Security Appliances

- Security can be achieved through appliances that directly address security and by using the security features in standard networking devices
- Using both standard networking devices and security appliances can result in a layered security approach
- Appliances include:
  - Firewalls
  - Proxy servers
  - Deception instruments
  - Intrusion detection and prevention systems
  - Network hardware security models

Firewalls (1 of 6)

- To use firewalls effectively, you must understand the function of firewalls and know the different types of firewalls and specialized firewall appliances
- Firewall Functions
  - A firewall uses bidirectional inspection to examine outgoing and incoming packets
  - The actions are based on specific criteria or rules (called *rule-based firewalls*)
  - A more flexible type of firewall is a *policy-based firewall* which allows more generic statements instead of specific rules
  - Firewalls can also apply **content/URL filtering**

Firewalls (2 of 6)

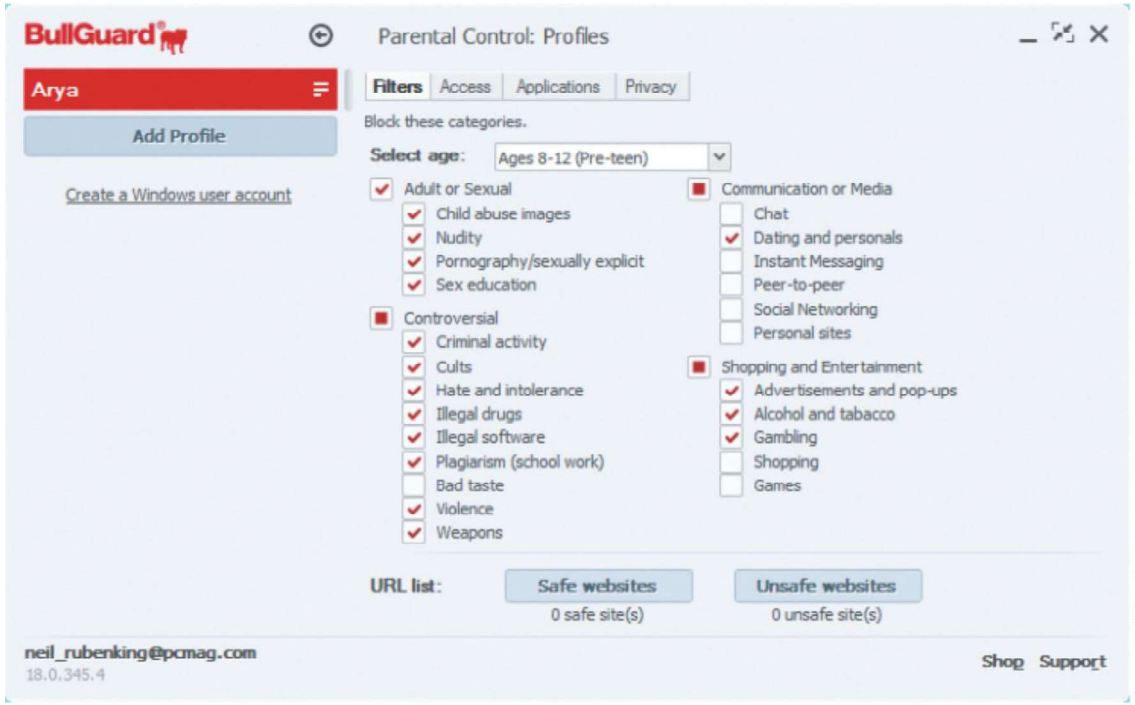


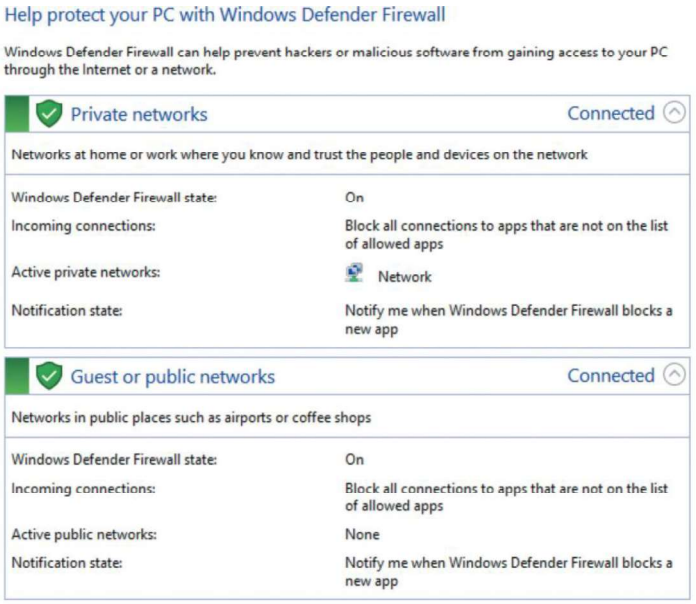
Figure 9-1 Content/URL filtering

Figure 9-1 Content/URL filtering

Firewalls (3 of 6)

