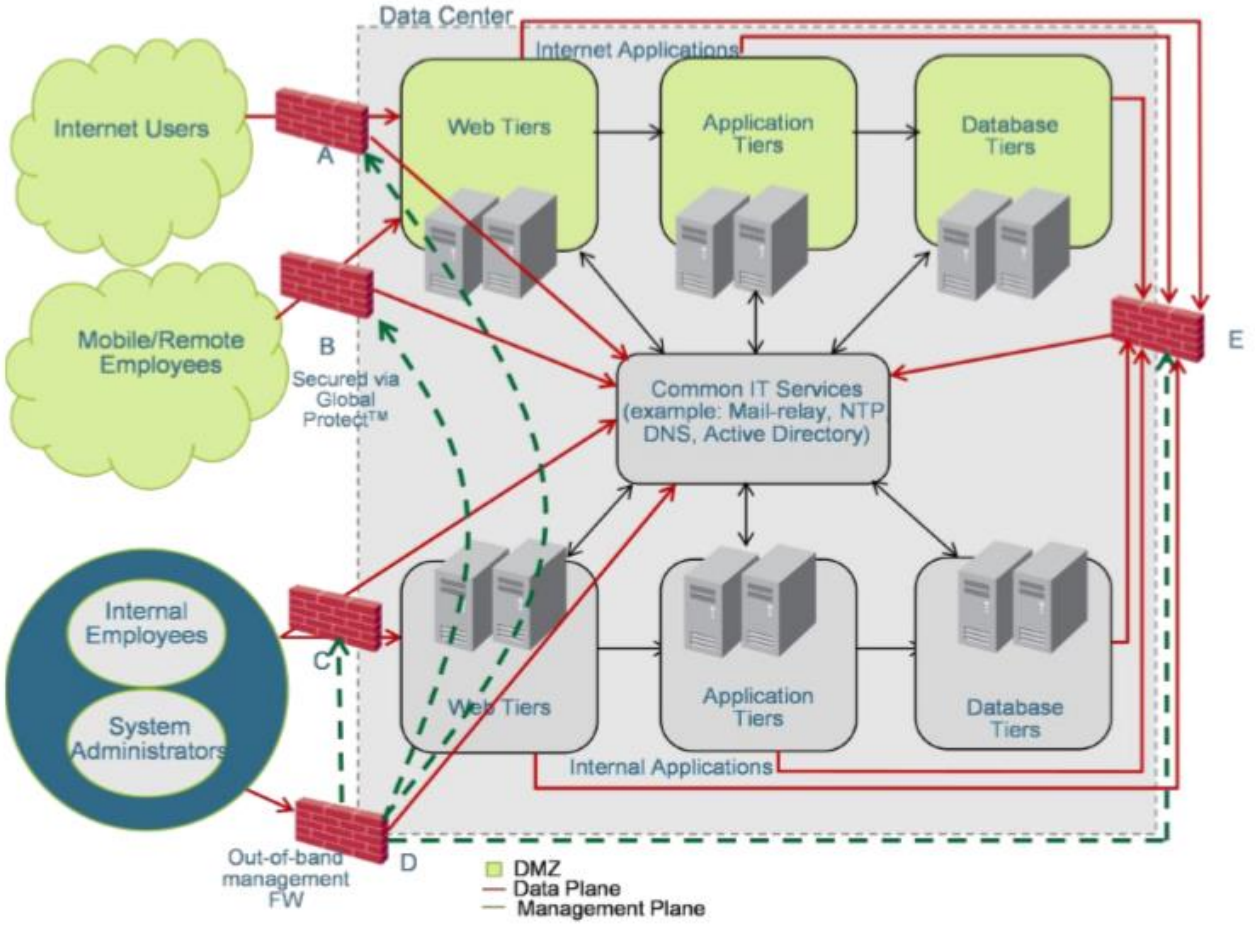
Evolving Trust model – Zero Trust:



Perimeter Security

Determine the best enforcement points for firewalls using Traditional approach and Zero – Trust model





Recap and Questions

ENDPOINT SECURITY

Endpoint Security & Evolution

Introduction:

- Endpoint security, or endpoint protection, are systems that protect computers and other devices on a network or in the cloud from security threats.

Traditional Endpoint Solutions:

- Deploying Anti-Viruses
- Frequent Signature updates.
- Effectiveness is based on the Signatures.
- Unable to cope up with the evolution of Malware and new types of threats.

Next-Gen Endpoint Solutions:

- Detection speed and confidence have improved with the incorporation of behavioral analysis , ML and AI.
- Near real-time protection against new Malwares and 0-day attacks.
- Endpoint Detection and Response (EDR)
- Application Whitelisting
- Forensics

Trends:

- Machine Learning and AI.
- SaaS-Based Endpoint Security
- Protection Against File less Attacks
- IoT Devices Under the Protective Umbrella
- Reducing Complexity and Consolidating Agents

Endpoint Security – NextGen Features

Next Gen AVs provides detailed forensics on the detections.

