CIA Triad

CompTIA Network+ (N10-007)

Network Security Fundamentals

- Networks are increasingly dependent on interconnecting with other networks
- Risks exist not just on the untrusted Internet, but also inside our own organization's networks and must be minimized or eliminated
- Understanding the various threats facing our networks is important in order to best defend the network against the onslaught of cyber attacks they are constantly facing

Network Security Goals

- Commonly called the CIA Triad
  - Confidentiality
  - Integrity
  - Availability

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Confidentiality

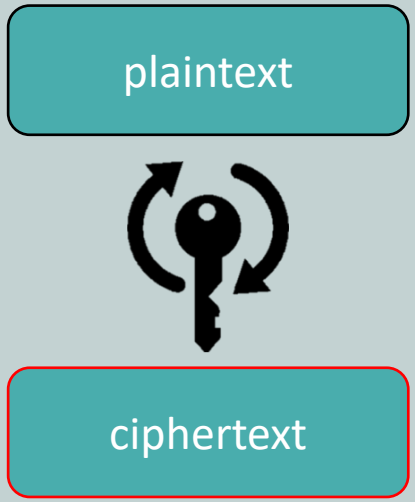
- Keeping the data private and safe
  - Encryption
  - Authentication to access resources

- Encryption ensures that data can only be read (decoded) by the intended recipient
  - Symmetric encryption
  - Asymmetric encryption

Symmetric Encryption (Confidentiality)

- Both sender and receiver use the same key

- DES (Data Encryption Standard)
  - Developed in the mid-1970s
  - 56-bit key
  - Used by SNMPv3
  - Considered weak today

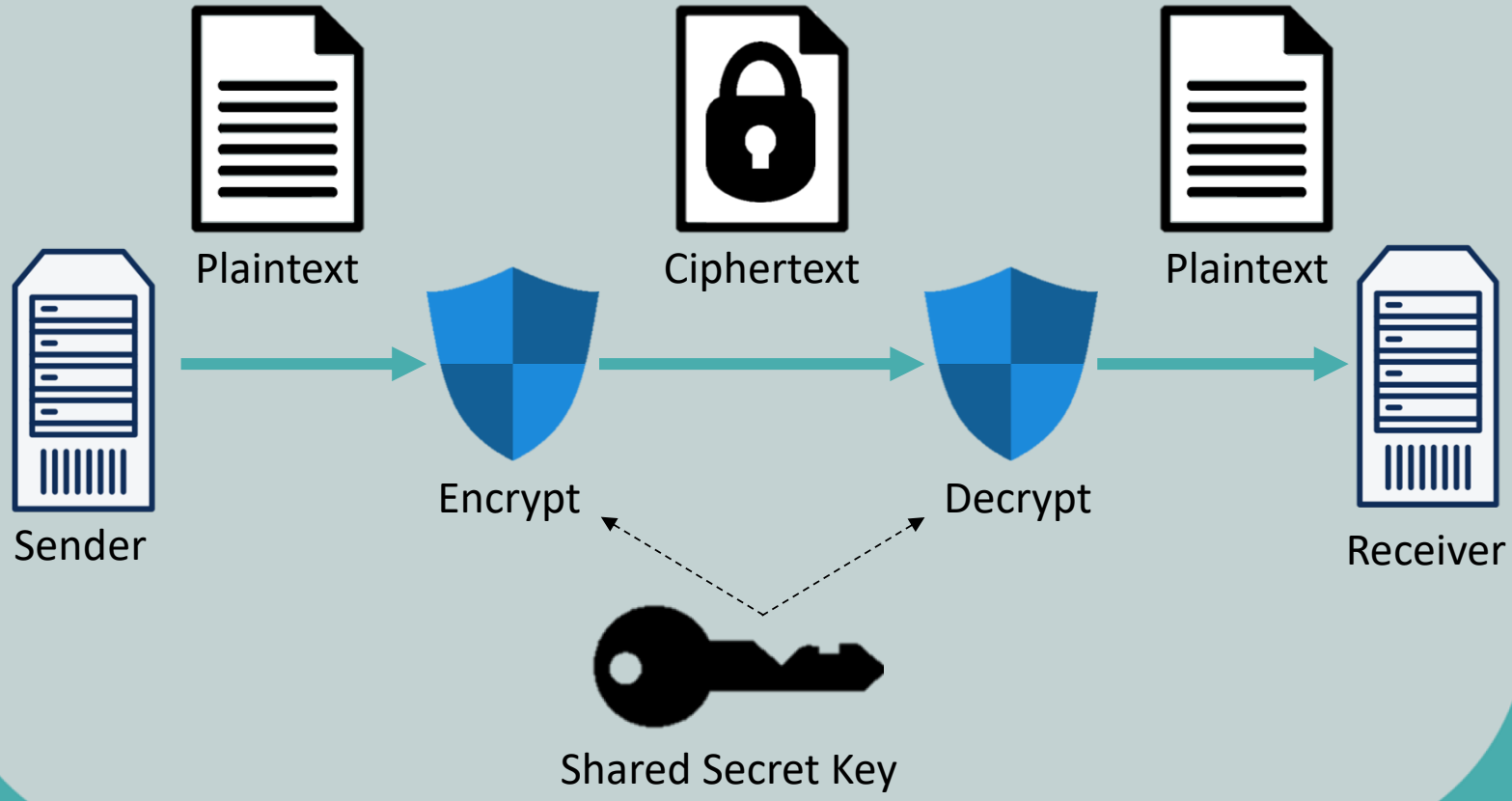


- 3DES (Triple DES)
  - Uses three 56-bit keys (168-bit total)
  - Encrypt, decrypt, encrypt

- AES (Advanced Encryption Standard)
  - Preferred symmetric encryption standard
  - Used by WPA2
  - Available in 128-bit, 192-bit, and 256-bit keys

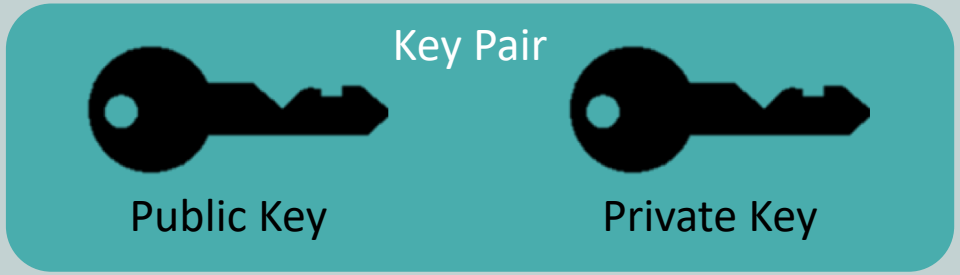
Symmetric Encryption (Confidentiality)

- Sender and receiver use the same key to encrypt and decrypt the messages



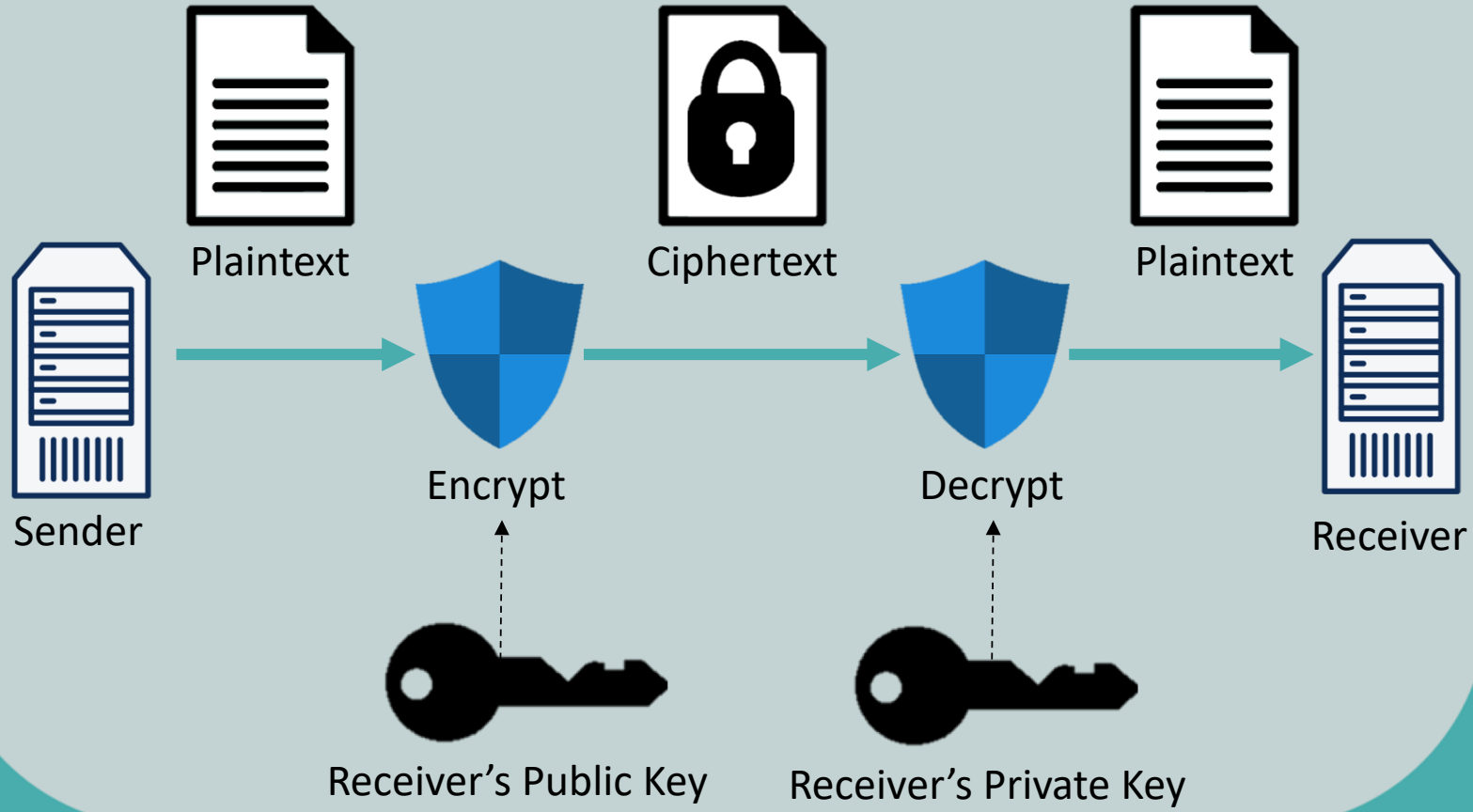
Asymmetric Encryption (Confidentiality)

- Uses different keys for sender and receiver
- RSA is the most popular implementation
- RSA algorithm is commonly used with a public key infrastructure (PKI)
- PKI is used to encrypt data between your web browser and a shopping website
- Can be used to securely exchange emails



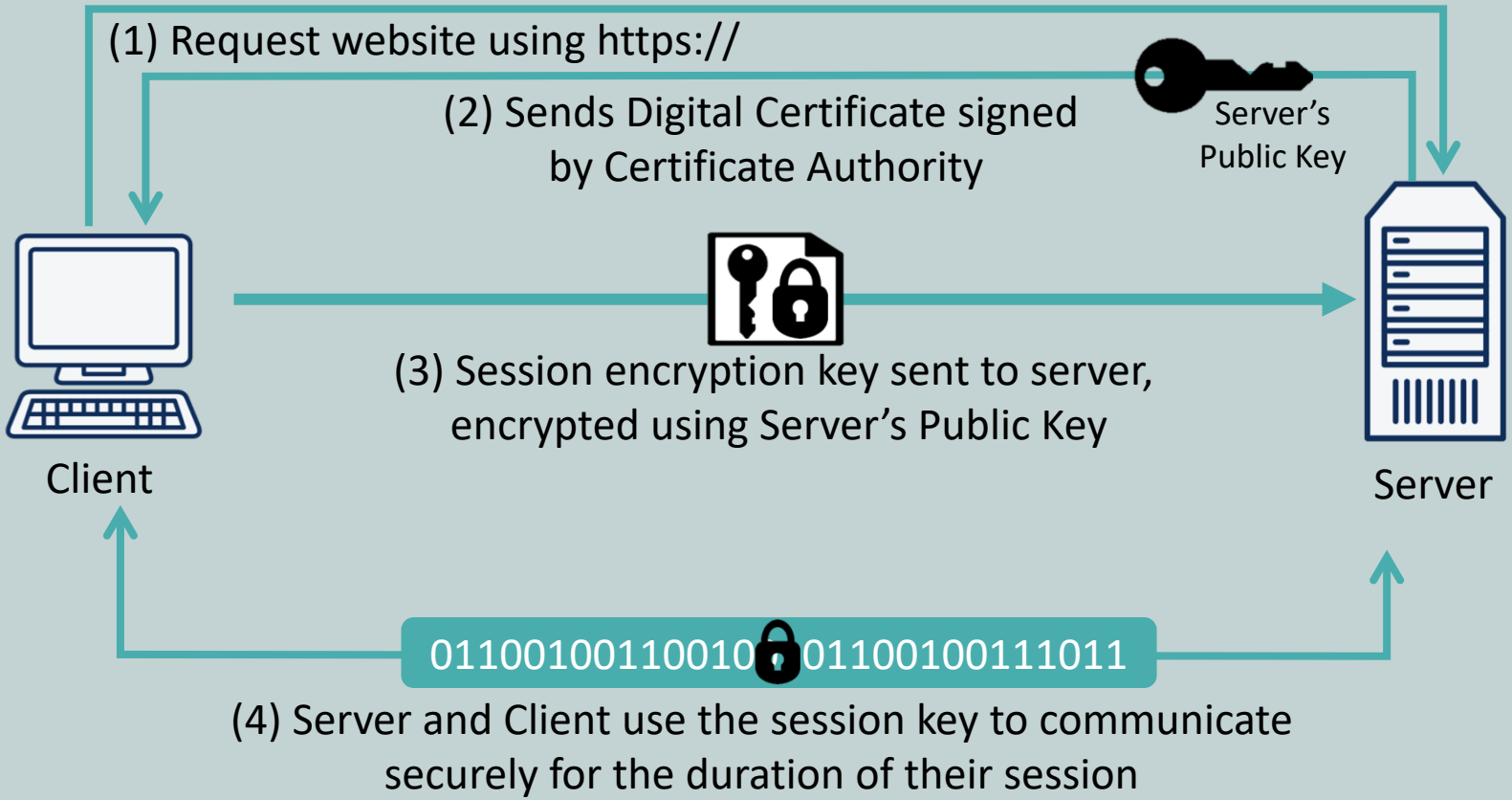
Asymmetric Encryption (Confidentiality)

- Sender and receiver use different keys to encrypt and decrypt the messages



Confidentiality with HTTPS

- Uses asymmetrically encrypted messages to transfer a symmetric key



Integrity

- Ensures data has not been modified in transit
- Verifies the source that traffic originates from
- Integrity violations
  - Defacing a corporate web page
  - Altering an e-commerce transaction
  - Modifying electronically stored financial records

Hashing (Integrity)

1. Sender runs string of data through algorithm
   - Result is a *hash* or *hash digest*

2. Data and its hash are sent to receiver

3. Receiver runs data received through the same algorithm and obtains a hash

4. Two hashes are compared
   - If the same, the data was not modified

password 5f4dcc3b5aa765d61d8327deb882cf99
Password dc647eb65e6711e155375218212b3964
Password. ead0c1b0e080b14538d28a6b3929c6cc

Hashing Algorithms (Integrity)

- Message digest 5 (MD5)
  - 128-bit hash digest

```
Jason (MD5)
472d46cb829018f9
dbd65fb8479a49bb
```

- Secure Hash Algorithm 1 (SHA-1)
  - 160-bit hash digest

```
Jason (SHA-1)
E7e312fea4c2c1aad2bb
075d739111890e1ce08b
```

- Secure Hash Algorithm 256 (SHA-256)
  - 256-bit hash digest

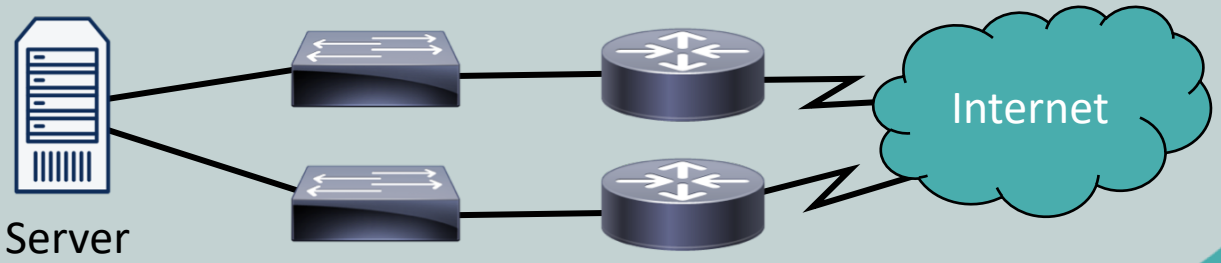
```
Jason (SHA-256)
7fa8a6e9fde2f4e1dfe6fb029af47c96
33d4b7a616a42c3b2889c5226a20238d
```

