CIT 270: SYSTEMS SECURITY I

CHAPTER 6: NETWORKING SECURITY DEVICES, DESIGN, AND TECHNOLOGY

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note 📎

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

SECURITY THROUGH NETWORK DEVICES

Pay careful attention to your reading on pages 235 – 243. These pages introduce you to the basics of a computer network. The terms below refer to network security and settings that can be configured on hardware devices covered in the linked video:

- Loop Prevention
- Flood Guard
- Port Security
- Access Control List (ACL)
- Anti-spoofing

Network Devices Explained
Hub, Bridge, Router, Switch

SECURITY THROUGH NETWORK DEVICES: LOAD BALANCERS

Load Balancer: dedicated hardware that helps evenly distribute work across a network; can be software based.

Load balancers typically use a round-robin scheduling protocol, where a rotation hands out request to devices in order, or an affinity scheduling protocol where scheduling is based on which devices have the lowest connections.

Layer 4 load balancers act upon data found in Network Transport layer protocols such as IP, TCP, FTP, and UDP. Layer 7 load balancers distribute based on Application Layer protocols such as HTTP; cookies, app messages, etc.

SECURITY THROUGH NETWORK DEVICES: PROXIES

Forward Proxy: computer or application that intercepts a users request and processes it on their behalf; caching.

Application / Multipurpose Proxy: special proxy server that *knows* the application protocols that it supports; FTP proxy servers.

Reverse Proxy: routes requests from an external network to the correct internal server; load balancers.

SECURITY THROUGH NETWORK DEVICES: FIREWALLS

Firewall: designed to limit the spread of malware.; software and hardware.

Host-based Firewall: a firewall included with an operating system, also called a personal firewall.

Implicit Deny: the principle of blocking data or network traffic by default; you must explicitly allow everything.

SECURITY THROUGH NETWORK DEVICES: FIREWALLS

Network-based Firewall: functions on the Network Layer (OSI layer 3) screening packets based on specific criteria; *packet filter*.

Stateless Packet Filtering: looks at incoming packets and approves or denies them based on conditions the administrator has set up.

Stateful Packet Filtering: keeps a record of all connections and makes decisions on what it does or does not see happening in that connection; request origin.

SECURITY THROUGH NETWORK DEVICES: FIREWALLS

Application-based Firewall: functions on the Application Layer (OSI layer 7) by watching which applications send packets through the firewall then makes decisions based on what it does or does not see; limit application use, bandwidth limiting.

Web Application Firewall: a special type of Application-based Firewall watching applications that use HTTP; can block websites, stop known exploits, and block SQL or XSS attacks.

SECURITY THROUGH NETWORK DEVICES: VPN

Virtual Private Network (VPN): enables authorized users to use an unsecured public network as if it were a secure private network.

Remote-access VPN: a user-to-LAN connection used by remote users.

Site-to-Site VPN: multiple sites connect to other sites over the internet.

Always-on VPN: a VPN that allows users to always stay connected and never have to disconnect.

SECURITY THROUGH NETWORK DEVICES: VPN

VPN Concentrator: the end point of a VPN connection on dedicated hardware.

Full Tunnel: all traffic is sent to the VPN Concentrator and is protected.

Split Tunneling: only some traffic is routed through the VPN Concentrator and is protected, the rest of the traffic is directly sent in and out on the internet.

SECURITY THROUGH NETWORK DEVICES: MAIL GATEWAY

Earlier email systems used TCP/IP protocols to send messages and receive messages use Simple Mail Transfer Protocol (SMTP) for sending and Post Office Protocol (POP) for receiving incoming mail; copies are erased.

Newer email systems use Internet Mail Access Protocol (IMAP) for receiving incoming mail; the mail server keeps the original.

Mail Gateways monitor incoming messages to prevent unwanted messages from being delivered (malware, spam, phishing) and outgoing messages to protect the business' (SSN, sensitive data, healthcare records).

SECURITY THROUGH NETWORK DEVICES: DETECTION & PREVENTION

A Intrusion Detection System (IDS) can detect an attack as it occurs. In-band IDS systems are managed through the network itself using network protocols and tools, out-of-band IDS systems use an independent and dedicated channel.