- Firewall Categories
  - *Stateful vs. stateless*
  - *Open source vs. proprietary*
  - *Hardware vs. software*
  - *Host vs. appliance vs. virtual*

Firewalls (4 of 6)



Used with permissions from Microsoft

Figure 9-3 Windows host-based firewall

Figure 9-3 Windows host-based firewall

Firewalls (5 of 6)

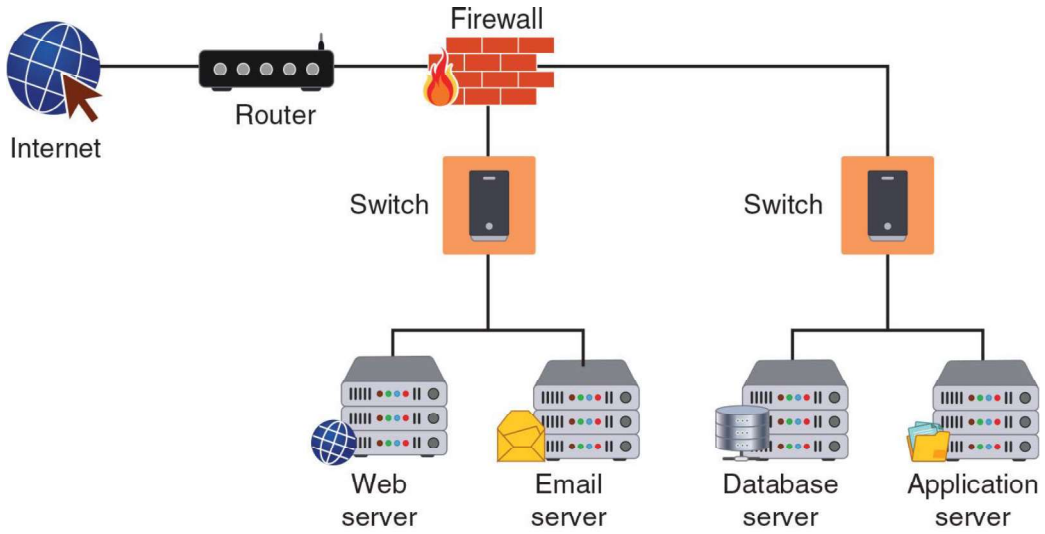


Figure 9-4 Appliance firewall

Figure 9-4 Appliance firewall

Firewalls (6 of 6)

- Specialized Firewall Appliances
  - *Web application firewall*
  - *Network address translation gateway*
    - Network address translation (NAT) is a technique that allows private IP addresses to be used on the public internet
  - *Next generation firewall*
  - *Unified threat management (UTM)*
    - UTM is a device that combines several security functions such as packet filtering, antispam, antiphishing, antispyware, encryption, intrusion protection, and web filtering

Proxy Servers (1 of 2)

- Proxies are devices that act as substitutes on behalf of the primary device
- A **forward proxy** is a computer or an application that intercepts user requests from the internal secure network and processes the requests on behalf of the user
- A **reverse proxy** routes requests coming from an external network to the correct internal server
- A proxy server can provide a degree of protection
  - It can look for malware by intercepting it before it reaches the internal endpoint
  - It can hide the IP address of endpoints inside the secure network so that only the proxy server's IP address is used on the open Internet

Proxy Servers (2 of 2)