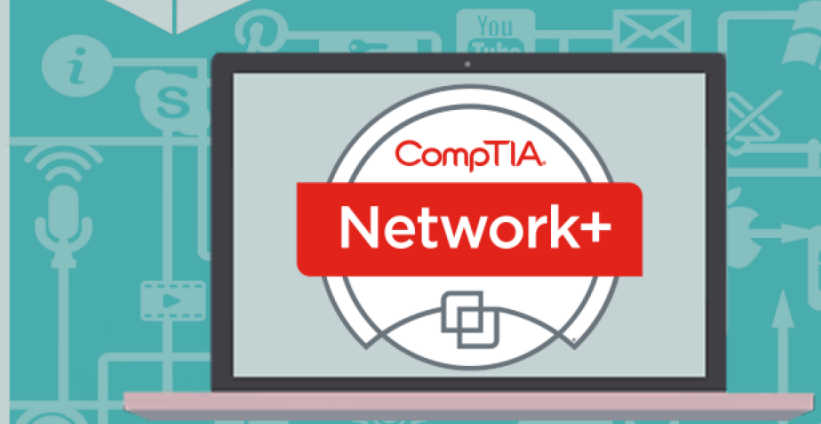
- Challenge-Response Authentication Mechanism Message Digest 5 (CRAMMD5)
  - Common variant often used in e-mail systems

password 5f4dcc3b5aa765d61d8327deb882cf99
Password dc647eb65e6711e15537521821 2b3964
Password. ead0c1b0e080b14538d28a6b3929c6cc

Availability

- Measures accessibility of the data
- Increased by designing redundant networks
- Compromised by
  - Crashing a router or switch by sending improperly formatted data
  - Flooding a network with so much traffic that legitimate requests cannot be processed
    - Denial of Service (DoS)
    - Distributed Denial of Service





Network Security Attacks (Part 1)

CompTIA Network+ (N10-007)

Network Security Attacks

- Our security goals (CIA) are subject to attack
- Confidentiality attack
  - Attempts to make data viewable by an attacker
- Integrity attack
  - Attempts to alter data
- Availability attack
  - Attempts to limit newtork accessibility and usability

Attacks on Confidentiality

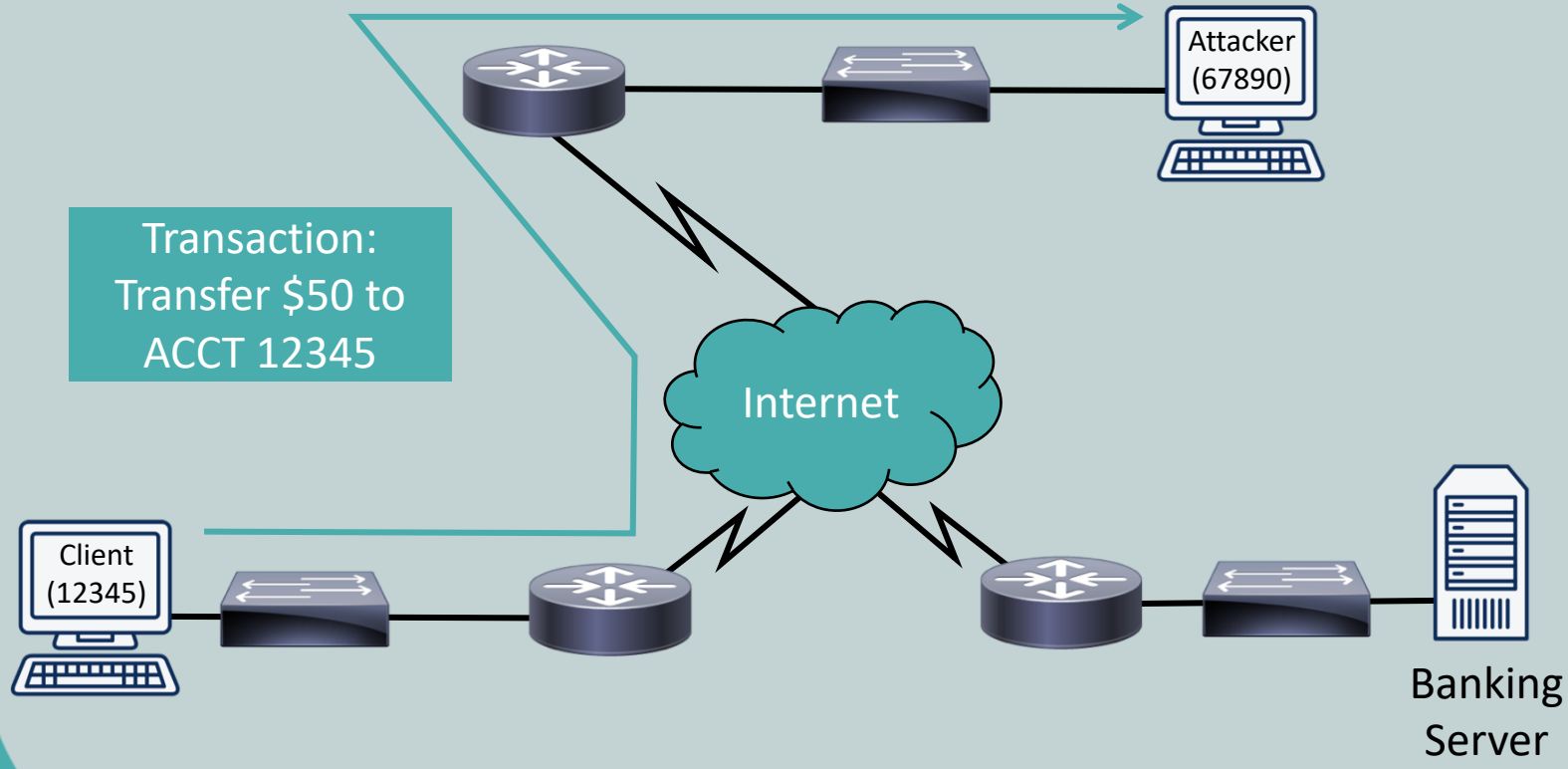
- Packet capture
- Wiretapping
- Dumpster diving
- Ping sweep
- Port scan
- Wireless interception
  - EMI interference interception
- Man-in-the-Middle
- Social engineering
- Malware/Spyware

Attacks on Integrity

- Man-in-the-middle
- Session hijacking
- Data diddling
  - Changes data before storage
- Botnet
- Trust relationship exploitation
- Salami attack
  - Puts together many small attacks to make one big attack
- Password attack
  - Trojan Horse, Packet Capture, Keylogger, Brute Force, Dictionary Attack

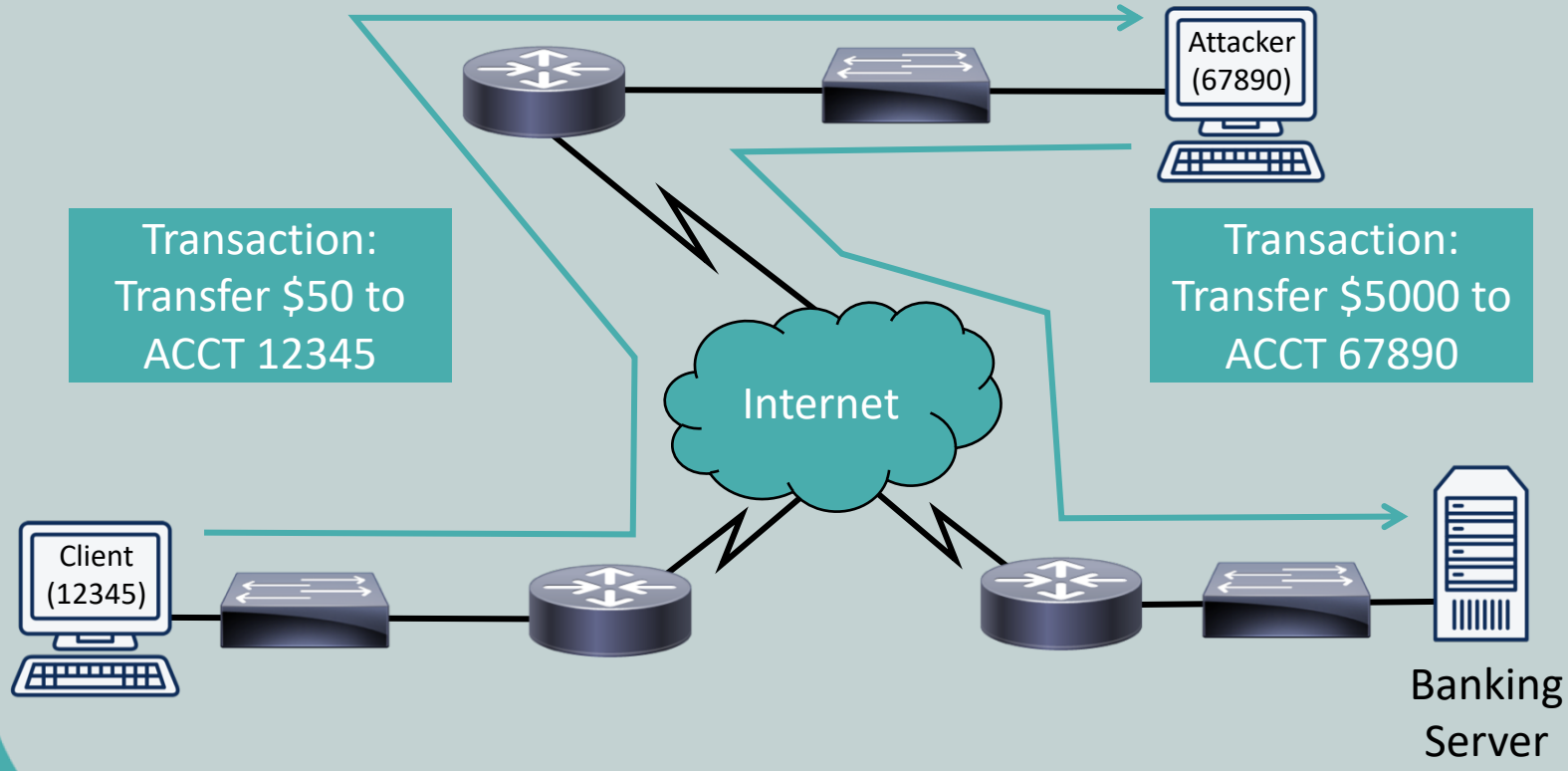
Man-in-the-Middle

- Causes data to flow through the attacker's computer where they can intercept or manipulate the data



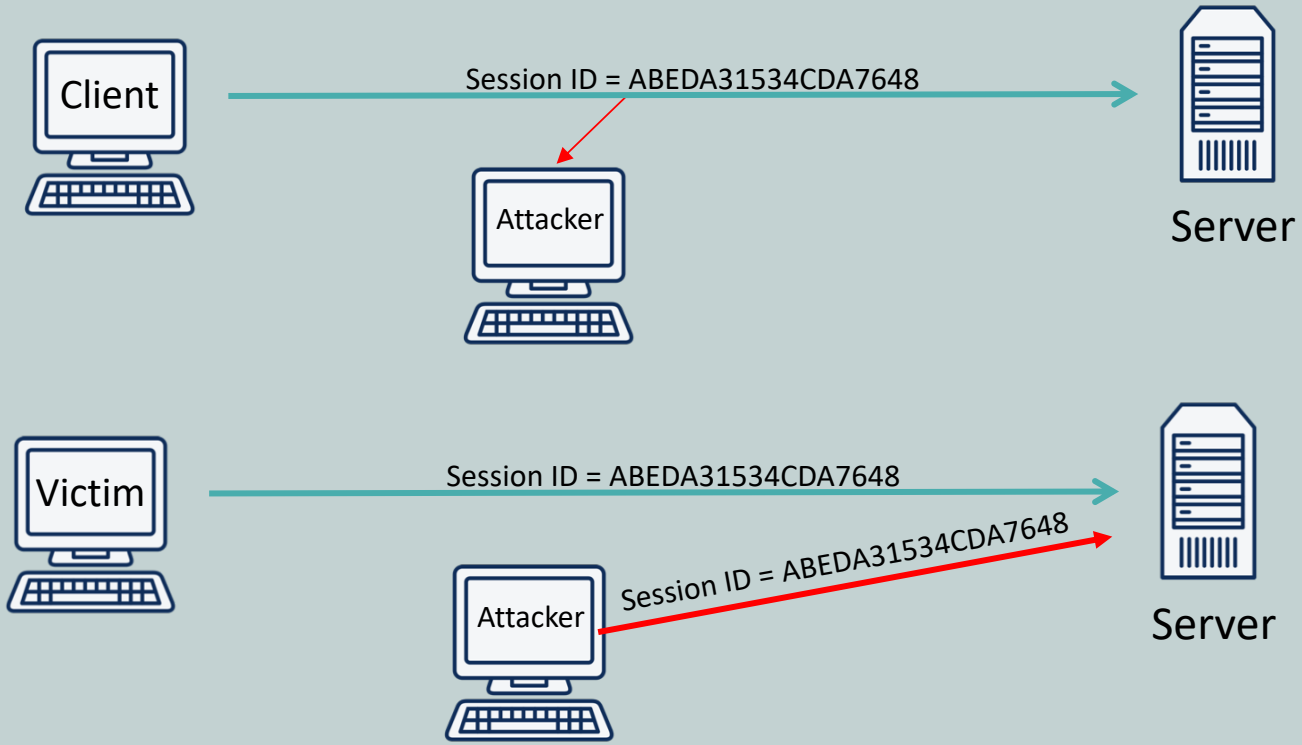
Man-in-the-Middle

- Causes data to flow through the attacker's computer where they can intercept or manipulate the data



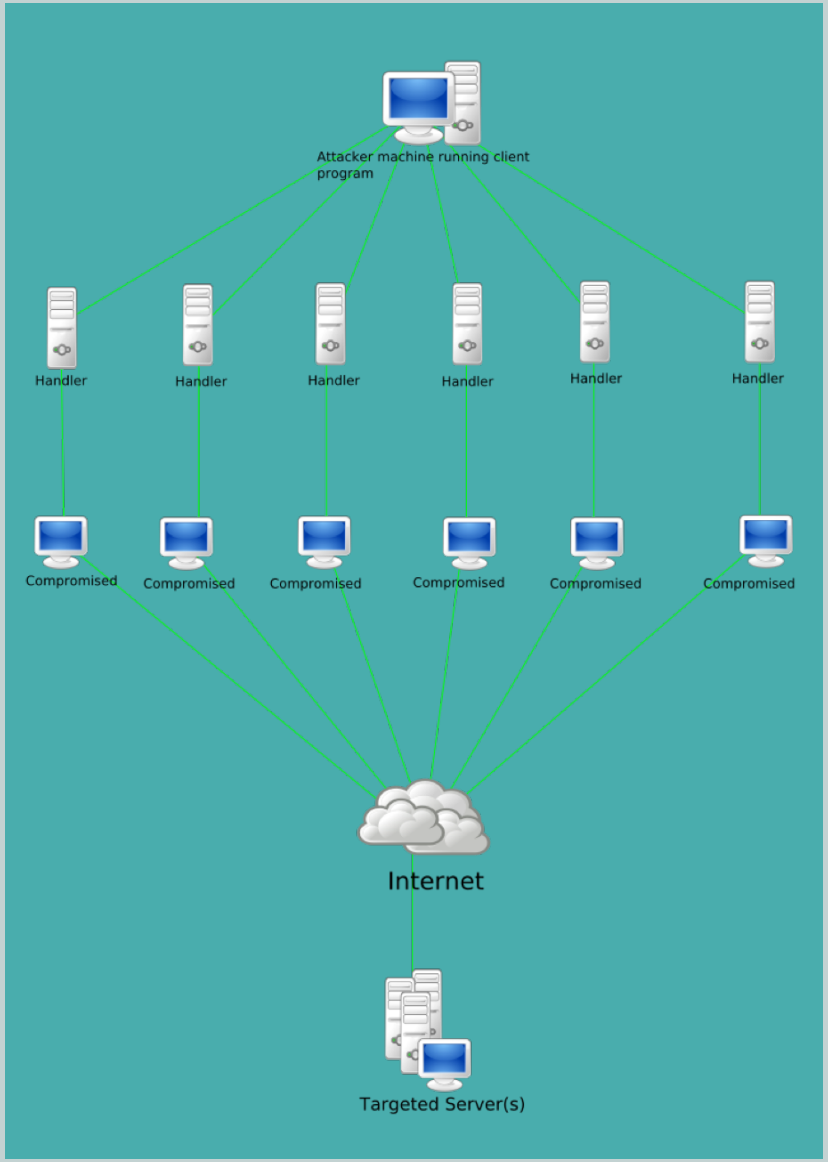
Session Hijacking

- Attacker guesses the session ID for a web session, enabling them to takeover the already authorized session of the client



Botnets

- Software robot that lies on a compromised computer
- Collection of computers (called zombies) can be controlled by a remote server to perform various attacks/functions for the criminals



Network Security Attacks (Part 2)

