BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

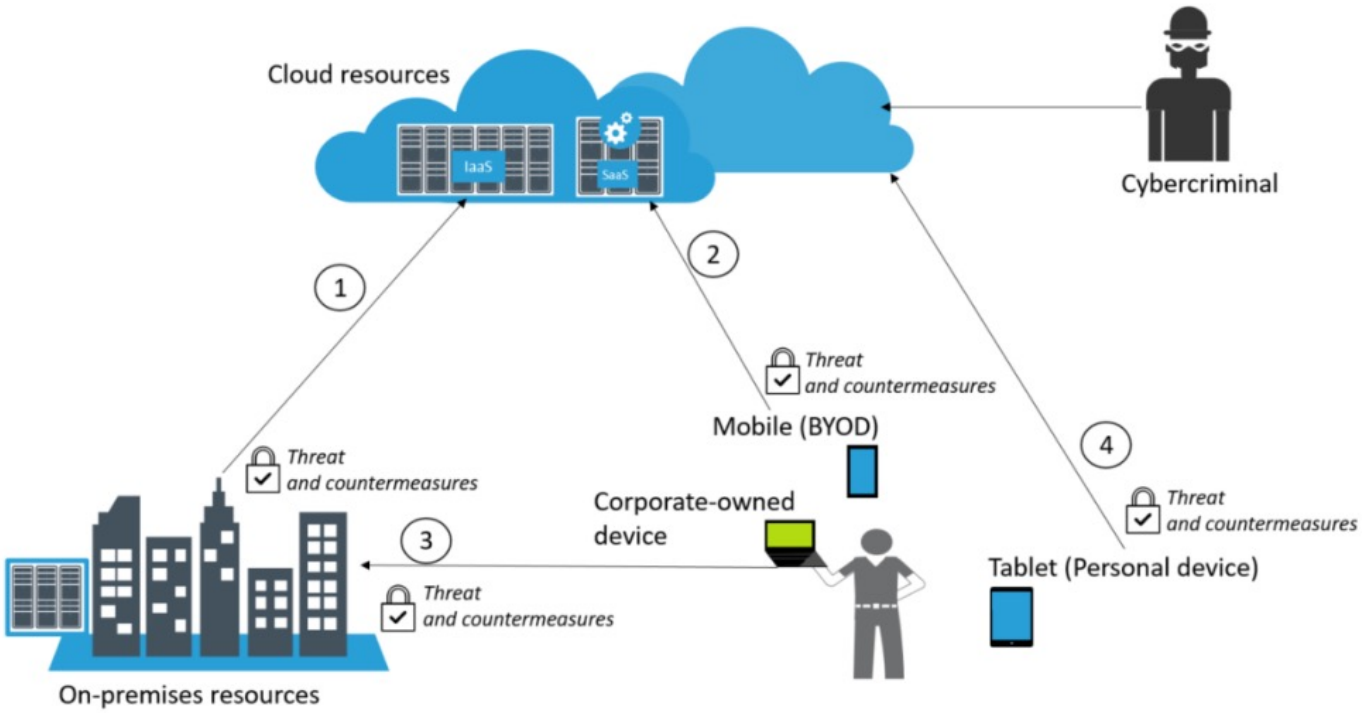
SSZG575: Ethical Hacking
Session: 13 (Defense Processes and Tools)

Agenda

- Attack Entry Points
  - User authentication
  - Data security
  - Continuous security monitoring
- Network Security
- Firewalls
  - Firewall penetration testing steps
- Honeypots