Inline IDS: connected directly to the network and monitors the flow of data live.

Passive IDS: connected to a port on a switch and receives a copy of all or selected network traffic.

SECURITY THROUGH NETWORK DEVICES: DETECTION & PREVENTION

Function	**Inline**	**Passive**
Connection	Directly to the network	Connected to port on a switch
Traffic Flow	Routed through the device	Receives a copy of traffic
Blocking	Can block attacks	Cannot block attacks
Detection Error	May disrupt service	May cause false alarm

SECURITY THROUGH NETWORK DEVICES: METHODOLOGIES

Anomaly Monitoring: detects statistical anomalies by comparing it to a baseline.

False Positives: alarms raised when there is no actual abnormal behavior.

False Negatives: failure to raise an alarm or catch an abnormality when there actually was one.

Signature Based Monitoring: look for and record well known network traffic, activities, transactions, and behaviors so a signature can be built to compare against future activities.

SECURITY THROUGH NETWORK DEVICES: METHODOLOGIES

Behavioral Monitoring: attempts to overcome the limitations of anomaly based monitoring and signature based monitoring by being adaptive and proactive to its monitoring instead of reactive; abnormal actions or processes.

Heuristic Monitoring: attempts to answer the question *will this do something harmful*? Uses an algorithm to determine if a threat exists.

Network Intrusion Detection and Prevention Overview by Professor Messer

SECURITY THROUGH NETWORK DEVICES: IDS TYPES

Host-based Intrusion Detection System (HIDS): software application that runs on a local host computer and detects attacks as they occur; system calls, file system access, system registry changes, host input or output.

Network Intrusion Detection System (NIDS): watches for attacks on the network.

Network Intrusion Prevention System (NIPS): operates in a similar way to a HIDS but protects the network itself.

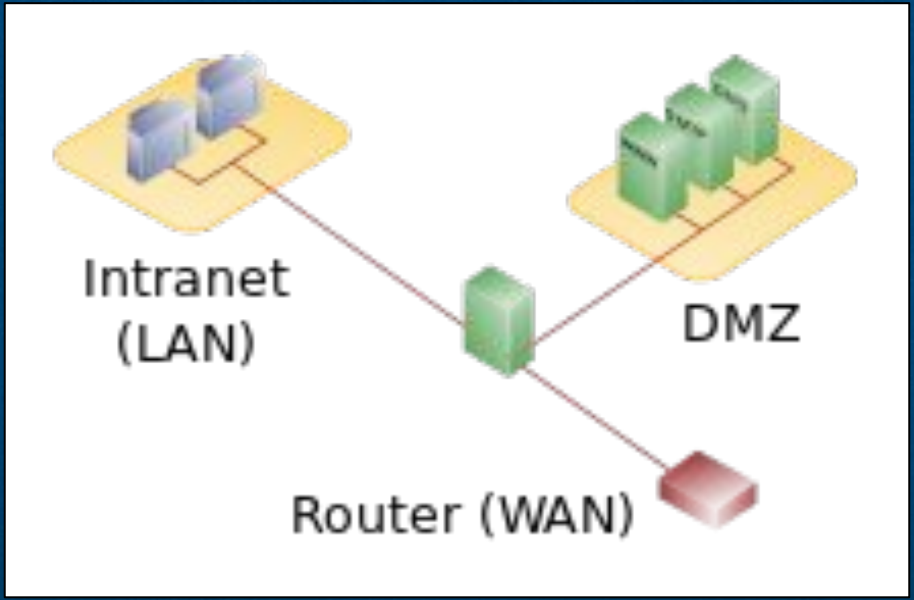
SECURITY THROUGH NETWORK DEVICES: MANAGEMENT

Large scale networks and enterprise have a lot to monitor and respond to so they use Security and Information Event Management (SIEM) products that consolidate real-time monitoring and management of security information:

- SIEM aggregation combines data from multiple sources.
- SIEM correlation searches aggregated data and finds common characteristics.
- SIEM automated alerting and triggers can inform security personnel of issues and trigger predefined responses.
- SIEM time synchronization shows the order events occured in.
- SIEM event duplication can detect and filter multiple alerts into one.
- SIEM logs record events for future analysis and show enterprises have complied with regulations.