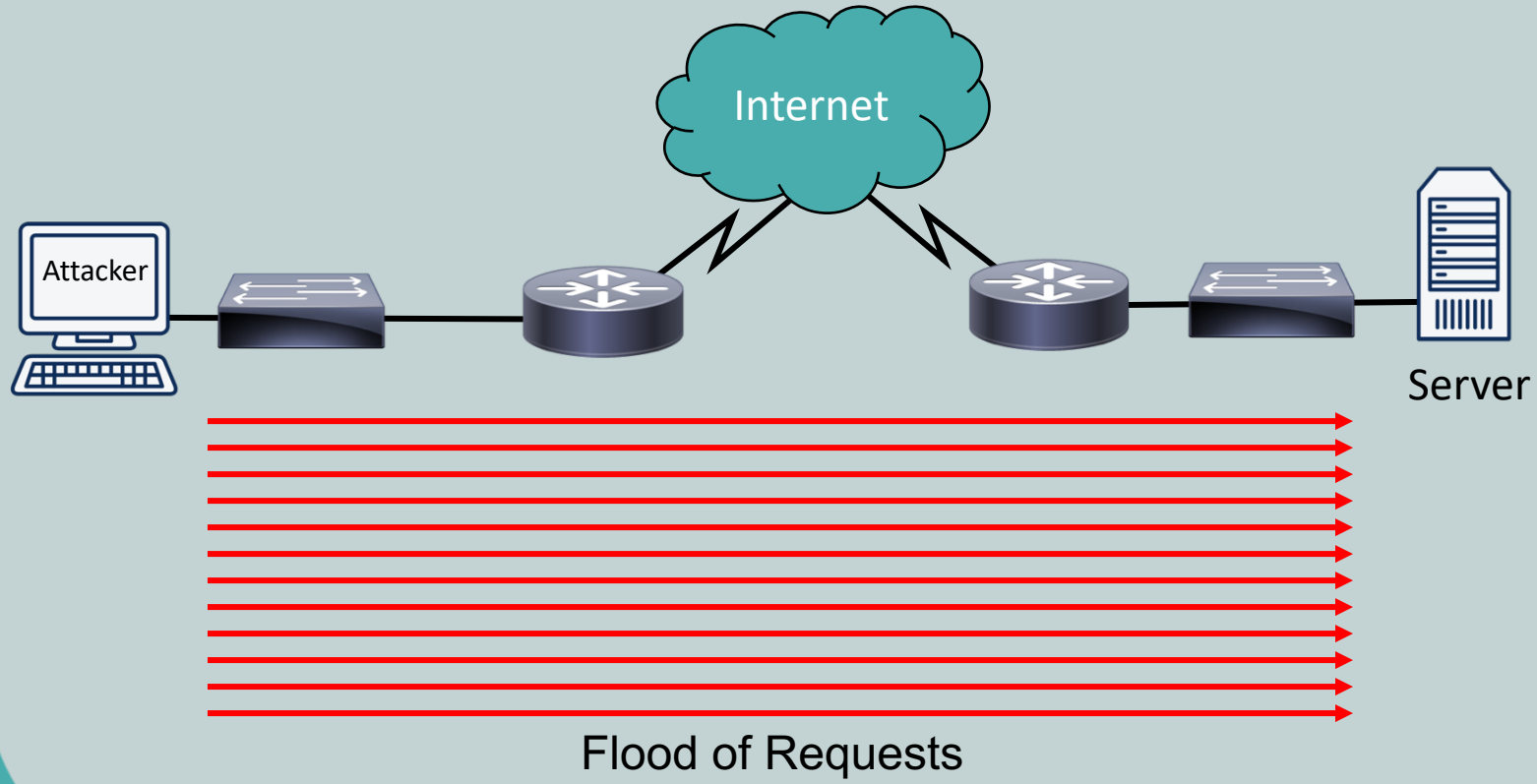
CompTIA Network+ (N10-007)

Attacks on Availability

- Attack vary widely from consuming server resources to physically damaging the system
  - Denial of service (DoS)
  - Distributed Denial of Service (DDoS)
  - TCP SYN flood
  - Buffer overflow
  - ICMP attacks (Smurf)
  - UDP attacks (Fraggle)
  - Ping of Death
  - Electrical disturbances
  - Physical environment attacks

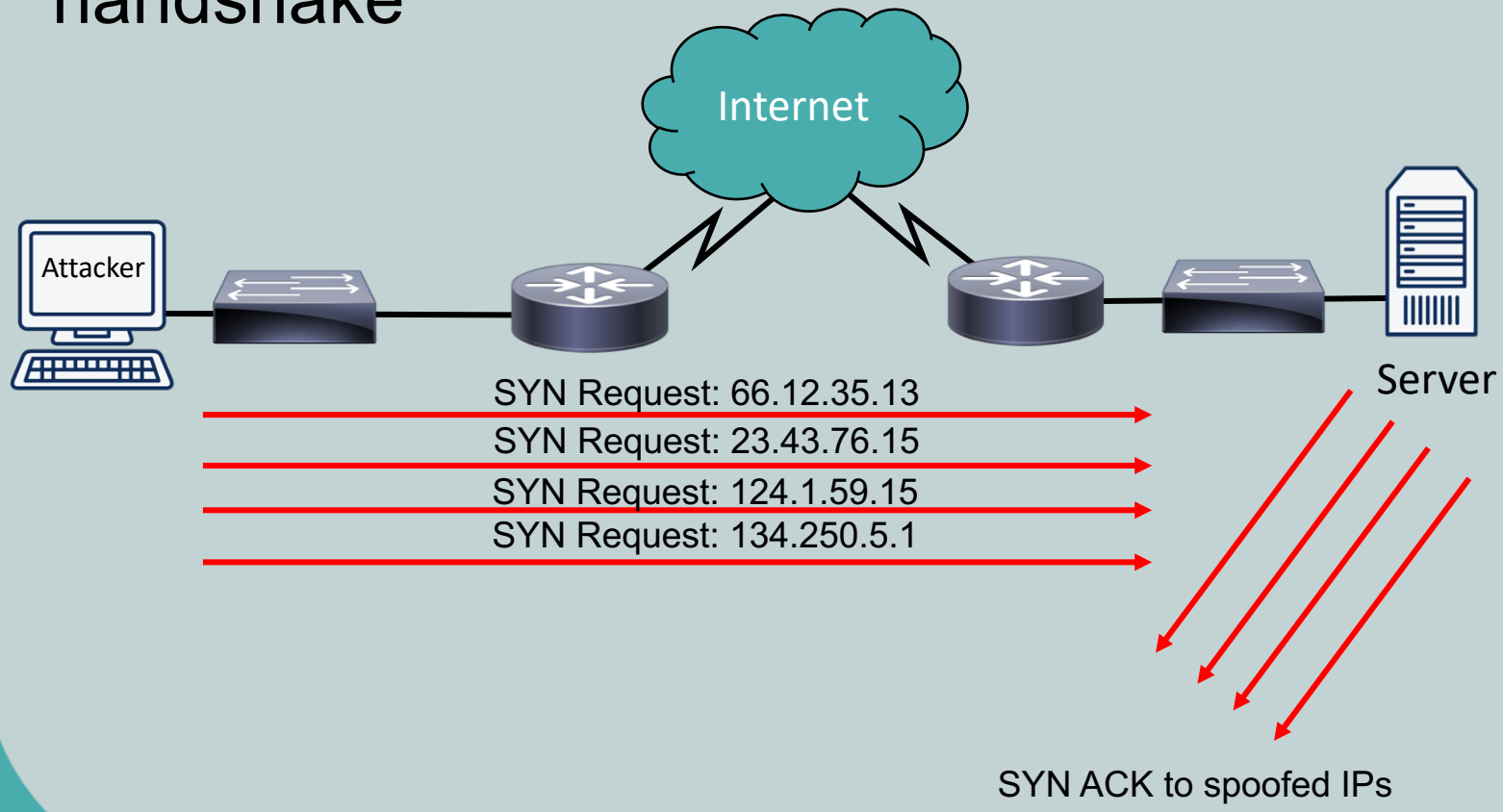
Denial of Service

- Continually floods the victim system with requests for services and causes the system to run out of memory and crash



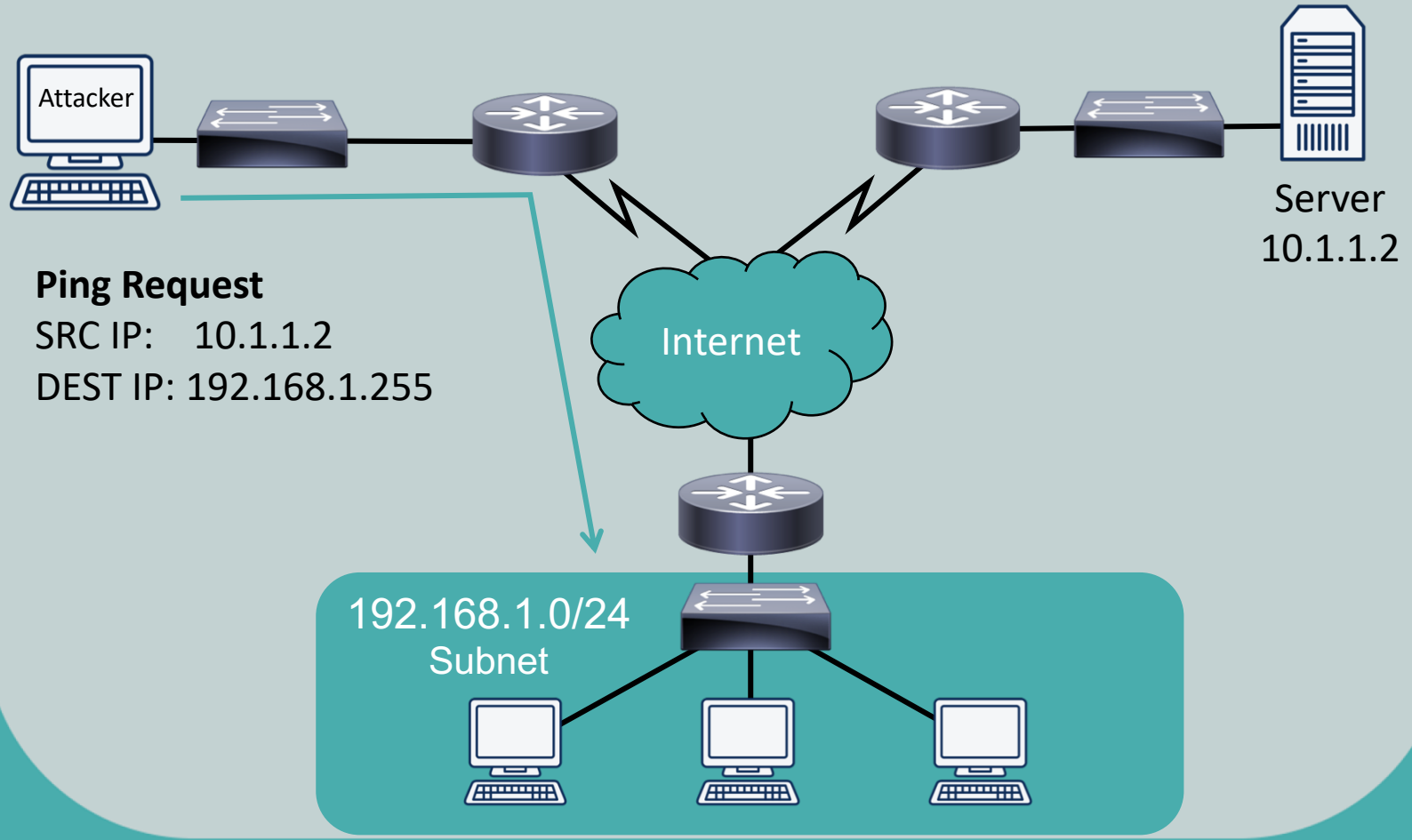
TCP SYN Flood

- Variant on a Denial of Service (DOS) attack where attacker initiates multiple TCP sessions, but never completes the 3-way handshake



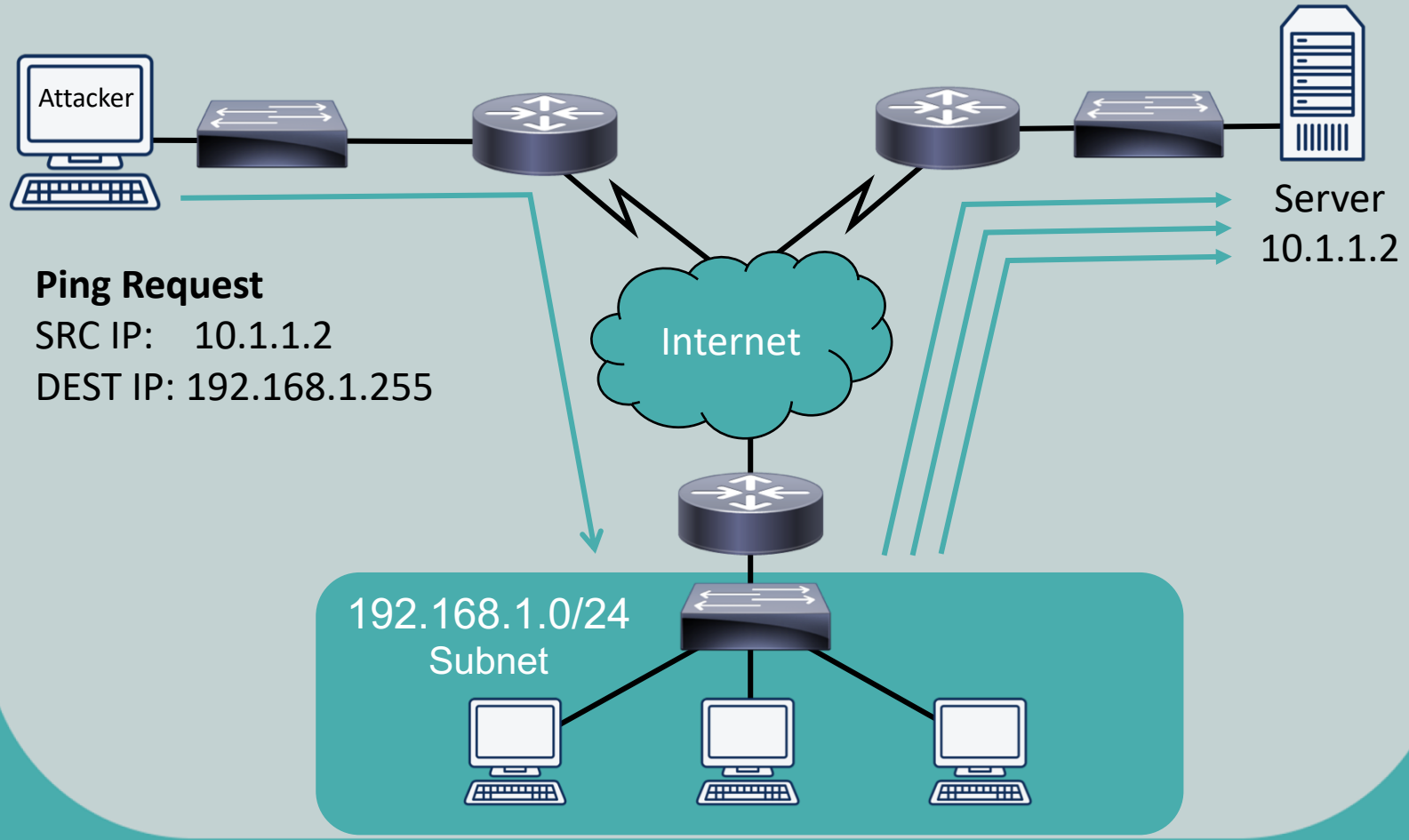
Smurf (ICMP Flood)

- Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (the victim) using up bandwidth and processing



Smurf (ICMP Flood)

- Attacker sends a ping to subnet broadcast address and devices reply to spoofed IP (the victim) using up bandwidth and processing



Electrical Disturbance

- Launched by interrupting or interfering with electrical service available to a system
- Uninterruptable power supply (UPS), line conditioners, and backup generator can help to combat these threats
- Examples
  - Power spikes
  - Electrical surges
  - Power faults
  - Blackouts
  - Power sag
  - Brownout

Physical Environment

- Computing equipment can be damaged by influencing the physical environment
  - Temperature
    - Attacker disturbs the HVAC to overheat your systems
  - Humidity
    - Create a high level of moisture/humidity
  - Gas
    - Inject gas into an environment that could ignite
- Threats generally mitigated through physical restrictions, access credentials, and visual monitoring

Network Security Attacks (Part 3)

CompTIA Network+ (N10-007)

Other Attacks to Consider

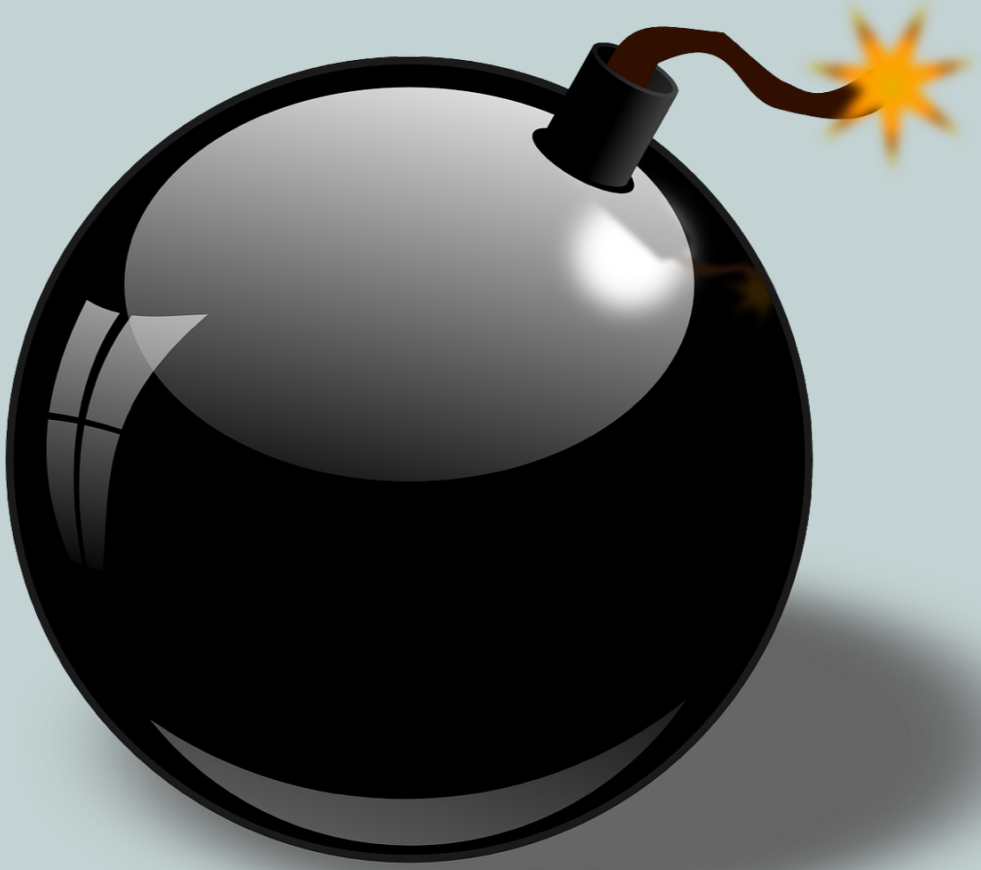
- Insider Threats
- Phishing
- Ransomware
- Logic Bombs
- Deauthentication
- VLAN Hopping