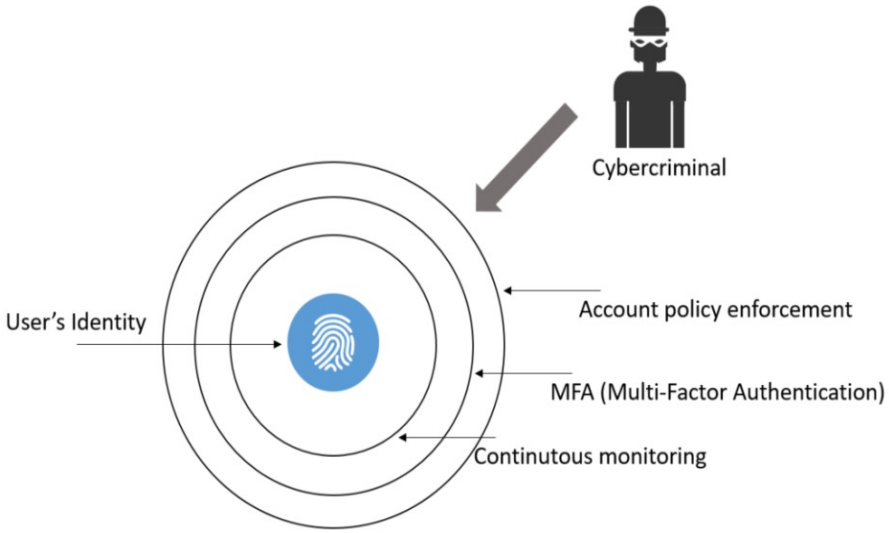
Attack Entry Points

Attack Entry Points



- Connectivity between on-premises and cloud (**1**)
- Connectivity between BYOD devices and cloud (**2**)
- Connectivity between corporate-owned devices and on-premises (**3**)
- Connectivity between personal devices and cloud (**4**)

User Authentication Methods



- Three methods of authentication:
  - Something you know (password, PIN etc)
  - Something you have (smart card, debit card, hand held token, OTP)
  - Something you are (fingerprint, iris scan, facial features)
- Others:
  - Location, Device id, Typing speed etc

User Authentication Types

- Password based authentication
  - Security policy enforcement for accounts
  - Strong password (string of letters, numbers, or special characters)
  - Frequent password changes
  - Average person has 25 on-line accounts but only 54% use different passwords across accounts
  - Hackers can easily guess user credentials by running through all possible combinations until they find a match
- Multi-Factor Authentication
  - Multi-layer authentication
  - Two or more independent ways to identify a user
  - Ex: Captcha, OTP, Email, Call back etc

User Authentication Types

- Certificate based authentication
  - Identify users, machines or devices by using digital certificates
  - Digital certificates prove the ownership of a public key and are issued by a certification authority
  - Users provide their digital certificates when they sign in to a server
  - Server verifies the credibility of the digital signature with the certificate authority.
- Biometric authentication
  - Use of unique biological characteristics of an individual
  - Common biometric authentication methods include:
    - Facial recognition
    - Finger print scanner
    - Eye scanners
    - Voice biometrics

User Authentication Types

- Token based authentication
  - Enable users to enter their credentials once and receive a unique encrypted string of random characters in exchange
  - User can then use the token to access protected systems instead of entering credentials all over again
  - Digital token proves that user already have access permission
  - Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.