Example:

Detection Details display a wealth of information about the detection, including

Detection's name

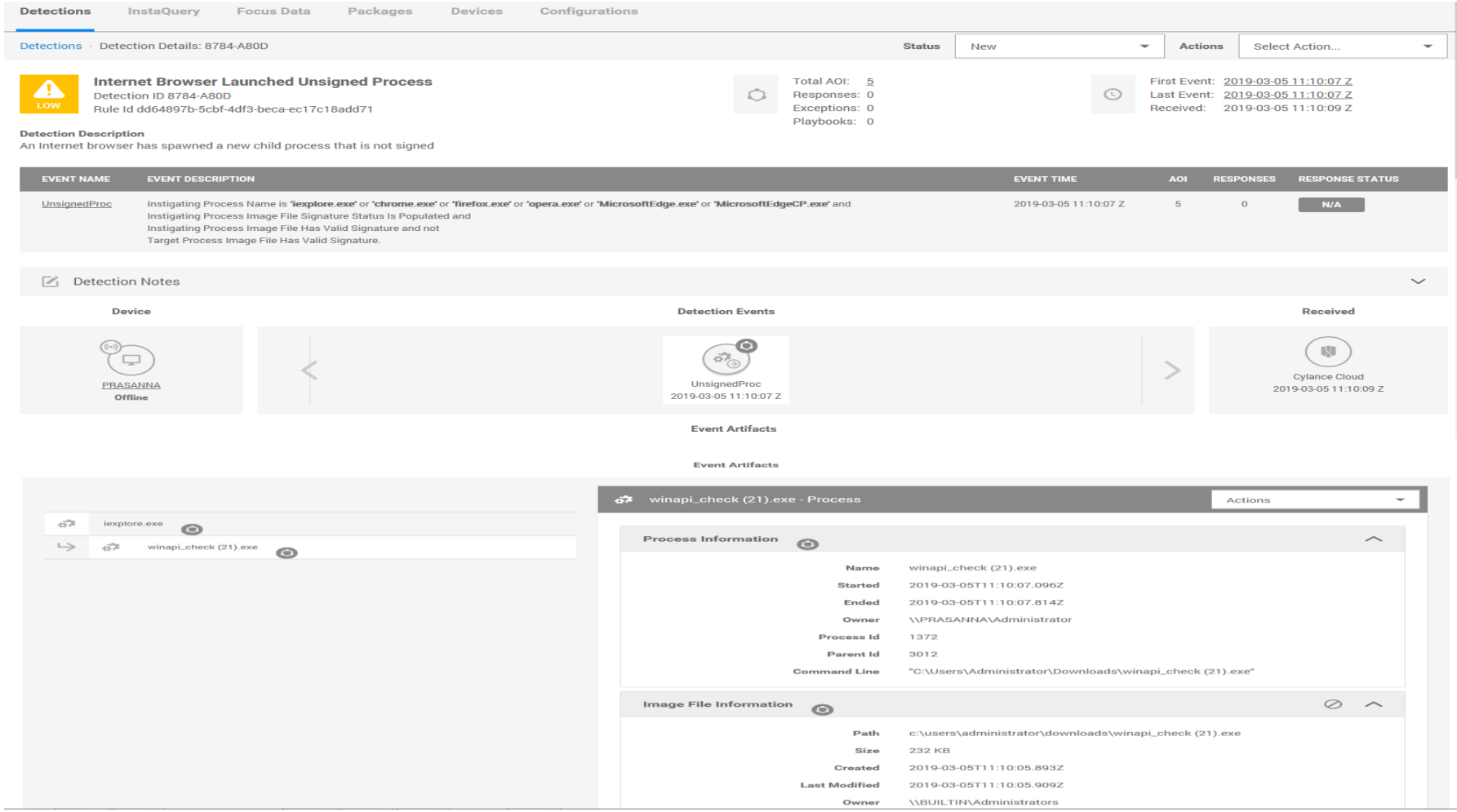
Severity

Description

Number of events

Artifacts of interest

Automated responses associated with that detection.