Insider Threats

- Employees or other trusted insiders who use their network access to harm the company

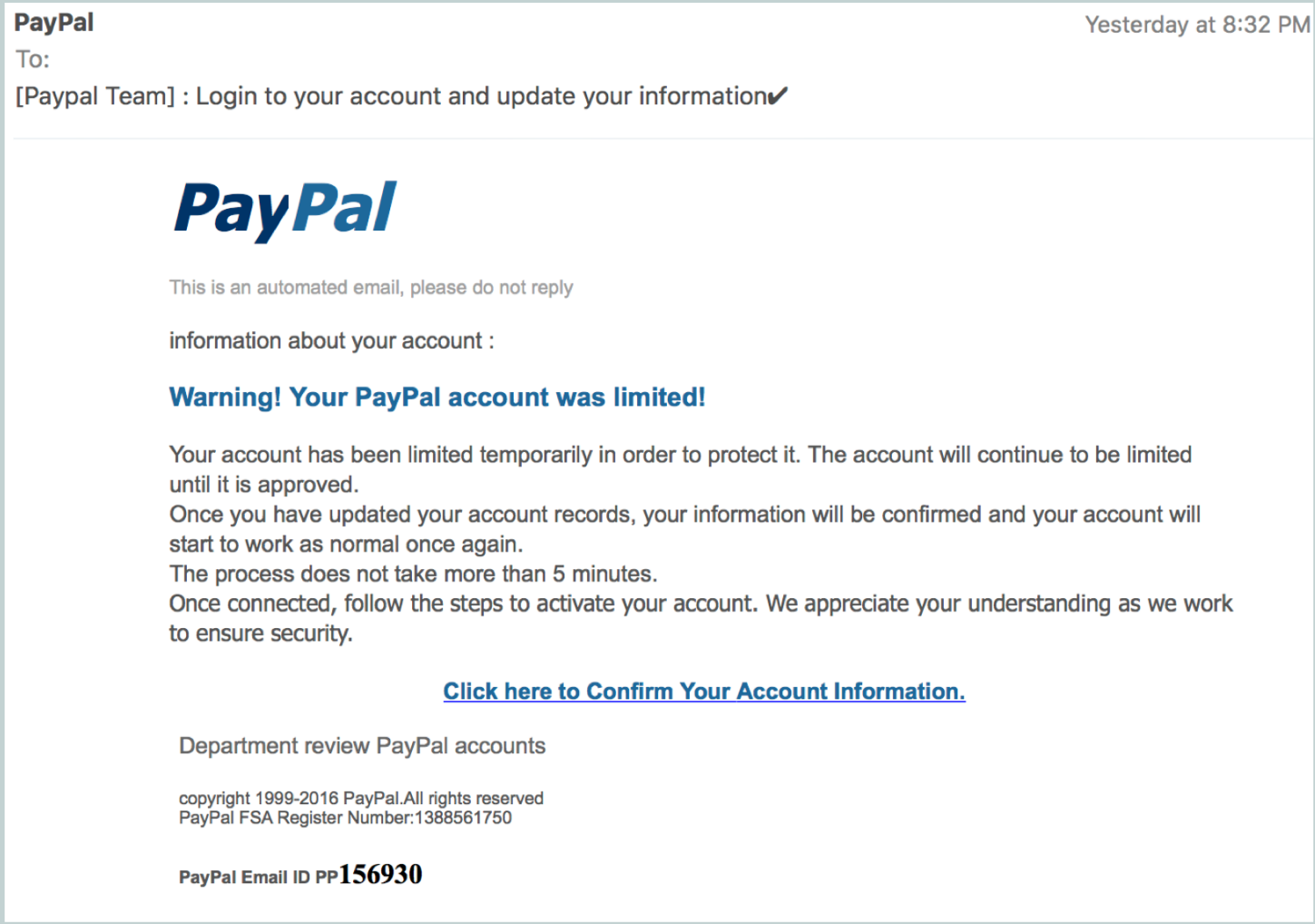
Logic Bomb

- Specific type of malware that is tied to a time or logical event



Phishing

- Attackers send email to get a user to click link



PayPal Yesterday at 8:32 PM

To:

[Paypal Team] : Login to your account and update your information✔

PayPal

This is an automated email, please do not reply

information about your account :

Warning! Your PayPal account was limited!

Your account has been limited temporarily in order to protect it. The account will continue to be limited until it is approved.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.
The process does not take more than 5 minutes.
Once connected, follow the steps to activate your account. We appreciate your understanding as we work to ensure security.

Click here to Confirm Your Account Information.

Department review PayPal accounts

copyright 1999-2016 PayPal.All rights reserved
PayPal FSA Register Number:1388561750

PayPal Email ID PP156930

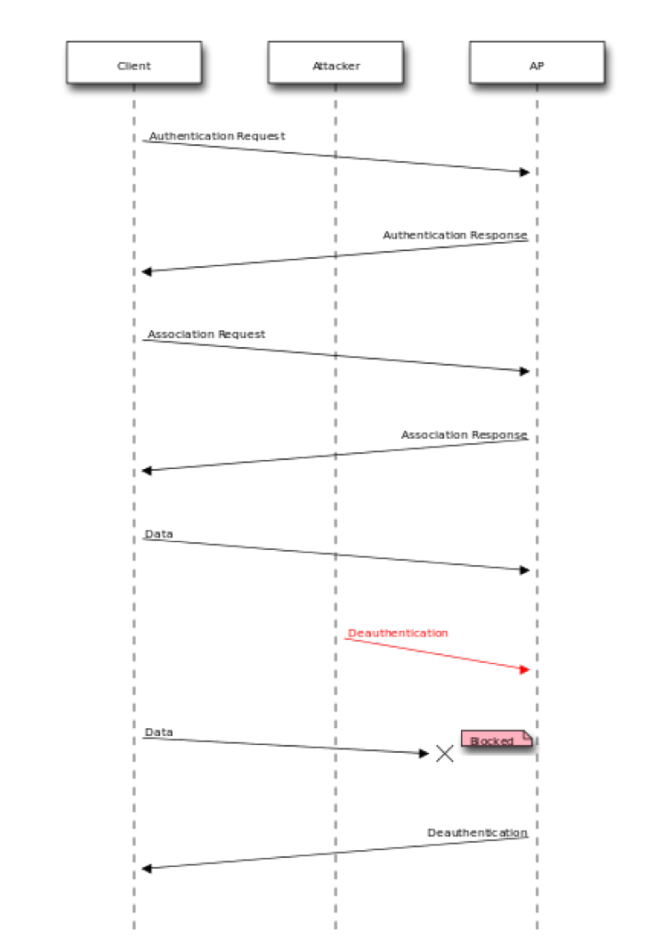
Ransomware

- Attackers gain control of your files, encrypt them, and hold them for a ransom

Deauthentication

- Attacker sends a deauthentication frame a victim to disconnect them from the network

- Often used in wireless hacking attacks



VLAN Hopping

- Attacker physically connects to a different switch port to access a different VLAN
- Manually assigning switch ports and using NAC can help prevent this

```
Switch(config-if)# switchport nonegotiate
Switch(config-if)# switchport mode access
```

Protecting the Network

CompTIA Network+ (N10-007)

Protecting the Network

- To successfully defend a network attacks use
  - Physical controls
  - User training
  - Patching
  - Vulnerability scanners
  - Honey pots and Honey nets
  - Remote-access security
  - Security policies*
  - Incident response*

* Covered in separate lesson*

Physical Controls

- Reduces unauthorized access
- Mantraps
- Keypads
- Locked facilities
- Authenticated access
  - Badges
  - Biometrics
  - Key fobs
  - Passwords/Pins

User Training

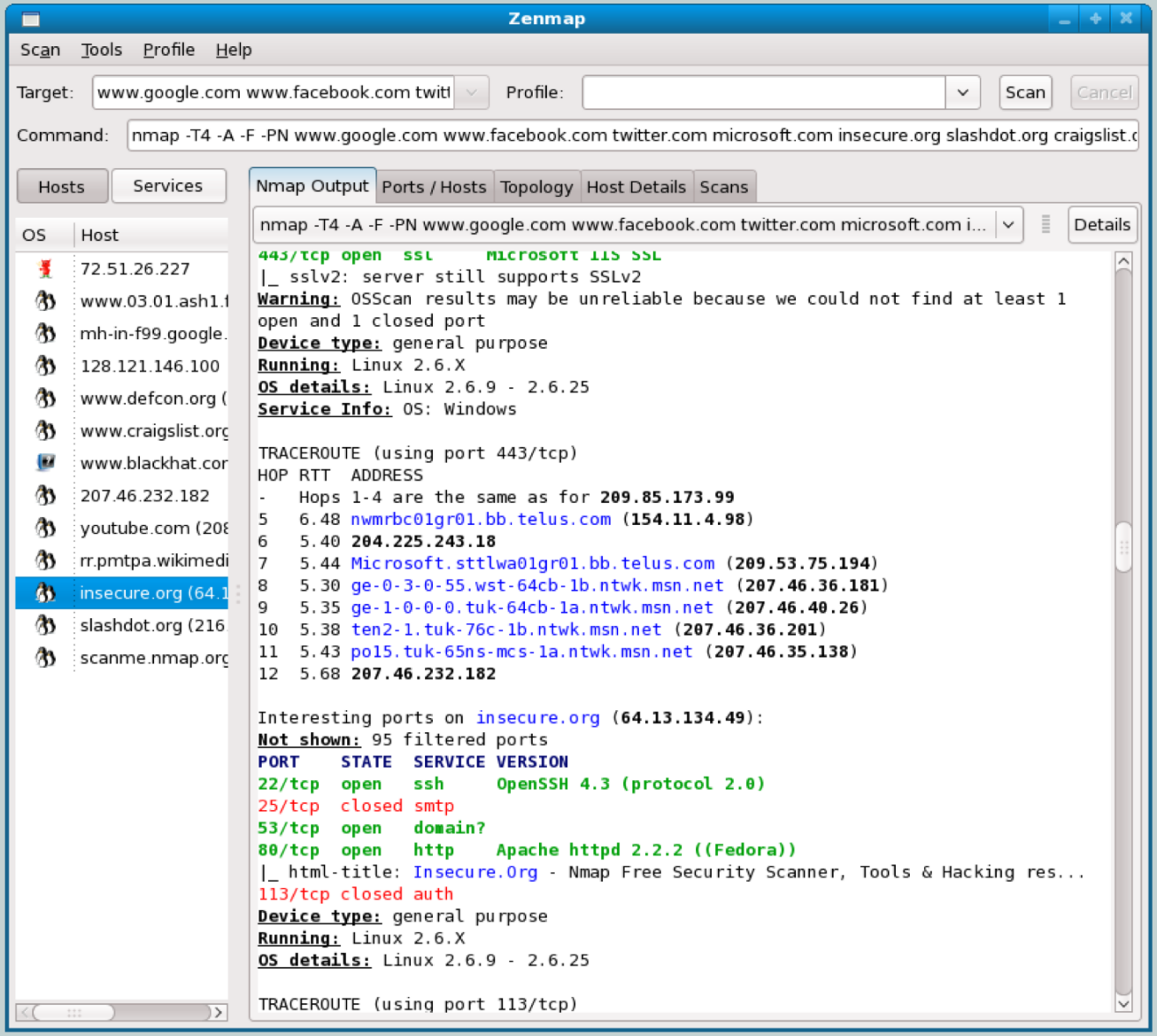
- Users present one of the greatest vulnerabilities to the network

- Training should include
  - Social engineering awareness
  - Virus transmission dangers
  - Password security
  - E-mail security
  - Physical security

Vulnerability Scanners

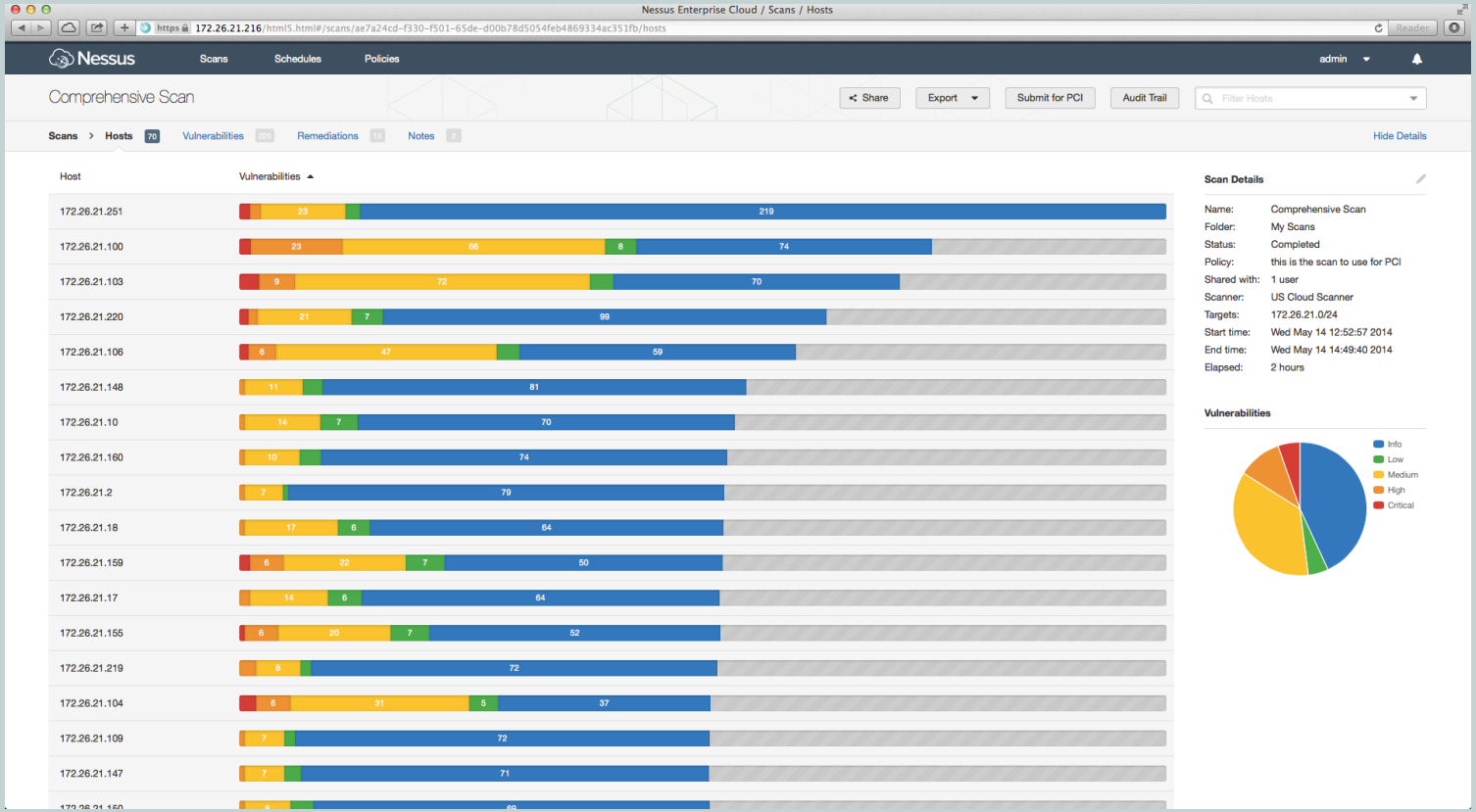
- Periodically test the network to verify that network security components are behaving as expected and to detect known vulnerabilities
- Vulnerability scanners are applications that conduct these tests
- Examples
  - Nessus
  - Zenmap
  - Nmap

Zenmap Vulnerability Scanner

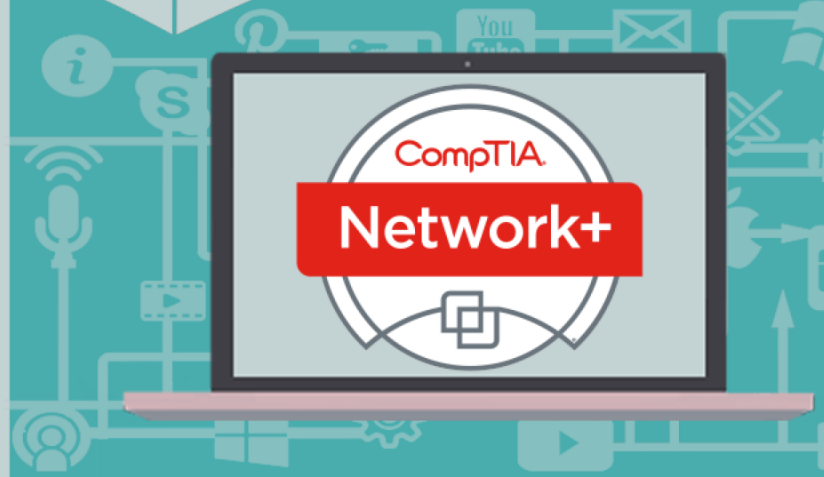


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Nessus Vulnerability Scanner