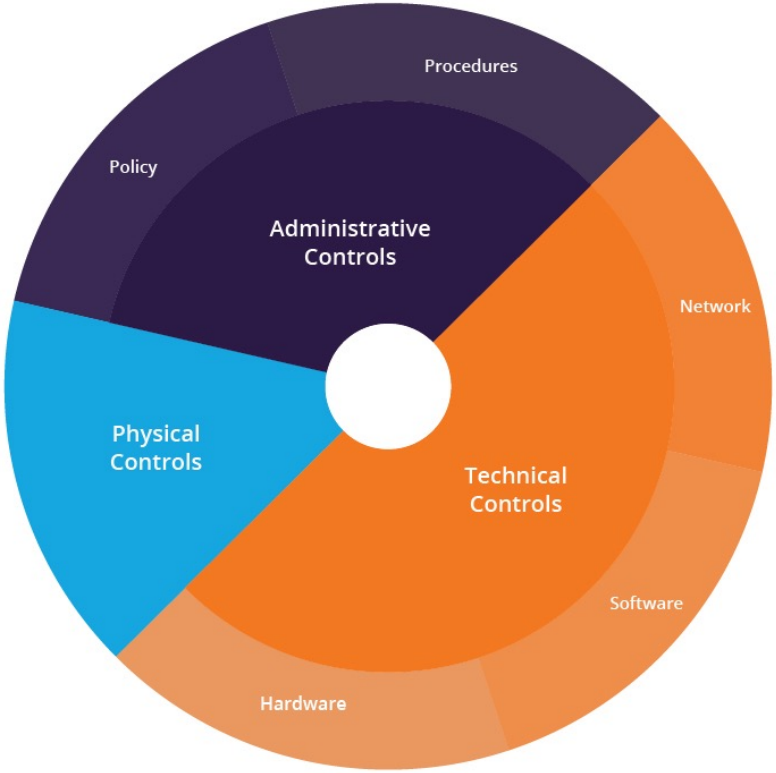
Data Security

State	Description	Threats	Countermeasures	Security triad affected
Data at rest on the user's device	The data is currently located on the user's device.	The unauthorized or malicious process could read or modify the data.	Data encryption at rest. It could be file-level encryption or disk encryption.	Confidentiality and integrity.
Data in transit	The data is currently being transferred from one host to another.	A man-in-the-middle attack could read, modify, or hijack the data.	SSL/TLS could be used to encrypt the data in transit.	Confidentiality and integrity.
Data at rest on-premise (server) or cloud	The data is located at rest either on the server's hard drive located on-premise or in the cloud (storage pool).	Unauthorized or malicious processes could read or modify the data.	Data encryption at rest. It could be file-level encryption or disk encryption.	Confidentiality and integrity.

Defense in Depth

- An information assurance strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited
- Originates from a military strategy by the same name
  - Seeks to delay the advance of an attack, rather than defeating it with one strong line of defense
- Defense in depth includes:
  - End user security
  - Product design
  - Network security

Defense in Depth



- **Physical controls:** Security measures that prevent physical access to IT systems, such as security guards or locked doors.
- **Technical controls:** Security measures that protect network systems or resources using specialized hardware or software, such as a firewall appliance or antivirus program.
- **Administrative controls:** Security measures consisting of policies or procedures directed at an organization's employees, e.g. instructing users to label sensitive information as "confidential", changing password, strong password etc.

Defense in Depth: Technical Controls

Control Type	Description
Access Measures	Access measures include authentication controls, biometrics, timed access and VPN
Workstation Defenses	Workstation defense measures include antivirus and anti-spam software
Data Protection	Include data at rest encryption, hashing, secure data transmission and encrypted backups
Perimeter Defenses	Network perimeter defenses include firewalls, intrusion detection systems and intrusion prevention systems.
Monitoring and Prevention	Monitoring and prevention of network attacks involves logging and auditing network activity, vulnerability scanners, sandboxing and security awareness training.

Continuous Security Monitoring (CSM)

- CSM is a threat intelligence approach that automates the monitoring of information security controls, vulnerabilities and other cyber threats to support organizational risk management decisions.
- Organizations need real-time visibility of indicators of compromise, security misconfiguration, and vulnerabilities in their infrastructure and networks.
- Traditional security controls like firewalls, antivirus software, and penetration testing are no longer enough to protect against a sophisticated attacker.
- Even if your infrastructure is relatively stable, attackers find new zero-days to exploit and researchers share vulnerabilities to the CVE database on a daily basis.

Why Continuous Security Monitoring?

- Enables organizations to continually assess their overall security architecture to determine whether they are complying with their internal information security policies
- Reasons why CSM is required:
  - Increasing digitization of sensitive data
  - General data protection laws (EU-GDPR, Brazil-LGPD, New York-Shield Act, California-CCPA, India-ITAct 2000)
  - Data breach notification laws
  - Out-sourcing, On-sourcing and Sub-contracting

How Does CSM Work?