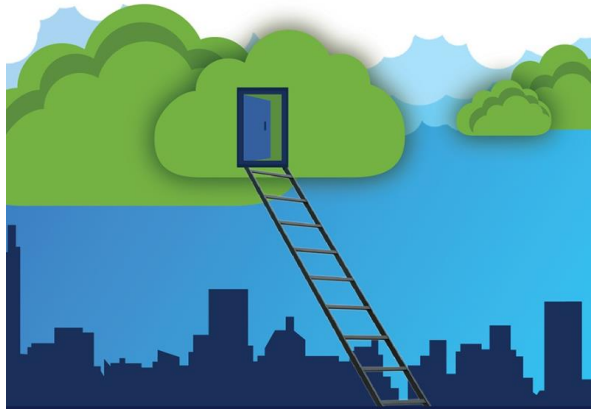
Recap and Questions

BOUNDARYLESS ORGANIZATIONS – SECURITY CHALLENGES

Boundaryless Organizations – Security Challenges

Drivers for Cloud adoption:

- ❑ Business growth
- ❑ Efficiency
- ❑ Experience
- ❑ Agility
- ❑ Cost
- ❑ Assurance

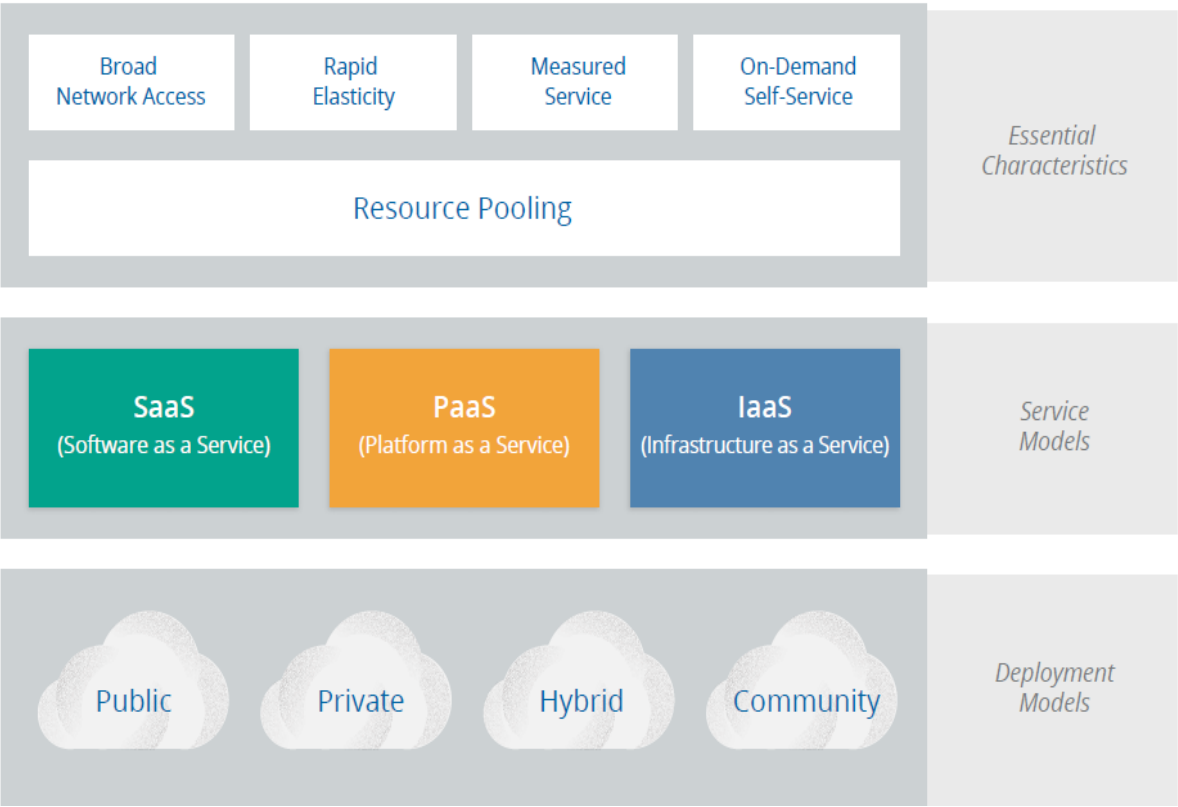


NIST – Definition of Cloud Computing

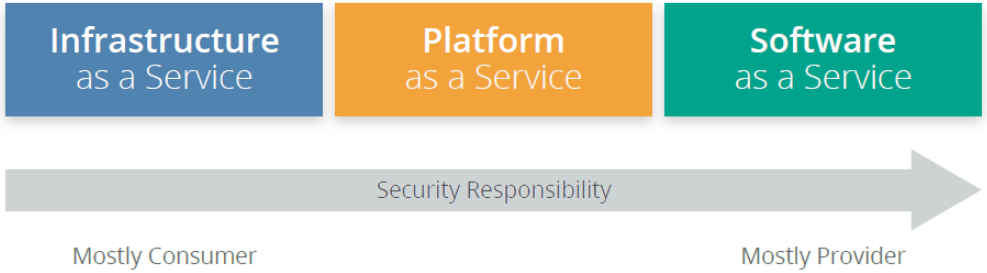
> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Boundaryless Organizations – Security Challenges