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

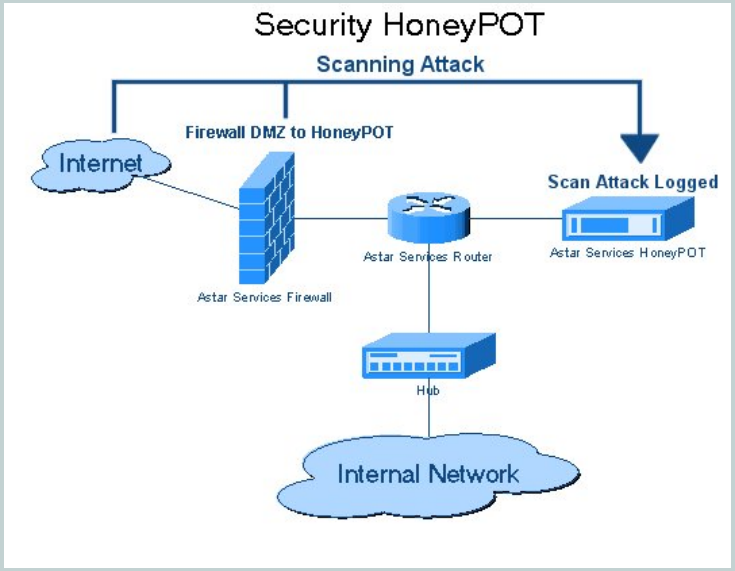


Patching

- Designed to correct a known bug or fix a known vulnerability in programs and apps
- Should be implemented as they become available
- *Updates add new features, but patches fix known vulnerabilities*

Honey Pots and Honey Nets

- Systems designed as an attractive target
  - Distraction for the attacker
- Attackers use their resources attacking the honey pot and leave the real servers alone
  - Honey pot is a single machine
  - Honey net is a network of multiple honey pots
- Used to study how attackers conduct attacks



Remote Access Security

- Controls access to network devices such as routers, switches, servers, and clients

Method	Description
SSH	Secure remote access via terminal emulator
RADIUS	Open standard, UDP-based authentication protocol
TACACS+	Cisco proprietary, TCP-based authentication protocol
Kerberos	Authentication in Windows domains
IEEE 802.1X	Permits or denies a wired or wireless client access to a LAN
Two-factor authentication	Requires two types of authentication: Something you know, Something you have, or Something you are
Single sign-on	Authenticate once and access multiple systems

Security Policies

CompTIA Network+ (N10-007)

Security Policy

- Lack of a security policy, or lack of enforcement of an existing policy, is a major reason for security breaches

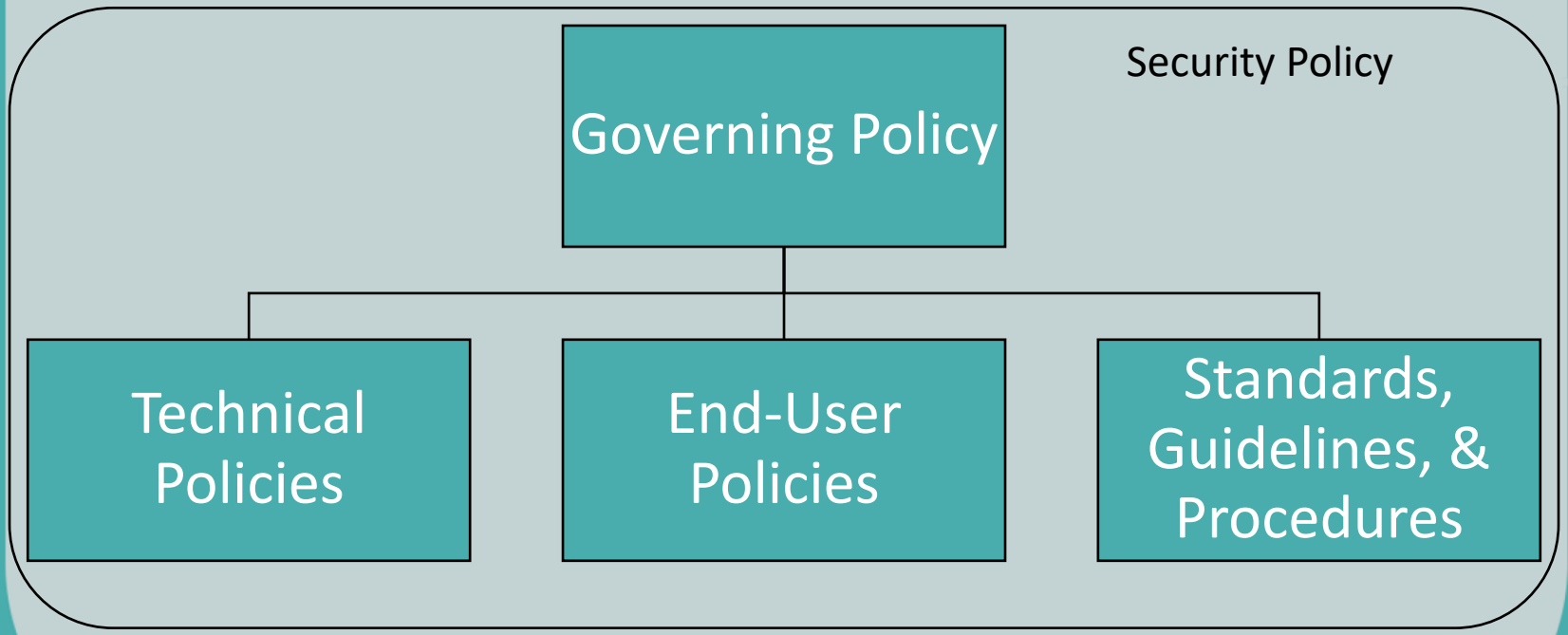
- Security policies serve multiple purposes
  - Protecting an organization's assets
  - Making employees aware of their obligations
  - Identifying specific security solutions
  - Acting as a baseline for ongoing security monitoring

- Acceptable Use Policy (AUP) is a common component of a corporate security policy

Security Policy

- Security policies contain a myriad of other complementary policies

- Larger organizations have complex policies



Parts of a Security Policy

- Governing Policy
  - Focused toward technicians and managers
  - High level document that focuses the organization
- Technical Policies
  - Password, E-mail, Wireless, Remote Access, and Bring Your Own Device (BYOD)
- End-User Policies
  - Acceptable Use (AUP), Privileged User Agreement, Onboarding/Off-boarding, Consent to Monitoring, Non-Disclosure (NDA), Cellular, etc.
- Standards, Guidelines, Procedures

Bring Your Own Device (BYOD)

- BYOD brings new vulnerabilities
  - Bluejacking
    - Sending of unauthorized messages over Bluetooth
  - Bluesnarfing
    - Provides unauthorized access to wireless through Bluetooth
  - Bluebugging
    - Unauthorized backdoor to connect Bluetooth back to attacker

Data Loss Prevention

- Policy that seeks to minimal accidental or malicious data losses
- Policy should cover the entire network, not just email or file storage
- How will your organization guard sensitive data at the…
  - Client level (data in operation)
  - Network level (data in transit)
  - Storage level (data at rest)

System Lifecycle

- You are responsible for your systems from cradle to grave…
  - Conceptual Design
  - Preliminary Design
  - Detailed Design
  - Production and Installation
  - Operations and Support
  - Phase Out
  - Disposal

How are you planning to dispose of your hard drives and devices when they aren't useful?

Licensing Restrictions and Export Controls

- All software needs to have proper licensing, including any virtual machines

- Some items are restricted from being exported to certain regions of the world (cryptography)
  - If your organization crosses international borders, check with your legal and compliance teams to ensure you aren't breaking any laws

Incident Response

- How will you react to a security violation?
- Prosecuting computer crimes can be difficult
- Successful prosecution relies on
  - Means
    - Did suspect have technical skills to perform the attack?
  - Motive
    - Why would they perform the attack?
  - Opportunity
    - Do they have the time and access?

Multifactor Authentication

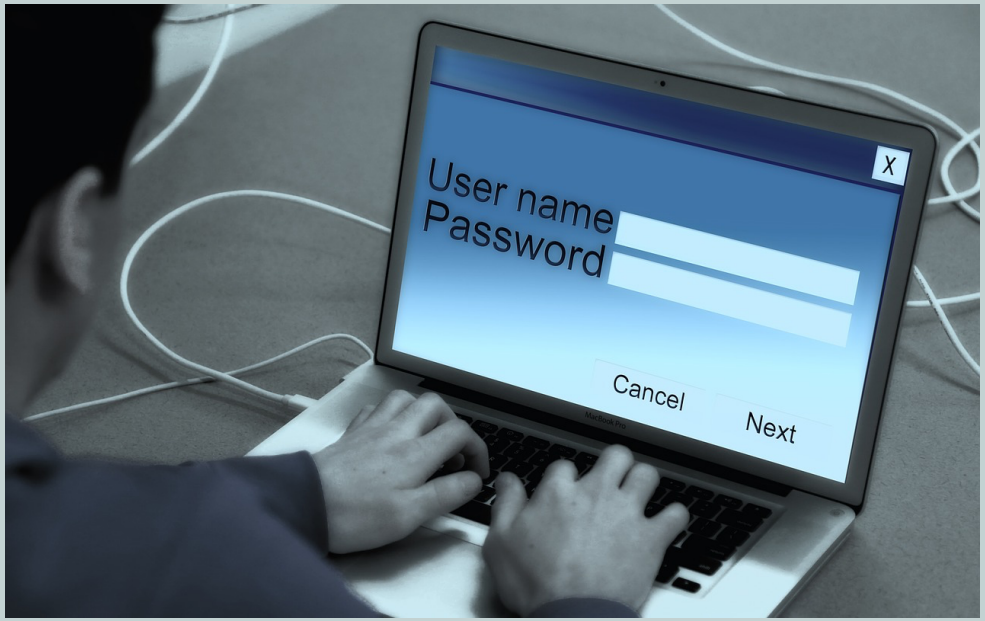
CompTIA Network+ (N10-007)

Multifactor Authentication

- Something you know
- Something you have
- Something you are
- Something you do
- Somewhere you are

Something You Know (Knowledge Factor)

- Usernames
- Passwords
- PINs
- Answers to personal questions



Weaknesses of Passwords

- Not changing the default credentials
- Using common passwords
- Weak and short passwords

Something You Have (Possession Factor)

- Smartcard
  - Stores digital certificates on the card which are accessed once a valid PIN is provided
- Key fobs
- RFID tags

Something You Are (Inherence Factor)

- Fingerprints
- Retina scans
- Voice prints

Something You Do (Action Factor)

- How you sign your name
- How you draw a particular pattern
- How you say a certain passphrase

Somewhere You Are (Location Factor)

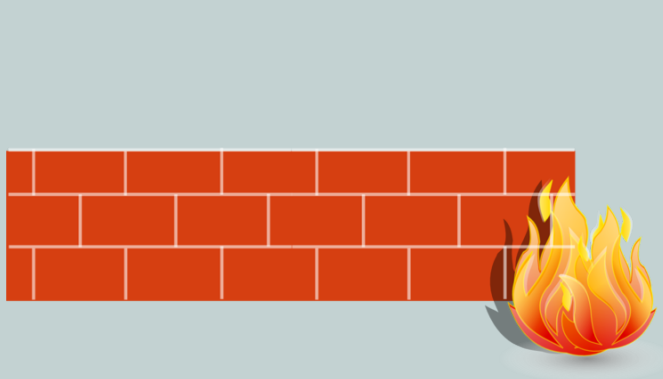
- Geotagging
- Geofencing

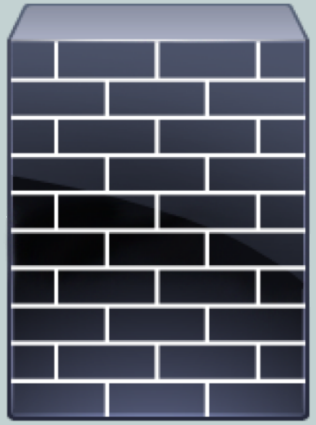
Firewalls

CompTIA Network+ (N10-007)

Firewalls

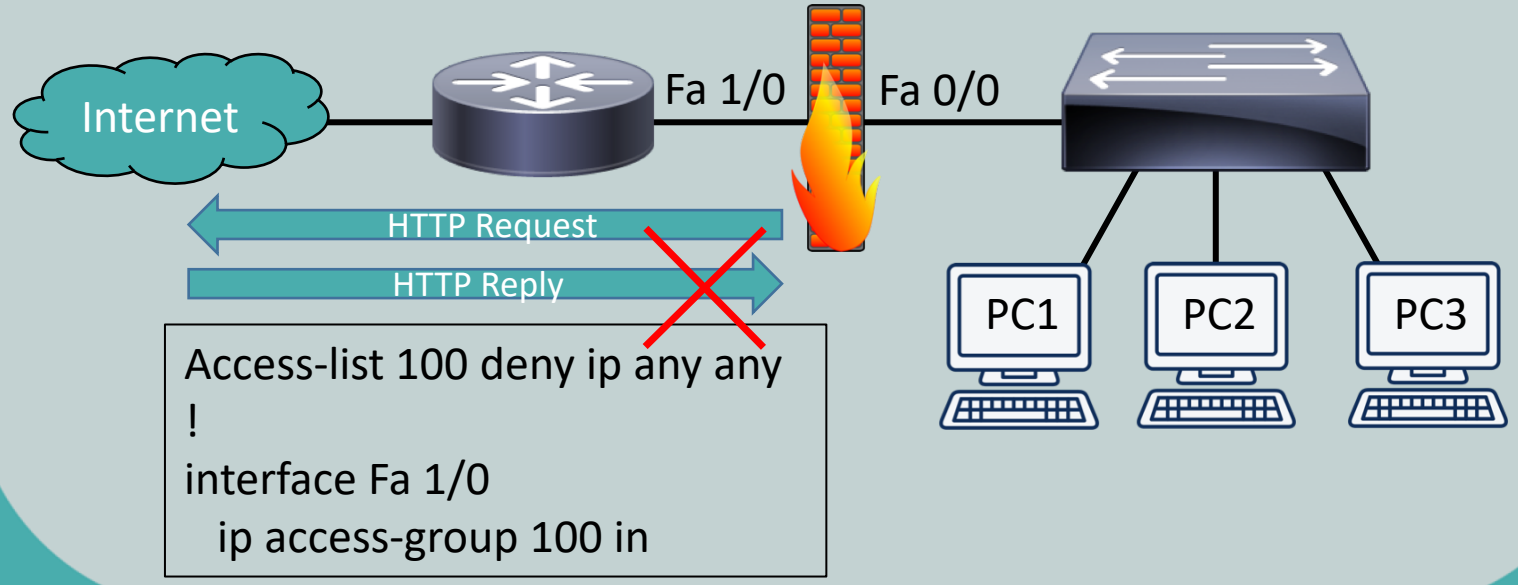
- Uses a set of rules defining the types of traffic permitted or denied through the device
- Can be either software or hardware
- Also can perform Network Address Translation (NAT) or Port Address Translation (PAT)





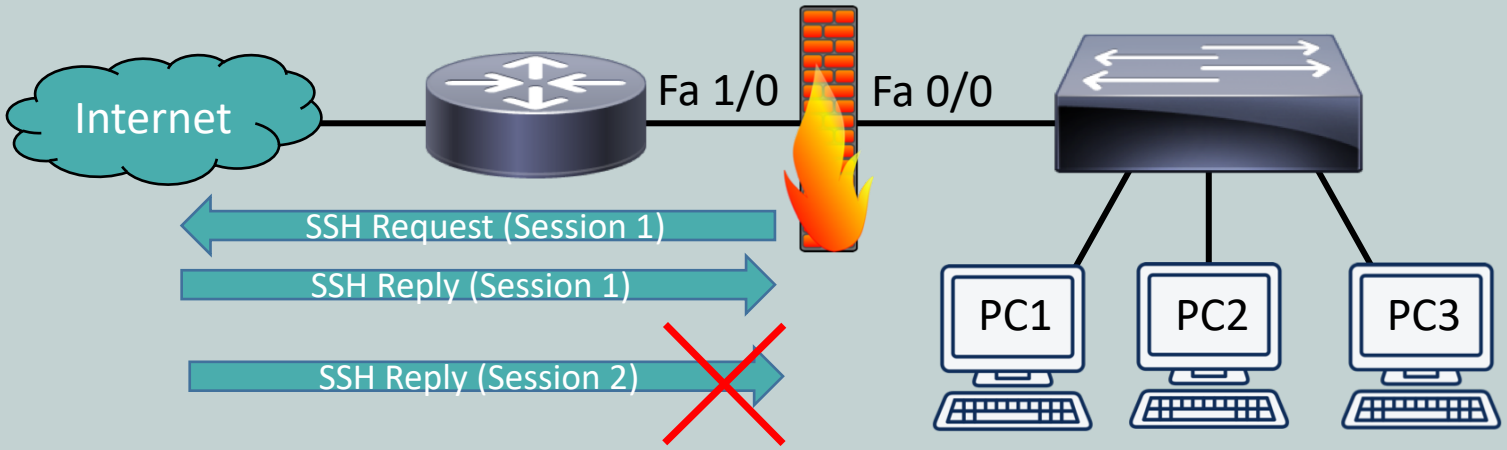
Packet-Filtering Firewalls

- Permits or denies traffic based on packet header
  - Source IP address/port number
  - Destination IP address/port number
- Looks at each packet individually



Stateful Firewalls

- Inspects traffic as part of a session
- Recognizes whether traffic originated from inside or outside the LAN