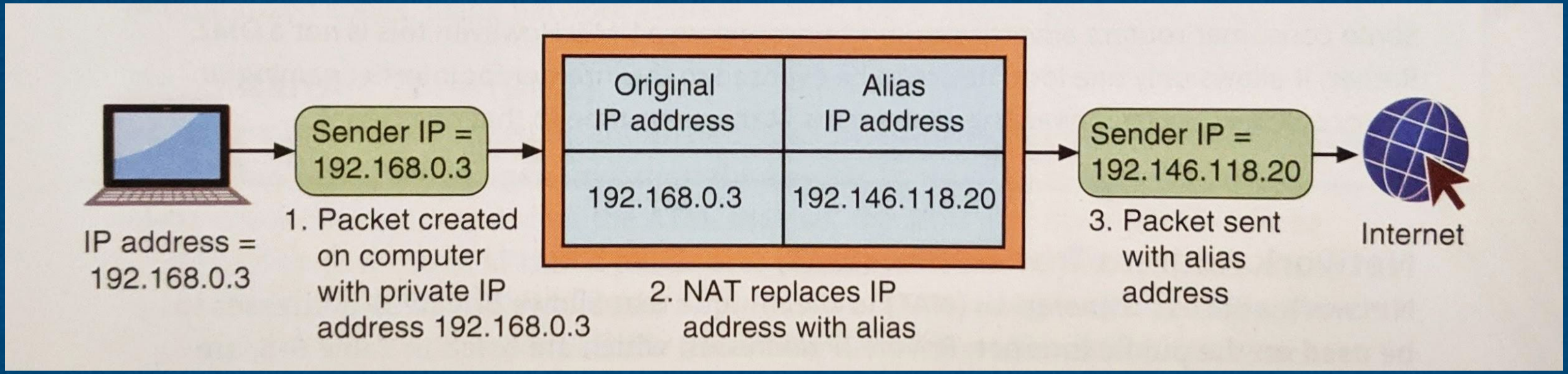
SECURITY THROUGH NETWORK ARCHITECTURE

A DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. (Wikipedia)



SECURITY THROUGH NETWORK ARCHITECTURE

Network Address Translation: a technique for allowing private IP addresses to be used on the public internet.



Original IP address	Alias IP address
192.168.0.3	192.146.118.20

1. Packet created on computer with private IP address 192.168.0.3

2. NAT replaces IP address with alias

3. Packet sent with alias address

Port Address Translation: a variation of NAT that uses the same IP address for all outgoing packets but assigns a different TCP port number; common with ISPs.

262

SECURITY THROUGH NETWORK ARCHITECTURE: OTHER ZONES

Networks can be setup in various other ways to insure a greater degree of security well still being convenient to use for an intended purpose:

Name	Description	Security Benefits
Intranet	A private network that belongs to an organization that can only be accessed by approved internal users.	Closed to the outside public, thus data is less vulnerable to external threat actors.
Extranet	A private network that can also be accessed by authorized external customers, vendors, and partners.	Can provide enhanced security for outside users compared to a publicly accessible website.
Guest Network	A separate open network that anyone can access without prior authorization.	Permits access to general network resources like web surfing without using the secure network.

SECURITY THROUGH NETWORK ARCHITECTURE: SEGREGATION

Physical Network Segregation: isolates the network so that it is not accessible by outsiders; air gap is an extreme implementation of this.

Virtual LAN (VLAN): separates devices into logical groups when they are not physically setup in such a way.

SECURITY THROUGH NETWORK TECHNOLOGIES

Read pages 265 – 269.

REFERENCES

Inline vs. passive IDS [Table 6-2]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 254. Boston, MA: Cengage.

Link Icon [PNG]. Share Icon. No license found, public domain inferred.

Paperclip Icon [PNG]. Copenhagen: Icon Finder. SIL Open Font License.

DMZ diagram [PNG]. San Francisco: Wikimedia Foundation. Public domain image.

“DMZ (Computing).” Wikipedia, Wikimedia Foundation, 13 May 2019, en.wikipedia.org/wiki/DMZ_(computing).