Cloud Model:

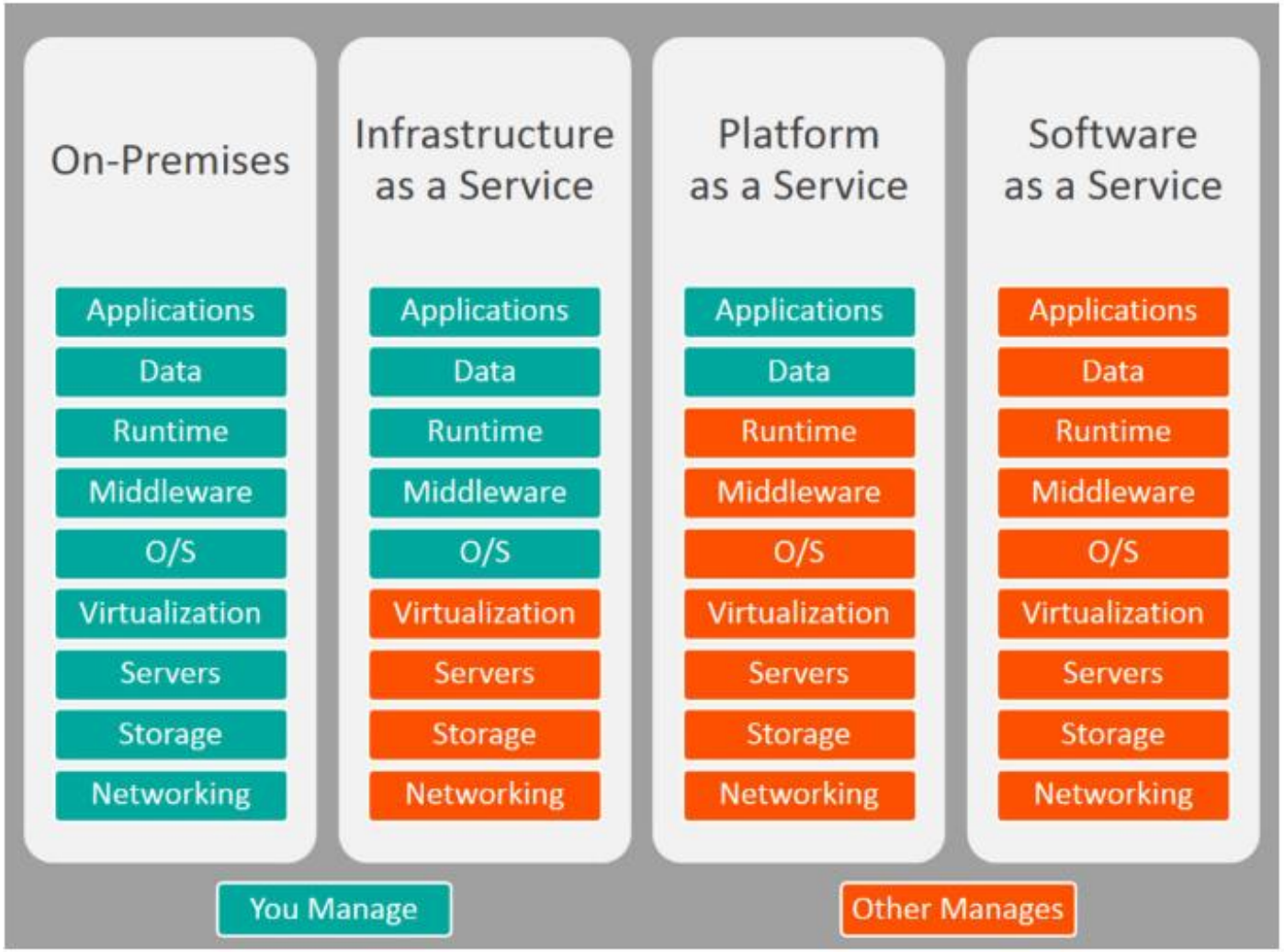


Cloud Security Scope



Boundaryless Organizations – Security Challenges

Cloud – Responsibility Matrix



Examples

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

Boundaryless Organizations – Security Challenges

CASB:
CASB is on-premises or cloud based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies.