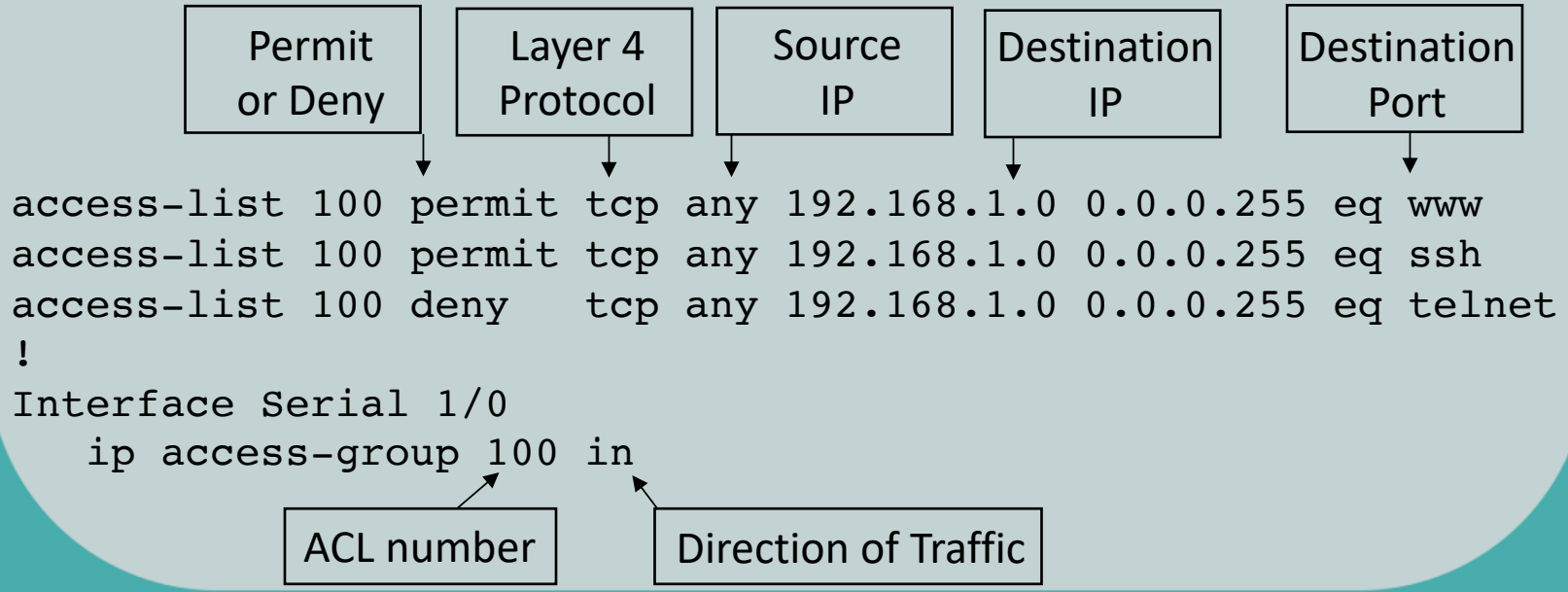
NextGen Firewalls (NGFW)

- Third generation firewalls that conduct deep packet inspection and packet filtering
- Operates at higher levels of the OSI model than traditional stateful firewalls
- Web Application Firewalls are a good example of these, as they inspect HTTP traffic

Access Control List (ACL)

- Set of rules typically applied to router interfaces that permit or deny certain traffic

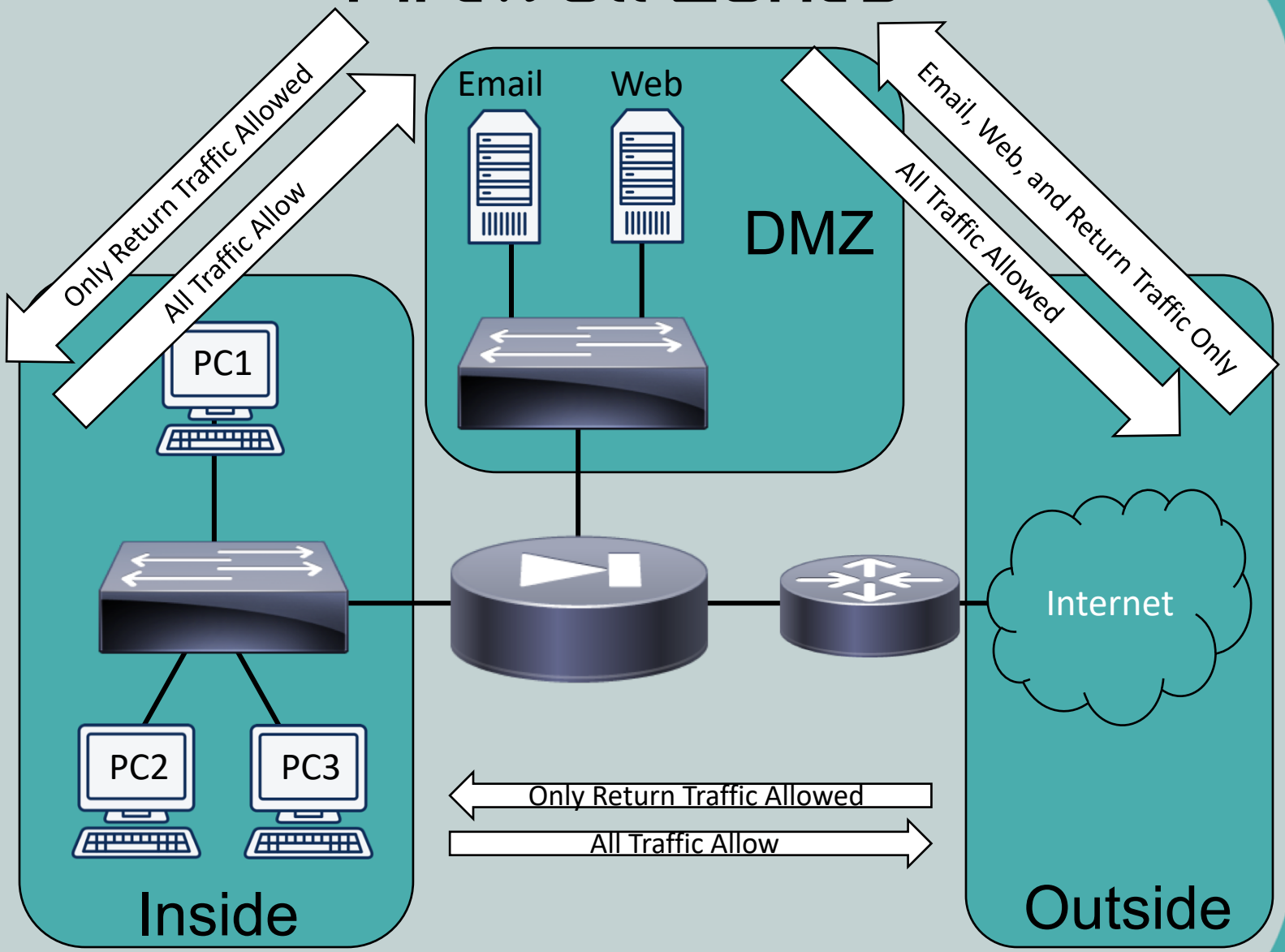
- ACL filtering criteria includes:
  - Source IP, Port, or MAC
  - Destination IP, Port, or MAC



Firewall Zones

- Firewall interfaces can be defined as zones
- You set up rules based on those zones
- Typical zones
  - Inside
    - Connects to your corporate LAN
  - Outside
    - Typically connects to the Internet
  - DMZ (Demilitarized Zone)
    - Connects to devices that should have restricted access from the outside zone (like web servers)

Firewall Zones



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Unified Threat Management (UTM) Devices

- Device that combines firewall, router, intrusion detection/prevention system, antimalware, and other security features into a single device
- Agent is run on an internal client and can be queried by the UTM before allowing connection to the network
- UTM can be purchased as a physical device to install in your network, or you can look to a cloud solution

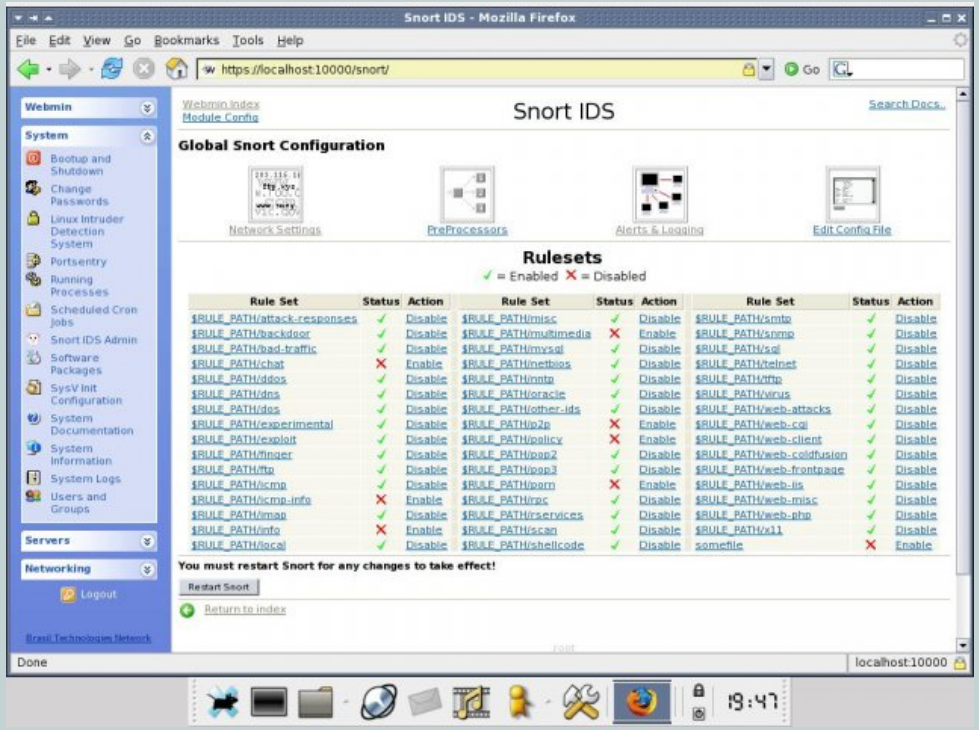
IDS and IPS

CompTIA Network+ (N10-007)

Intrusion Detection System and Intrusion Prevention System

- Can recognize a network attack and respond appropriately

- Incoming data streams are analyzed for attacks using different detection methods

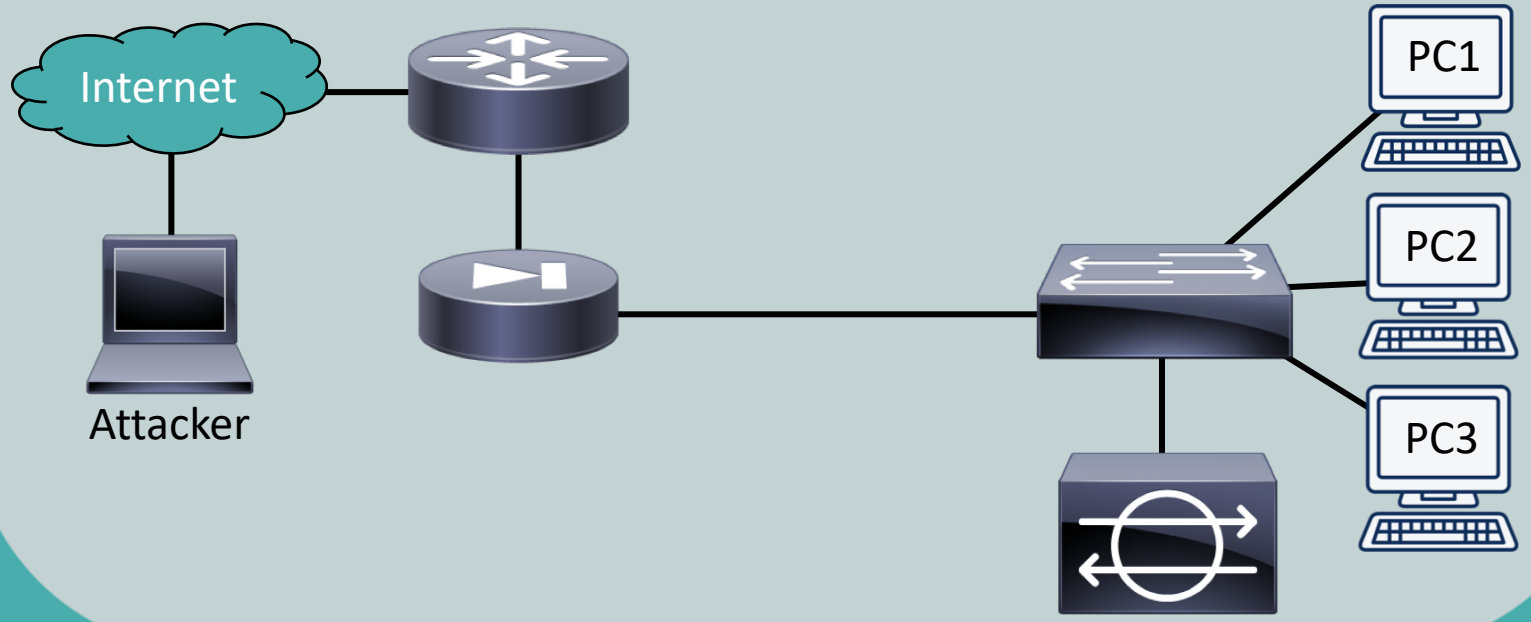


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

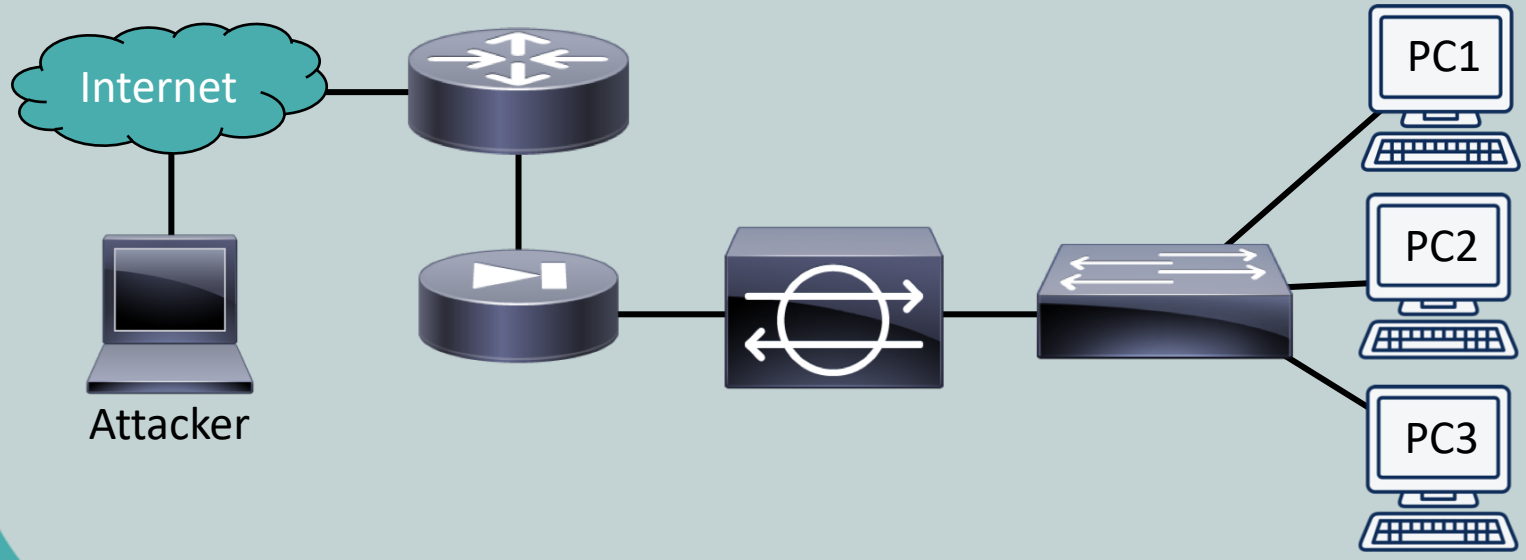
Intrusion Detection System

- Passive device
- Operates parallel to the network
- Monitors all traffic and sends alerts



Intrusion Prevention System

- Active device
- Operates in-line to the network
- Monitors all traffic, sends alerts, and drops or blocks the offending traffic