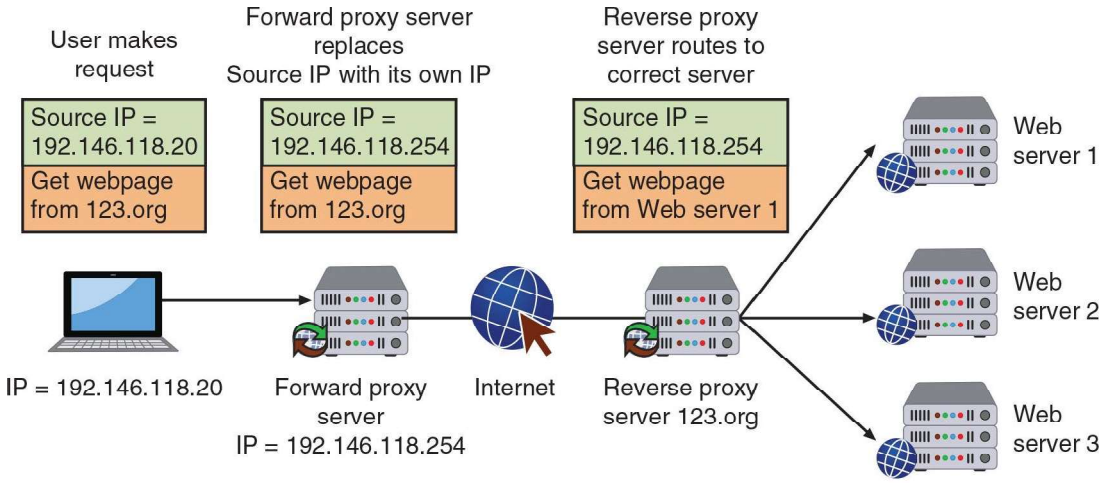


Figure 9-5 Forward and reverse proxy servers

Figure 9-5 Forward and reverse proxy servers

Deception Instruments (1 of 3)

- Deception can be used as a security defense
  - By directing threat actors away from a valuable asset to something that has little or no value
- Network deception can involve creating and using honeypots and sinkholes
- Honeypots
  - A **honeypot** is a computer located in an area with limited security that serves as "bait" to threat actors
  - Two goals of using a honeypot:
    - *Deflect*
    - *Discover*

Deception Instruments (2 of 3)

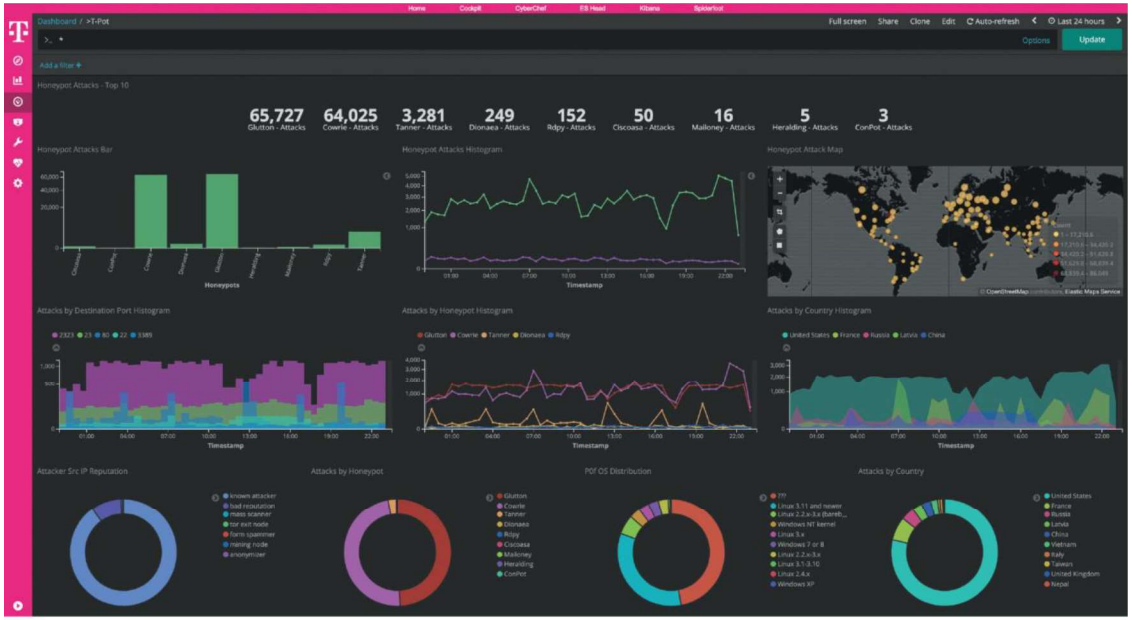


Figure 9-6 Honeypot dashboard

Figure 9-6 Honeypot dashboard

Deception Instruments (3 of 3)

