Network Security Technologies

This section describes traditional network security technologies, including firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), web content filters, virtual private networks (VPNs), data loss prevention (DLP), unified threat management (UTM), and security information and event management (SIEM).

Firewalls

Firewalls have been a cornerstone of network security since the early days of the internet. 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 if 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 using hiding techniques such as encryption and non-standard ports. Proxy servers can also 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.

Intrusion detection and intrusion 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 is typically 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 is thus 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.

IDSs and IPSs can also 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 may therefore be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

Web content filters

Web content filters are used to restrict the internet activity of users on a network. Web content filters match a web address (*uniform resource locator*, or URL) against a database of websites, which is typically maintained by the individual security vendors that sell the web content filters and is provided as a subscription-based service. Web content filters attempt to classify websites based on broad categories that are either allowed or blocked for various groups of users on the network. For example, the marketing and human resources departments may have access to social media sites such as Facebook and LinkedIn for legitimate online marketing and recruiting activities, while other users are blocked. Typical website categories include:

Gambling and online gaming

Hacking

Hate crimes and violence

Pornography

Social media

Web-based email

These sites lower individual productivity but also may be prime targets for malware that users may unwittingly become victims of via drive-by downloads. Certain sites may also create liabilities in the form of sexual harassment or racial discrimination suits for organizations that fail to protect other employees from being exposed to pornographic or hate-based websites.

Organizations may elect to implement these solutions in a variety of modes to either block content, warn users before they access restricted sites, or log all activity. The disadvantage of blocking content is that false positives require the user to contact a security administrator to allow access to websites that have been improperly classified and blocked or need to be accessed for a legitimate business purpose.

Key Terms

A *uniform resource locator* (URL) is a unique reference (or address) to an internet resource, such as a webpage.

Virtual private networks

A virtual private network (VPN) creates a secure, encrypted connection (or tunnel) across the internet back to an organization's network. VPN client software is typically 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.

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 to be very fast, it is perhaps the least secure of the various VPN protocols. It is commonly used with 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 is primarily 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. Alternatively, 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 can essentially bridge themselves over the internet, through the client endpoint, and into the network over the IPsec 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 is still the more commonly used terminology.

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 is still commonly referred to as SSL).

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 who 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.

Data loss prevention

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 – 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.

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."

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. DLP solutions often require many moving parts to effectively route traffic to and from inspection engines, which can add to the complexity of troubleshooting network issues.

Unified threat management

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:

- In some cases, they 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.