CASBs work by intermediating or “proxying” traffic between cloud apps and users. Once proxied, these tools provide:

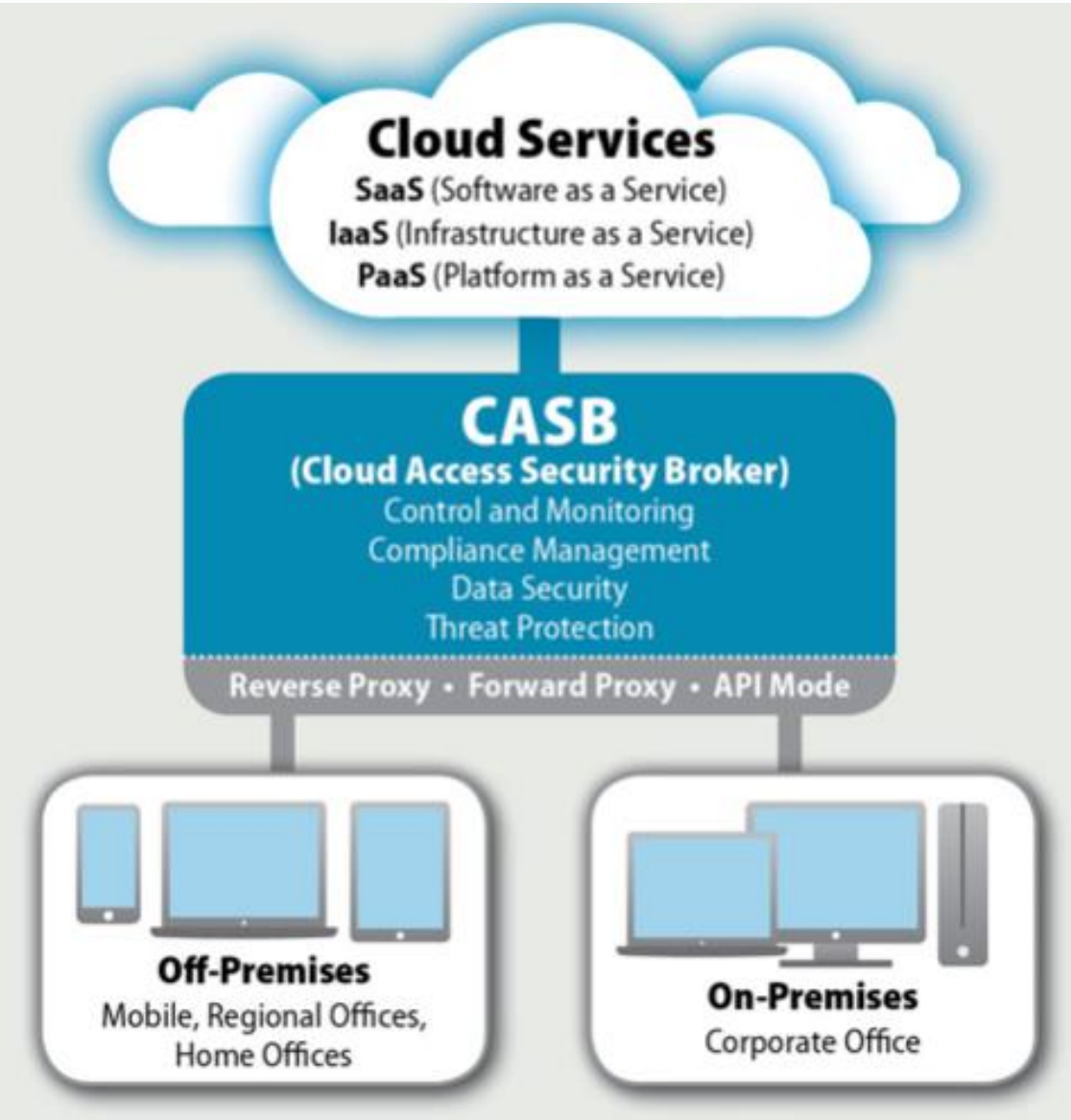
- ❑ Visibility—audit logs, security alerts, compliance reports, etc.
- ❑ Data Security—access control, data leakage prevention, encryption, etc.

Deployment

- ❑ On-Prem
- ❑ Cloud

Mode

- ❑Forward Proxy
- ❑Reverse Proxy
- ❑API based Systems



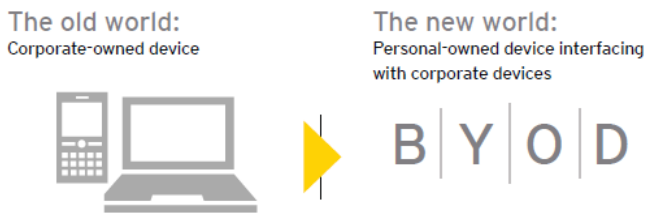
Boundaryless Organizations – Security Challenges

BYOD:

- ❑ BYOD - “Bring Your Own Device,” a phrase that refers to the practice of allowing employees to bring their own mobile devices to work for use with company systems, software, networks, or information.
- ❑ BYOD has become a huge trend amongst enterprises, with nearly 1/3 of employees using personal devices at workplaces worldwide.