- Honeypots (continued)
  - Different types of honeypots:
    - A *low-interaction honeypot* may only contain a login prompt
    - A *high-interaction honeypot* is designed for capturing more information from the threat actor
      - This type of honeypot can collect information from threat actors about attack techniques or the particular information they are seeking from the organization
  - A **honeynet** is a network of honeypots set up with intentional vulnerabilities
- Sinkholes
  - A **sinkhole** is a "bottomless pit" designed to steer unwanted traffic away from its intended destination to another device
    - The goal is to deceive the threat actor into thinking the attack was successful

Intrusion Detection and Prevention Systems (1 of 3)

- An *intrusion detection system (IDS)* can detect an attack as it occurs
- An *intrusion prevention system (IPS)* attempts to block the attack
- **Inline system** is connected directly to the network and monitors the flow of data as it occurs
- A **passive system** is connected to a port on a switch, which receives a copy of network traffic
- IDS systems can be managed in different ways:
  - In-band management is through the network itself by using network protocols and tools
  - Out-of-band management is using an independent and dedicated channel to reach the device

Intrusion Detection and Prevention Systems (2 of 3)

- Monitoring Methodologies
  - **Anomaly-based monitoring** compares current detected behavior with baseline
  - **Signature-based monitoring** looks for well-known attack signature patterns
  - **Behavior-based monitoring** detects abnormal actions by processes or programs
    - Alerts user who decides whether to allow or block activity
  - **Heuristic monitoring** uses experience-based techniques
    - Attempts to answer the question “Will this do something harmful if it is allowed to execute?”

Intrusion Detection and Prevention Systems (3 of 3)

- A network intrusion detection system (NIDS) watches for attacks on the network
  - NIDS sensors installed on firewalls and routers gather information and report back to central device
- A network intrusion prevention system (NIPS) monitors to detect malicious activities and also attempts to stop them

Network Hardware Security Modules

- A *hardware security module (HSM)* is a removable external cryptographic device
- For endpoints, an HSM is typically a USB device, an expansion card, or a device that connects directly to a computer through a port
- A **network hardware security module** performs cryptographic operations such as key management, key exchange, onboard random number generation, key storage facility, and accelerated symmetric and asymmetric encryption

Configuration Management

- It is essential that security appliances be properly configured
- Basic configuration management tools include:
  - *Secure baseline configurations*
  - *Standard naming conventions*
  - *Defined Internet Protocol schema*
  - *Diagrams*

Knowledge Check Activity 1

Which of the following network security devices is a computer that is purposely located in an area with limited security to attract threat actors?

a. Forward proxy
b. Honeypot
c. Inline system
d. Behavior monitor

Knowledge Check Activity 1: Answer

Which of the following network security devices is a computer that is purposely located in an area with limited security to attract threat actors?

Answer: b. Honeypot

A honeypot is a computer located in an area with limited security that serves as "bait" to threat actors. Its purpose is to deflect and discover threats.

Security Technologies

- There are general security technologies that can provide a defense
- Some of these technologies can be found in both standard networking devices (switches and routers) and specialized security appliances
- Categories of security technologies include:
  - Access technologies
  - Monitoring and managing technologies
  - Design technologies

Access Technologies (1 of 7)

- Access Control List (ACL)
  - An **access control list (ACL)** contains rules that administer the availability of digital assets by granting or denying access to the assets
  - Two types of ACLS include:
    - *Filesystem ACLs* filter access to files and directories on an endpoint by telling the OS who can access the device and what privileges they are allowed
    - *Networking ACLs* filter access to a network
      - Often found on routers
  - Router ACLs can be used on external routers to restrict vulnerable protocols and limit traffic from entering the network
  - Internal router ACLs are often configured with explicit *allow* and *deny* statements for specific addresses and protocol services

Access Technologies (2 of 7)

- Virtual Private Network (VPN)
  - A **VPN** is a security technology that enables authorized users to use an unsecured public network (the Internet) as if it were a secure private network
  - Two common types of VPNs:
    - A **remote access VPN**
    - A **site-to-site VPN**
  - A **full tunnel** sends all traffic to the VPN concentrator and protects it
  - A **split tunnel** routes only some traffic over the secure VPN while other traffic directly accesses the Internet (this helps preserve bandwidth)
  - The most common protocols used for VPNs are IPsec and SSL

Access Technologies (3 of 7)

- Network Access Control (NAC)
  - **NAC** examines the current state of a system or network device before it can connect to the network
  - Any device that does not meet a specified set of criteria can connect only to a "quarantine" network where the security deficiencies are corrected
  - NAC uses software "agents" to gather information and report back (called host agent health checks)
  - An agent may be a *permanent* NAC agent or a *dissolvable* NAC agent that disappears after reporting information to the NAC
  - The NAC technology can be embedded within a Microsoft Windows Active Directory (AD) domain controller
    - NAC uses AD to scan the device (called **agentless NAC**)