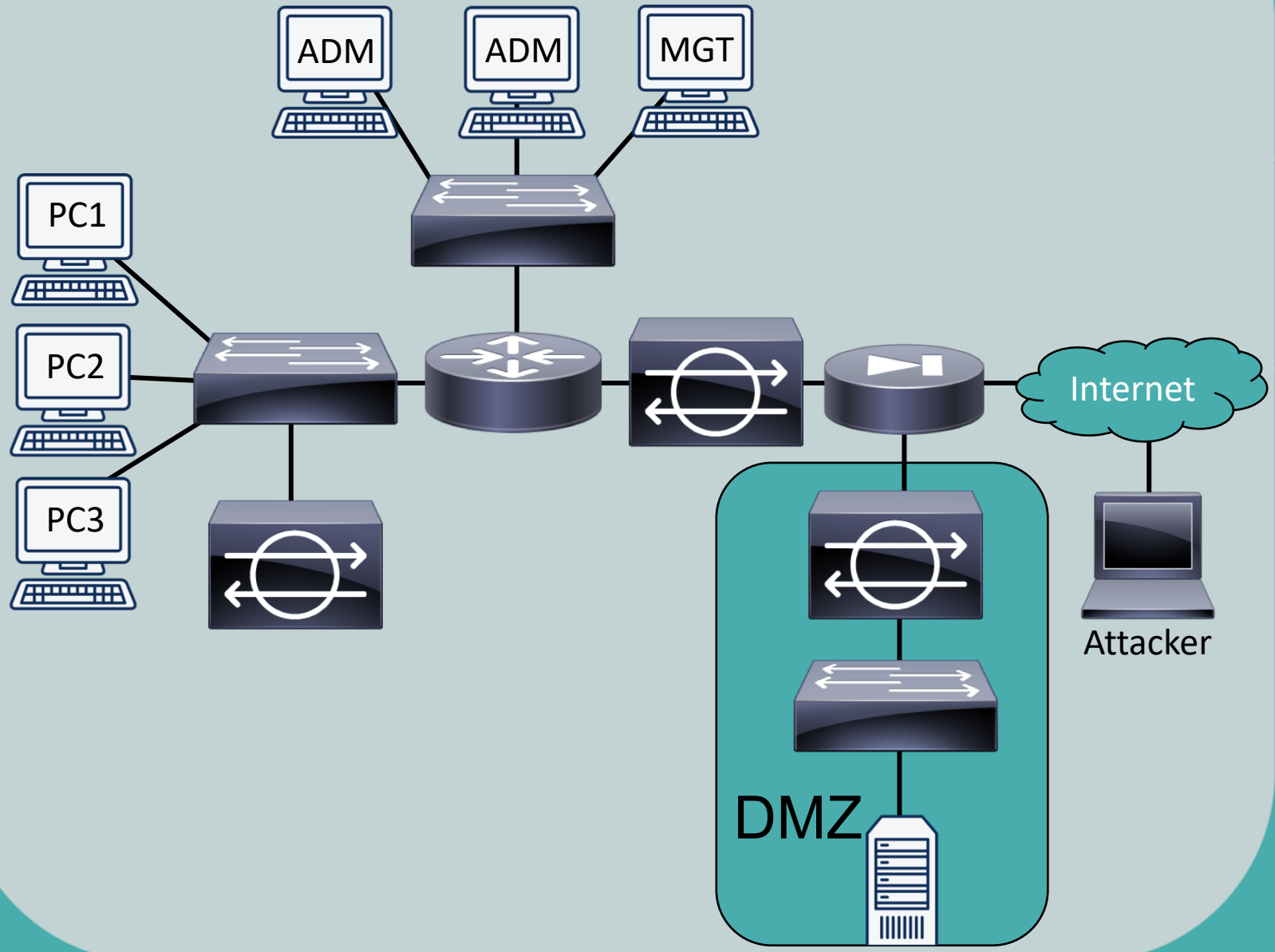
Detection Methods

- Signature-based detection
  - Signature contains strings of bytes (a pattern) that triggers detection
- Policy-based detection
  - Relies on specific declaration of the security policy
  - Example: No Telnet allowed
- Anomaly-based detection
  - Statistical anomaly
    - Watches traffic patterns to build baseline
  - Non-statistical anomaly
    - Administrator defines the patterns/baseline

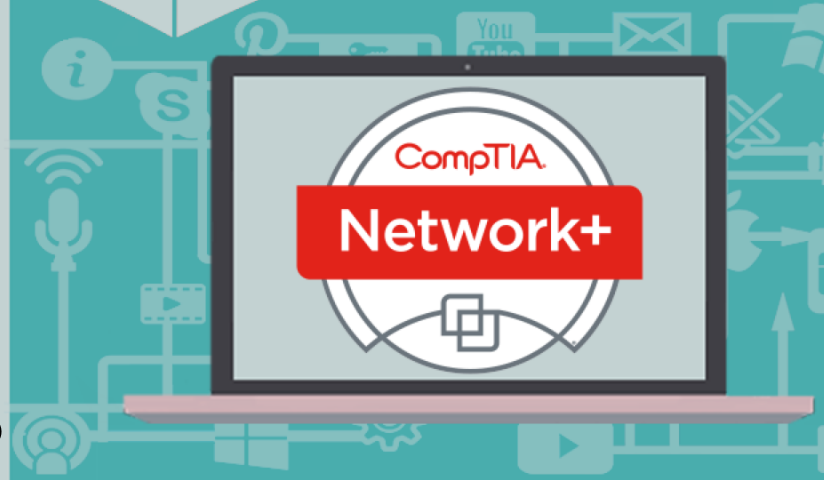
HIDS/NIDS and HIPS/NIPS

- Network-based (NIDS/NIPS)
  - Network device to protect entire network
- Host-based (HIDS/HIPS)
  - Software-based and installed on servers/clients
- Network and Host-based can work together for more complete protection
  - NIPS might prevent a DoS attack whereas a HIPS solution could focus on the protection of applications on a host from malware and other attacks

HIDS/NIDS and HIPS/NIPS



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



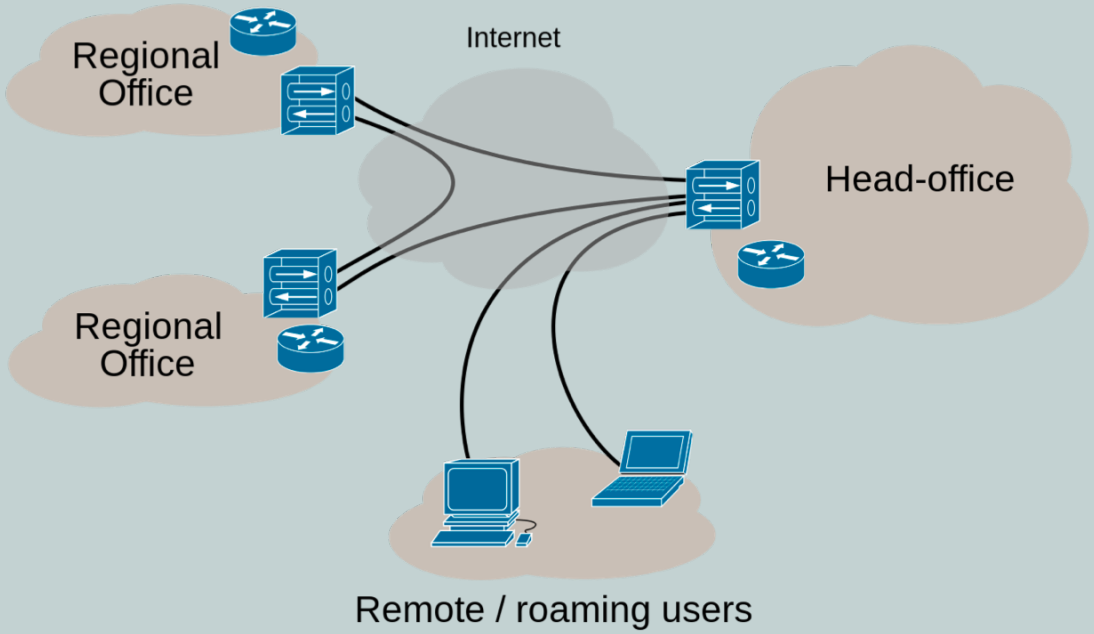
Virtual Private Networks (VPNs)

CompTIA Network+ (N10-007)

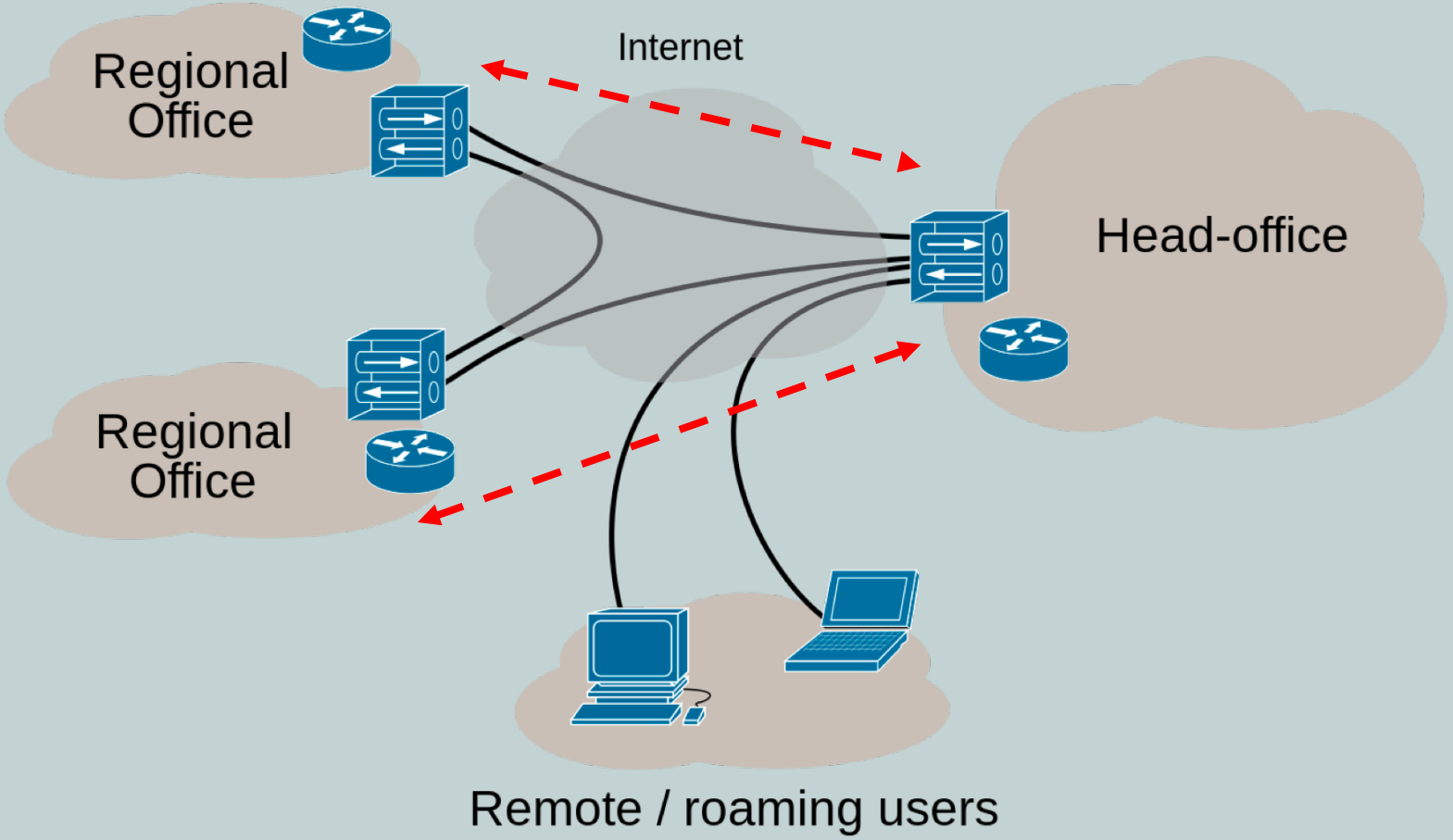
Virtual Private Networks (VPNs)

- Enables work in remote offices or telecommuting

- Allows users to securely connect to the corporate network over an untrusted network

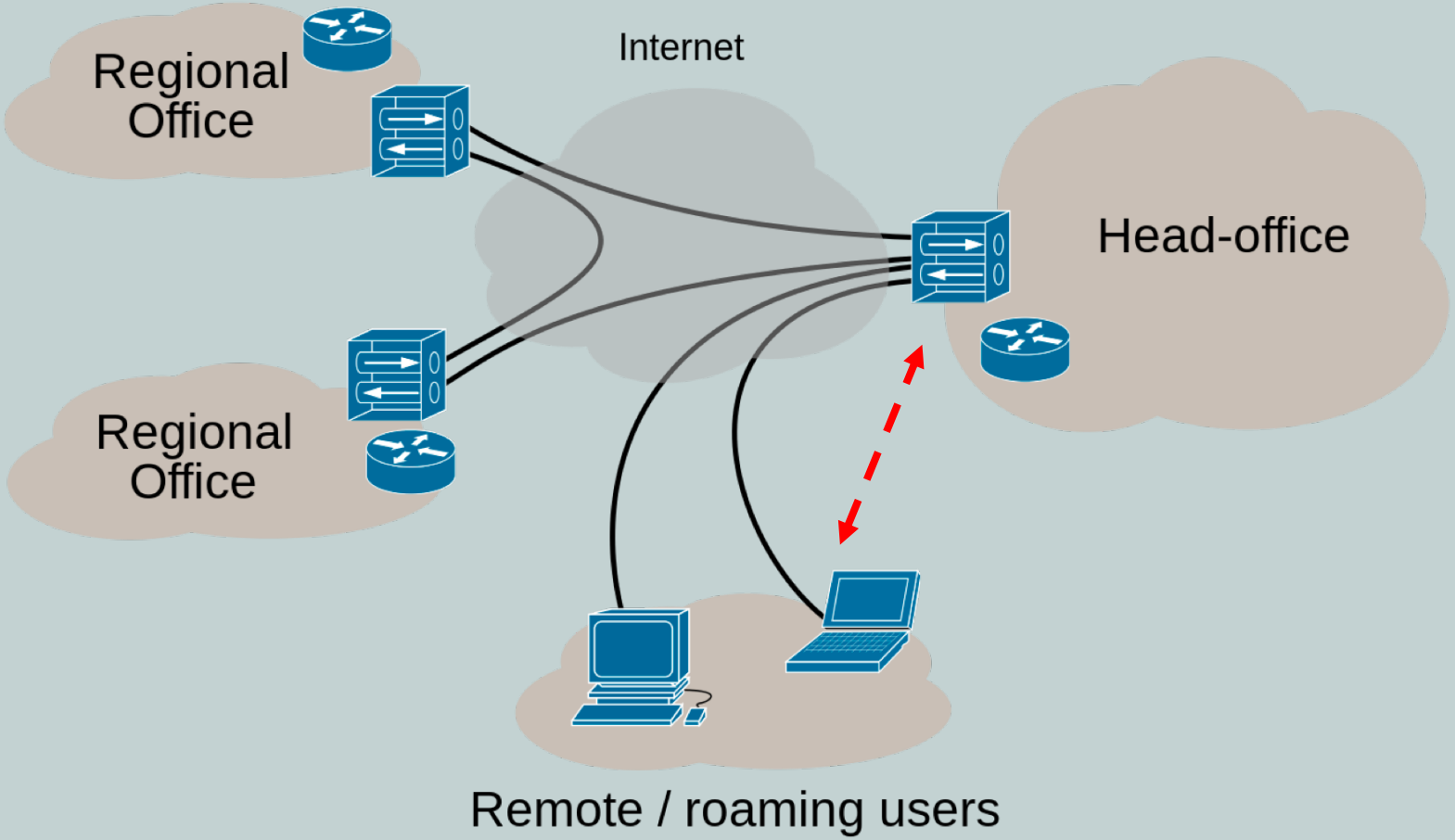


Site to Site



Interconnects two sites and provides an inexpensive alternative to a leased line

Client to Site



Connects a remote user with a site and commonly called remote access

VPN Types: SSL

- Secure Socket Layer (SSL) provides cryptography and reliability for upper layers of the OSI model (Layers 5-7)
- Largely replaced by TLS in current networks
- Provides for secure web browsing via HTTPS

VPN Types: TLS

- Transport Layer Security (TLS) has mostly replaced SSL

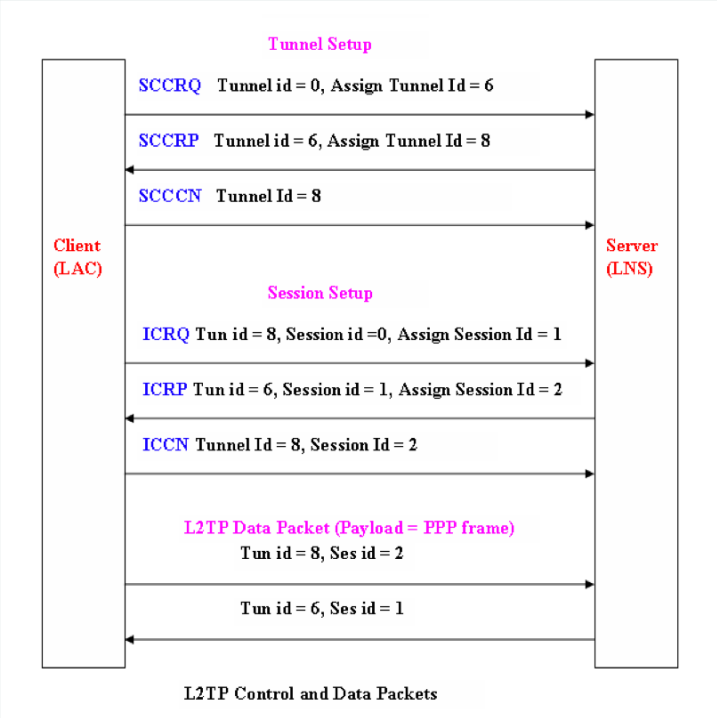
- If you are using an HTTPS websites, you are probably using TLS

VPN Types: DTLS

- Datagram Transport Layer Security (TLS) is used to secure UDP traffic
- Based on the TLS protocol
- Designed to give security to UDP by preventing eavesdropping, tampering, and message forgery

VPN Types: L2TP

- Layer 2 Tunneling Protocol (L2TP) lacks security features like encryption
- Can be used for secure VPN if combined with additional protocols for encryption services



L2TP Control and Data Packets

VPN Types: L2F

- Layer 2 Forwarding (L2F) was developed by Cisco to provide for tunneling of PPP