✓ Employee satisfaction
✓ Business productivity
✓ Enhanced collaboration and mobility
✓ Expanded mobile access to resources
✓ Reduced spending on sourcing and support of devices
✓ Lessened responsibility for device lifecycle management
✓ Consolidation of infrastructure and tools across many IT disciplines.

✓ Exposed data
✓ Data leakage
✓ Data loss
✓ Public exposure
✓ Malicious apps
✓ Cross contamination
✓ OS-specific security customization



Boundaryless Organizations – Security Challenges

SCENARIO		SECURITY GAP
Authorized users accessing approved cloud applications from unmanaged endpoint devices		Unmanaged endpoints are vulnerable to breaches and other exploits that can steal legitimate credentials.
Authorized users accessing unapproved cloud applications (shadow IT) from unmanaged devices		Organizations can't enforce endpoint protection—even when using enterprise mobile management or mobile device management solutions—on unmanaged personal devices that access unsanctioned cloud applications over public, mobile, and wireless networks.
Authorized users accessing approved cloud applications on managed devices		Managed devices can be vulnerable to insider abuse, attacks, and theft.
Unauthorized users (that is, cybercriminals or insiders with malicious intent) using stolen credentials to access cloud applications (both approved and unapproved)		Approved cloud applications can be targets for account takeovers and malicious insider threats. Security teams have no visibility into company usage and storage of sensitive corporate data in unapproved cloud applications.

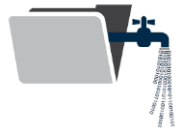
Recap and Questions

MOBILE SECURITY

Mobile Security

- Mobile security is the protection of portable devices such as laptops, smartphones, tablets, and smartwatches from threats and vulnerabilities.