Access Technologies (4 of 7)

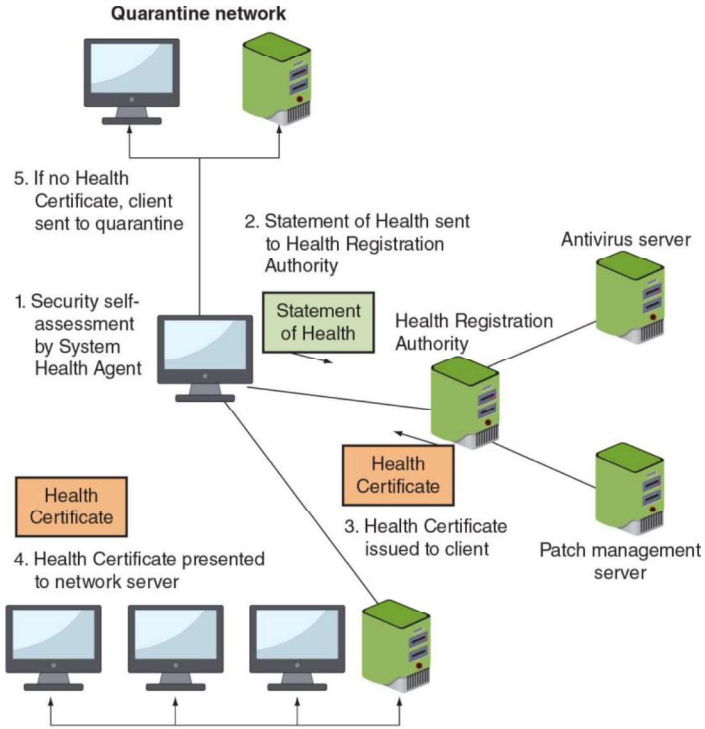


Figure 9-7 Network access control (NAC) process

Figure 9-7 Network access control (NAC) process

Access Technologies (5 of 7)

- Data Loss Prevention
  - DLP is considered as rights management, or the authority of the owner of the data to impose restrictions on its use
  - DLP is a system of security tools that is used to recognize and identify data that is critical to the organization
  - Most DLP systems use **content inspection** which is defined as a security analysis of the transaction within its approved context
  - An administrator creates DLP rules based on the data and the policy
  - These rules are loaded into a DLP server
  - When a policy violation is detected by the DLP agent it is reported back to the DLP server

Access Technologies (6 of 7)

- Data Loss Prevention (continued)
  - When a server is notified of a policy violation different actions can be taken:
    - Block the data
    - Redirect it to an individual who can examine the request
    - Quarantine the data until later
    - Alert a supervisor of the request
  - A process called *tokenization* obfuscates sensitive data elements, such as an account number, into a random string of characters (*token*)
    - The original sensitive data element and the token are stored in a database called a *token vault* so that if the actual data element is needed, it can be retrieved as needed
    - Tokenization is illustrated in Figure 9-8 on the following slide

Access Technologies (7 of 7)

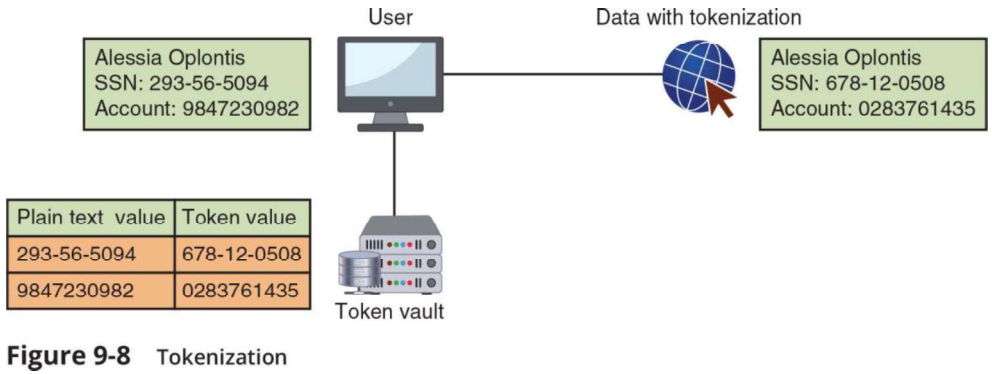


Figure 9-8 Tokenization

Figure 9-8 Tokenization