- Lacks native security features, like L2TP

Bits 0-12												13-15	16-23	24-31
F	K	P	S	0	0	0	0	0	0	0	0	Ver	Protocol	Sequence (opt)
Multiplex ID													Client ID	
Length													Payload offset (opt)	
Packet key (optional)														
Payload														
													L2F Checksum (opt)	

VPN Types: PPTP

- Point-to-Point Tunneling Protocol (PPTP) is an older protocol that supports dial-up networks

- Lacks native security features, but Windows added some features in their implementation

IP Security (IPSec)

CompTIA Network+ (N10-007)

IP Security (IPSec)

- VPNs most commonly use IPsec to provide protections for their traffic over the internet

Protection	Description
Confidentiality	Provided by data encryption
Integrity	Ensures data is not in transit through hashing
Authentication	Verifies the parties are who they claim to be

IKE Modes

- IPsec uses the *Internet Key Exchange* (IKE) to create a secure tunnel
  - IKE uses encryption between authenticated peers

Mode	Description
Main	3 separate exchanges occur
Aggressive	More quickly achieves results of main mode using only 3 packets
Quick	Negotiates parameters of the IPSec session

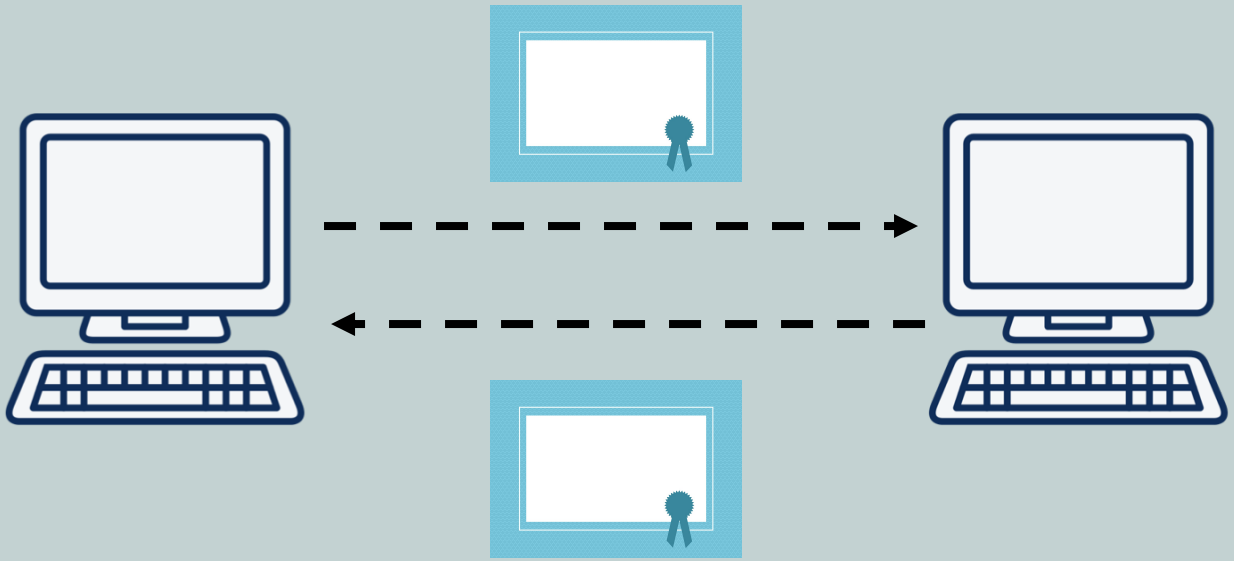
Establishing an IPSec Tunnel

- IKE Phase 1
  - Establishes encryption and authentication protocols between VPN endpoints to create the IKE Phase 1 tunnel
  - ISAKMP is established using main or aggressive mode to create a Security Association (SA)
  - Key exchange occurs in both directions

- IKE Phase 2
  - Within the secure IKE Phase 1 tunnel, establishes encryption and authentication protocols between VPN endpoints to create the IPsec tunnel
  - Each data flow uses a separate key exchange

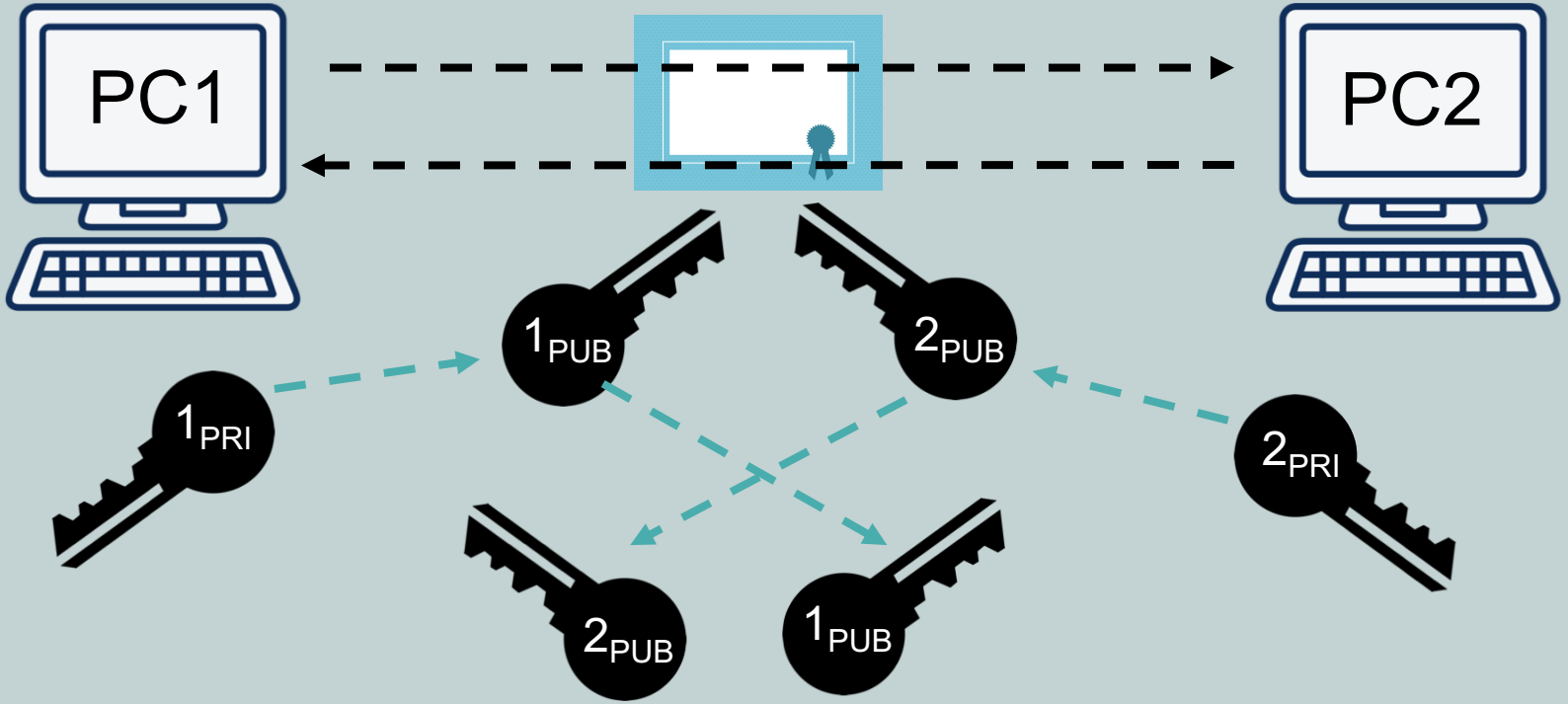
Establishing an IPSec Tunnel

- Peers authenticate using certificates or pre-shared secret



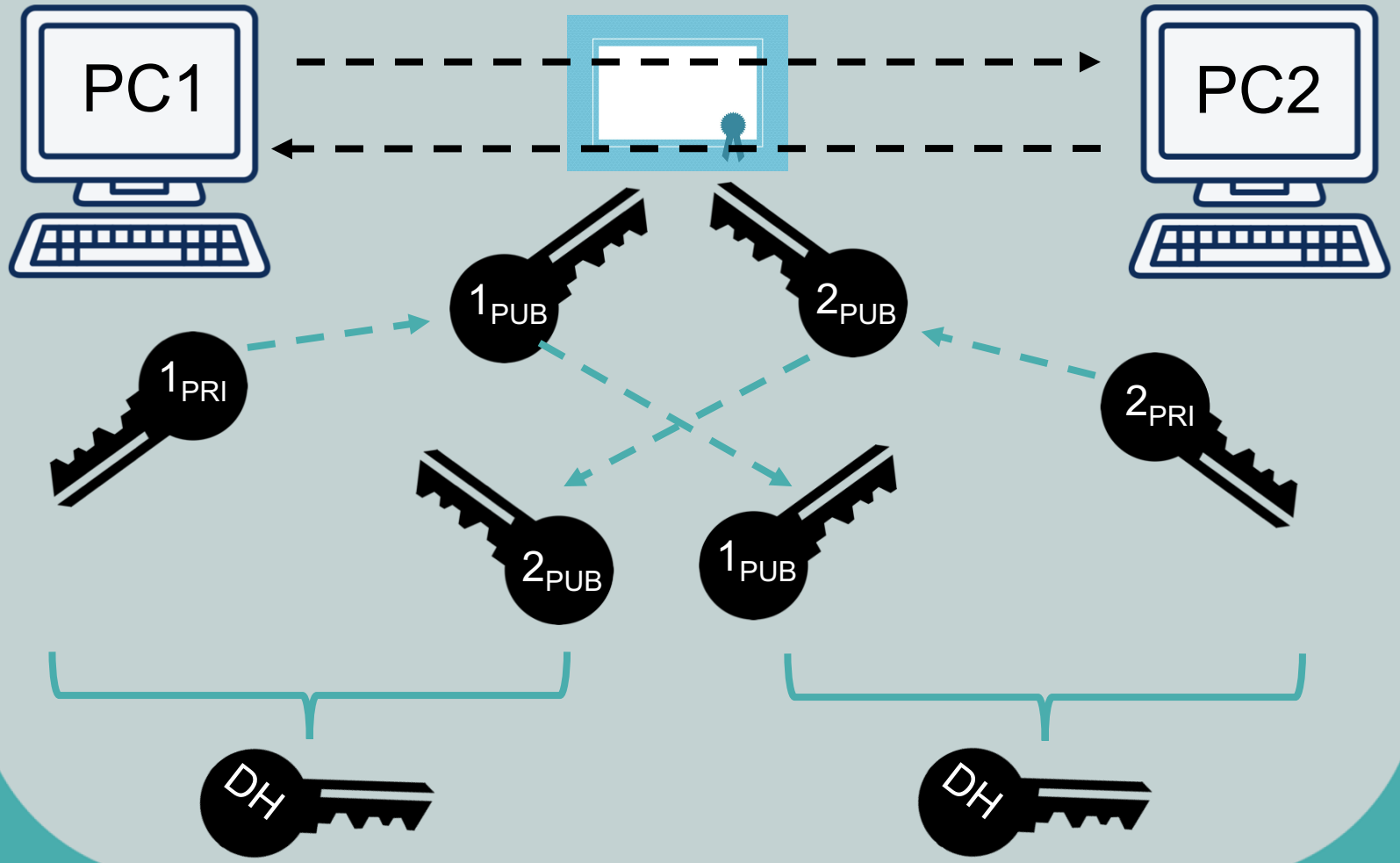
Establishing an IPSec Tunnel

- Each side creates a private key and derives a public key from it, which it then exchanges



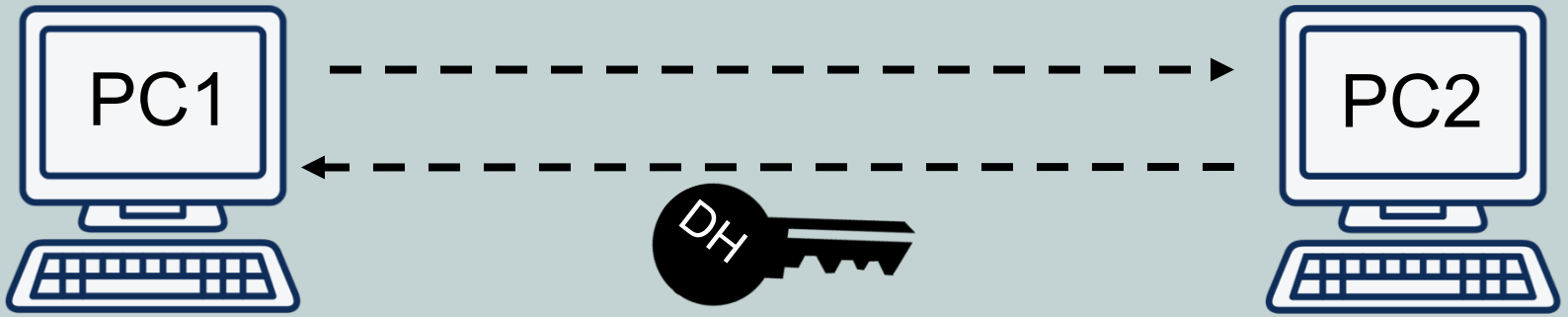
Establishing an IPSec Tunnel

- Each side calculates the Shared Secret (DH) using the public and private keys



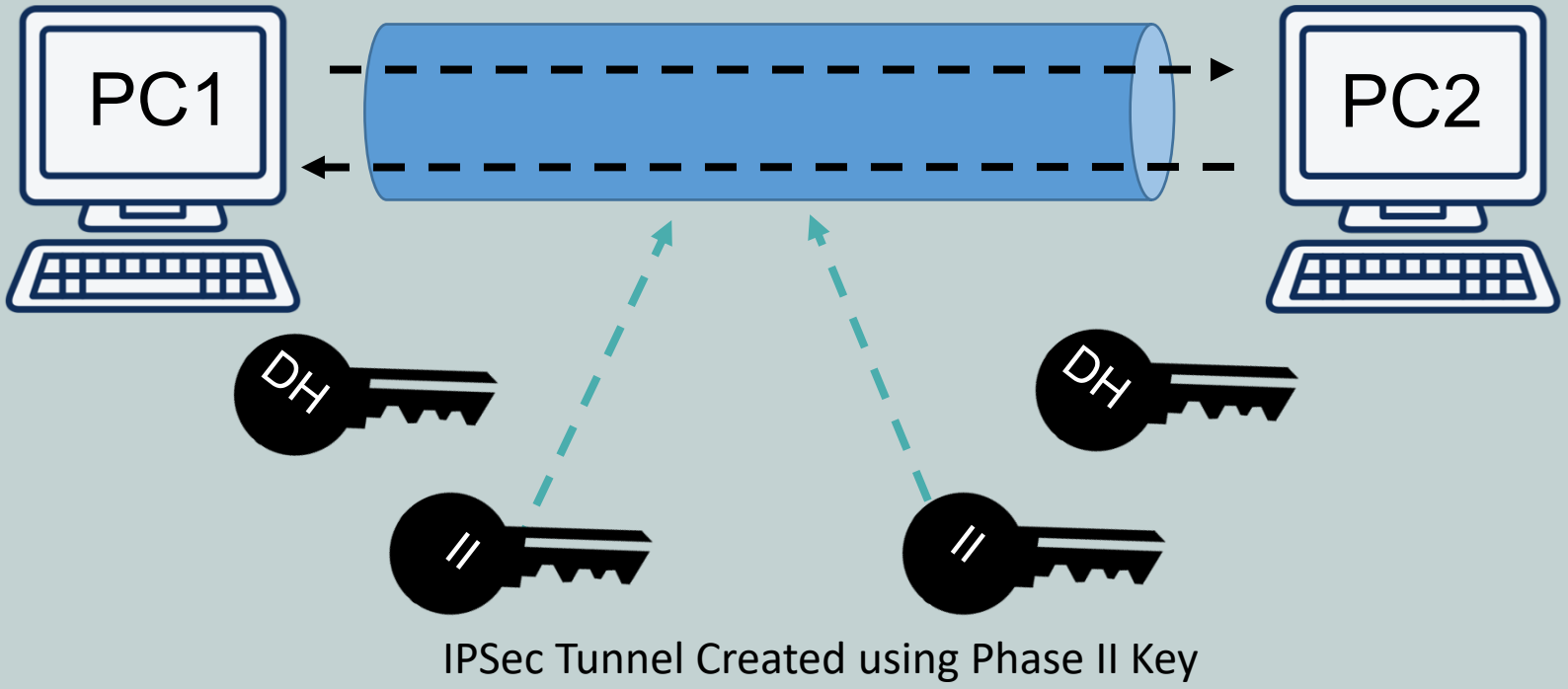
Establishing an IPSec Tunnel

- Both sides agree to encryption and integrity methods for IKE Phase II



Establishing an IPSec Tunnel

- Both sides agree to encryption and integrity methods for IKE Phase II



Steps for an IPSec VPN Session

1. PC1 sends traffic to PC2 and then RTR1 initiates creation of IPsec tunnel

2. RTR1 and RTR2 negotiate Security Association (SA) to form IKE Phase 1 tunnel (ISAKMP tunnel)

3. IKE Phase 2 tunnel (IPsec tunnel) is negotiated and setup

4. Tunnel is established and information is securely sent between PC1 and PC2

5. IPsec tunnel is torn down and the IPsec SA is deleted

Transport and Tunnel Modes

- Transport mode
  - Uses packet's original IP header
  - Used for client-to-site VPNs
  - Approach works well if increasing the packet size could cause issues

- Tunnel mode
  - Encapsulates entire packet to provide new header
  - New header has the source and destination of the VPN termination devices at the different sites
  - Used for site-to-site