- Major Security Concerns

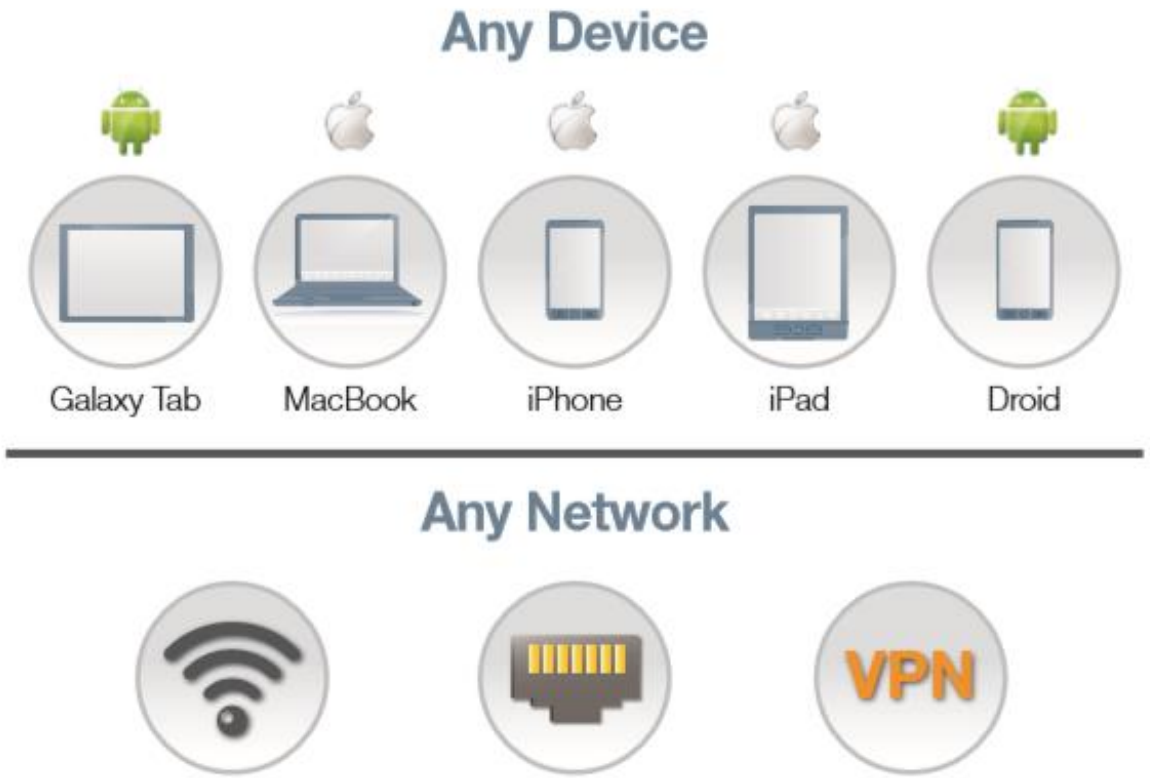


Data Leakage

Unauthorized Access

Unsafe apps download

Malware



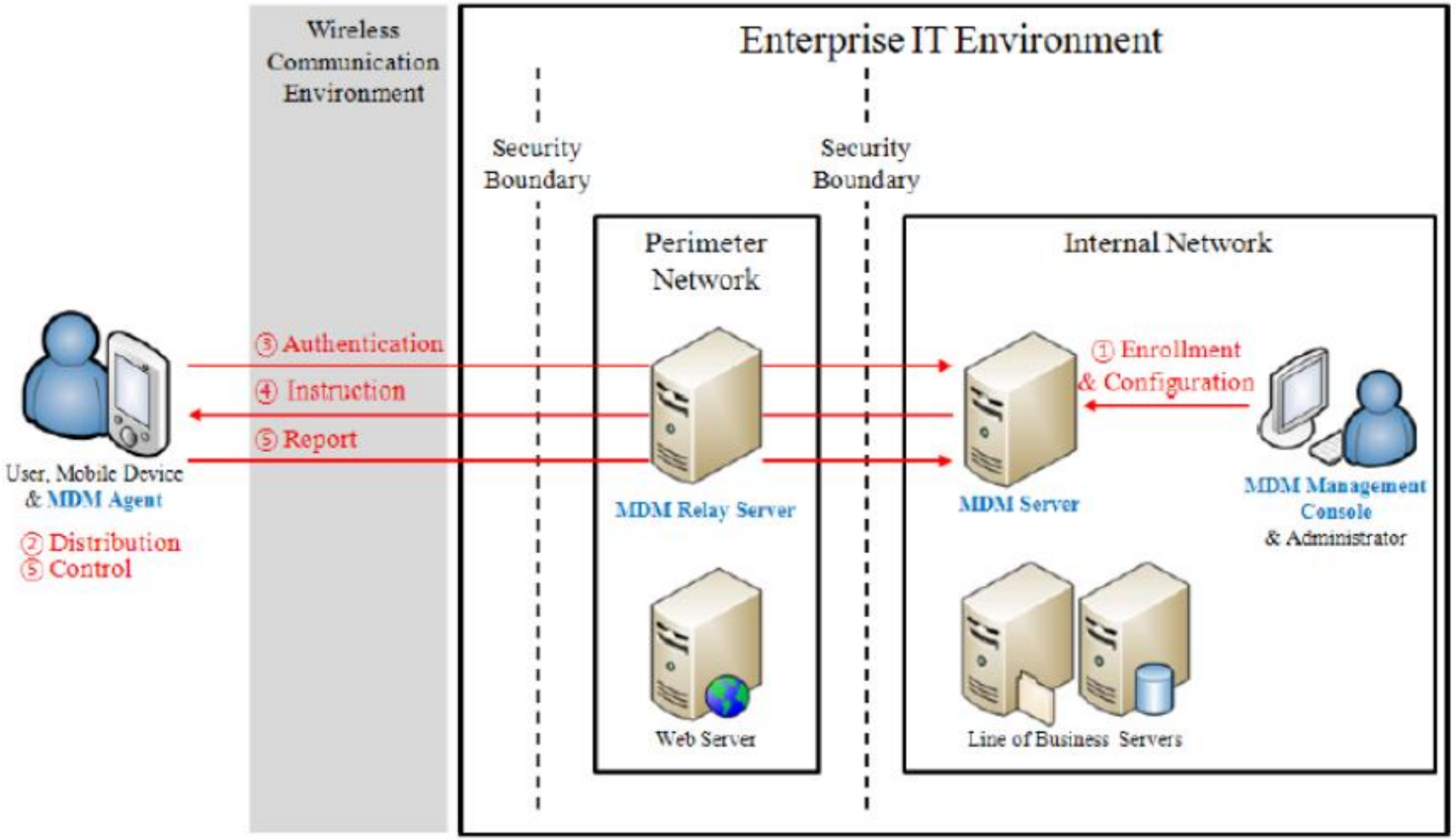
Mobile Security Strategies

Mobile device Management

Endpoint Security Tools

Network Access Control

Typical MDM Architecture



Basic Operations

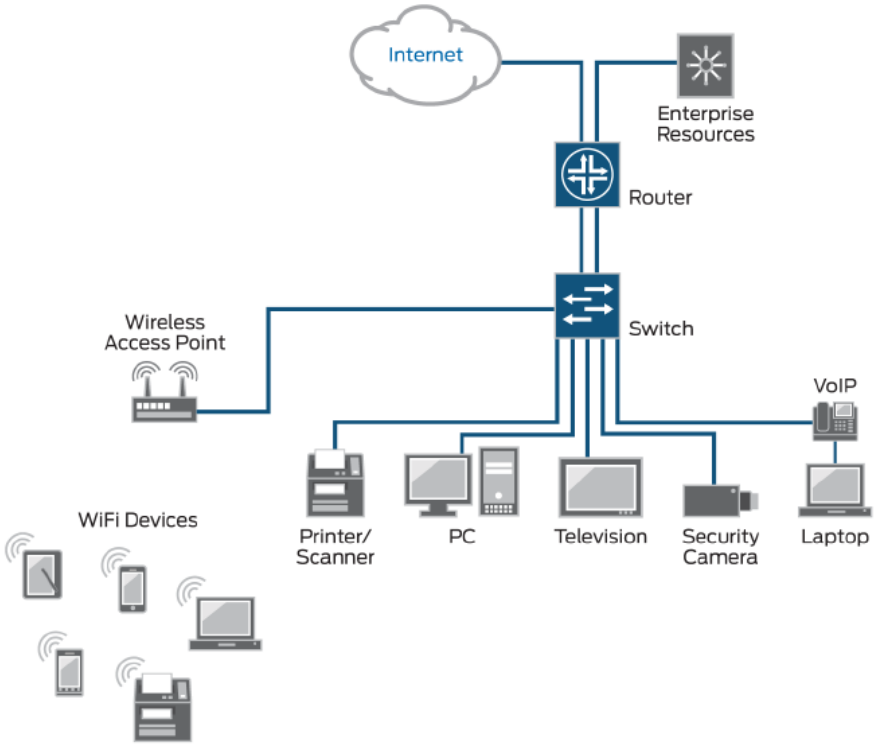
- ❑Enrollment/Configuration
- ❑Distribution
- ❑Authentication
- ❑Instruction
- ❑Control/Report

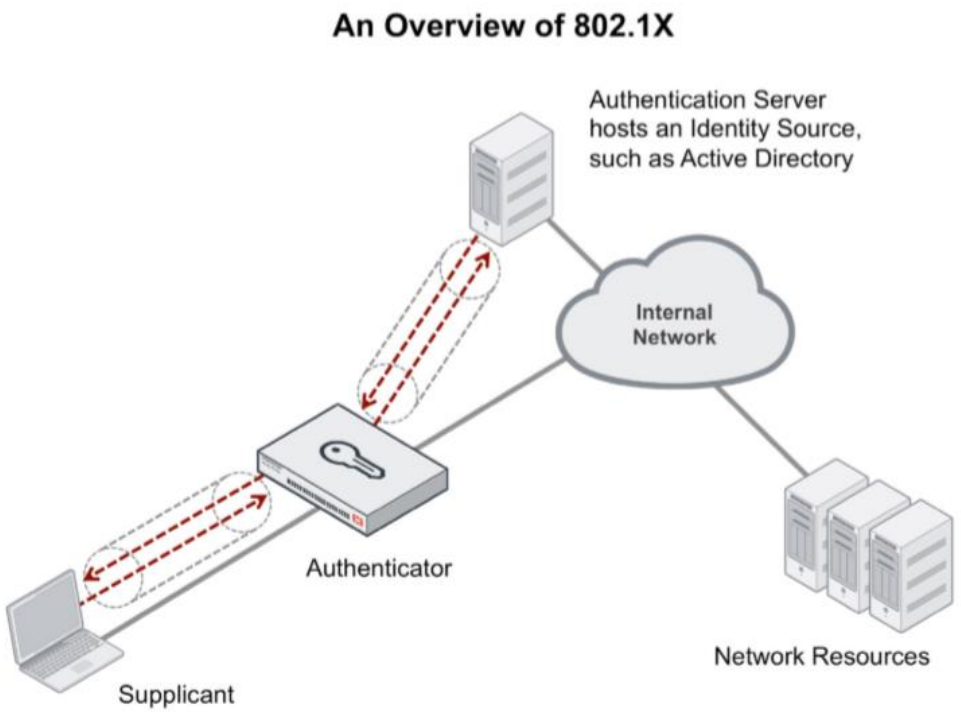
Mobile Security

Network Access Control

Can identify users and devices by controlling access to the network using one or more forms of authentication, and controlling access to enterprise resources using one or more forms of authorization and policy enforcement.

The 802.1X protocol is an IEEE standard for port-based network access control (PNAC) on both wired and wireless access points. The primary intent of 802.1X is to define authentication controls for *any* user or device trying to access a LAN or WLAN.





Recap and Questions

References

OSI Model, Protocols, Load balancing: https://www.f5.com/pdf/certification/exams/Certification_Study_Guide_101.pdf

Firewalls, Endpoint Security, VPNs, NAC: https://www.cisco.com/c/en/us/support/security/index.html

DLP : https://www.bankinfosecurity.com/case-study-omni-american-bank-takes-on-data-loss-prevention-a-898

Traditional and NextGen AV: https://www.crowdstrike.com/wp-content/brochures/avc_mrg_biz_2016_nextgen_en.pdf

Cloud:

https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/

https://aws.amazon.com/getting-started/?ref=docs_gateway