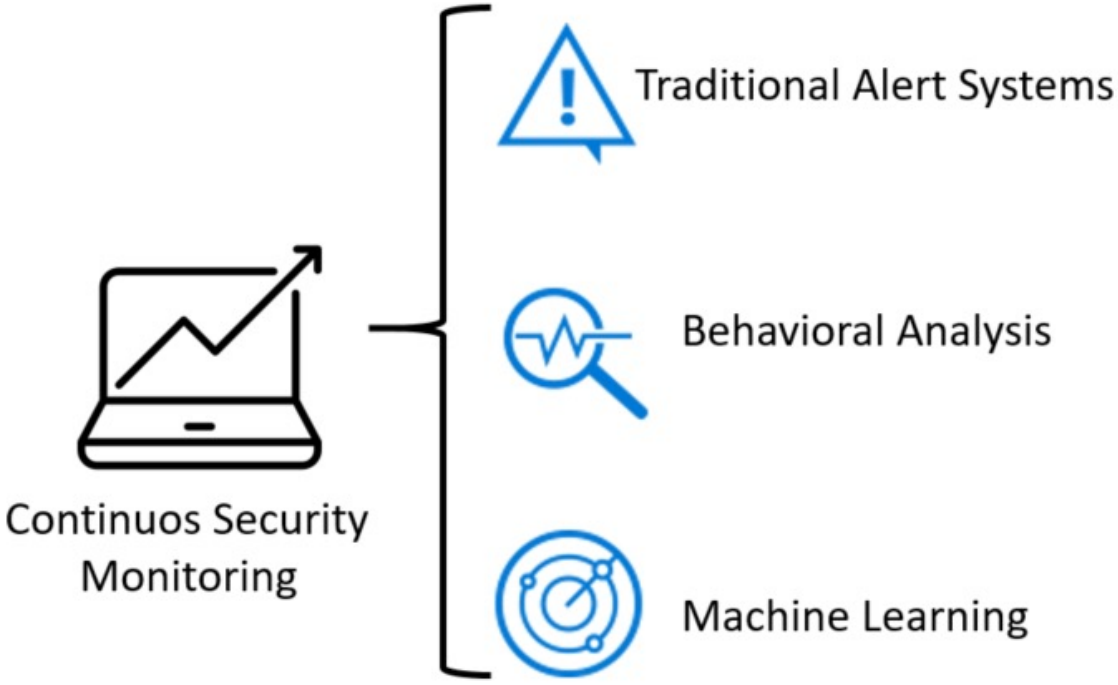
innovate achieve lead

- Works by providing real-time information about an organization's security posture.
- As per NIST (NIST SP 800-137) ISCSM works by:
  - Maintaining situational awareness of all systems across the organization and its vendor ecosystem
  - Maintaining an understanding of threats and threat activities
  - Assessing all security controls
  - Collecting, correlating, and analyzing security-related information
  - Providing actionable communication of security status across all tiers of the organization
  - Active management of risk by organizational officials
  - Integration of information security and risk management frameworks.

Digital Assets to be Monitored

- Web applications, services, and APIs
- Mobile applications and their backends
- Cloud storage and network devices
- Domain names, SSL certificates, and IP addresses
- IoT and connected devices
- Public code repositories such as GitHub, GitLab, and BitBucket
- Email servers

Continuous Security Monitoring

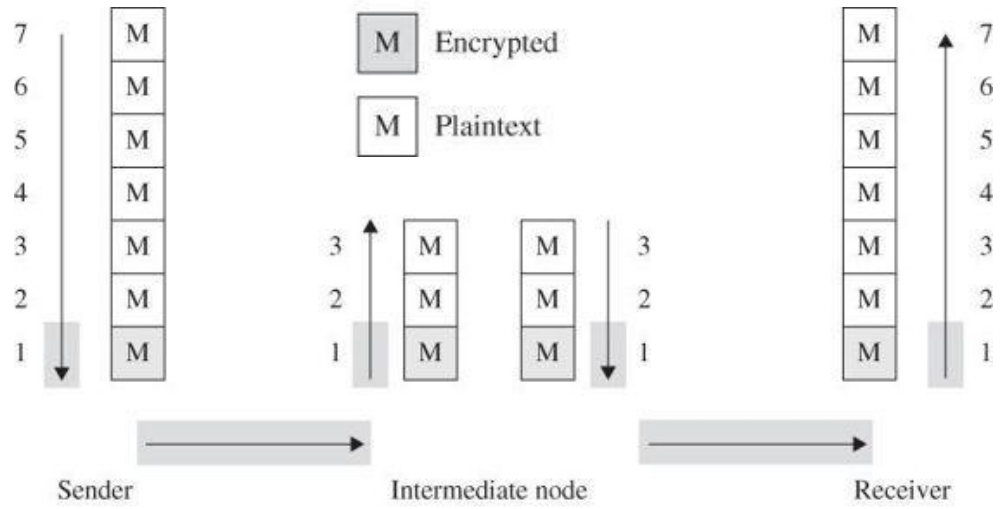


Network Security

Network Encryption

- Encryption protects only what is encrypted
  - At sender or receiver end once data is decrypted, it's exposed to threats
- Encryption is no more secure than its key management
  - Once key is revealed, encryption is of no use
- A flawed system design with super encryption is still a flawed system
- Encryption algorithm design is work of professionals
- Encryption implementation types:
  - **Link encryption:** Host to Host
  - **End to end encryption:** Application to Application

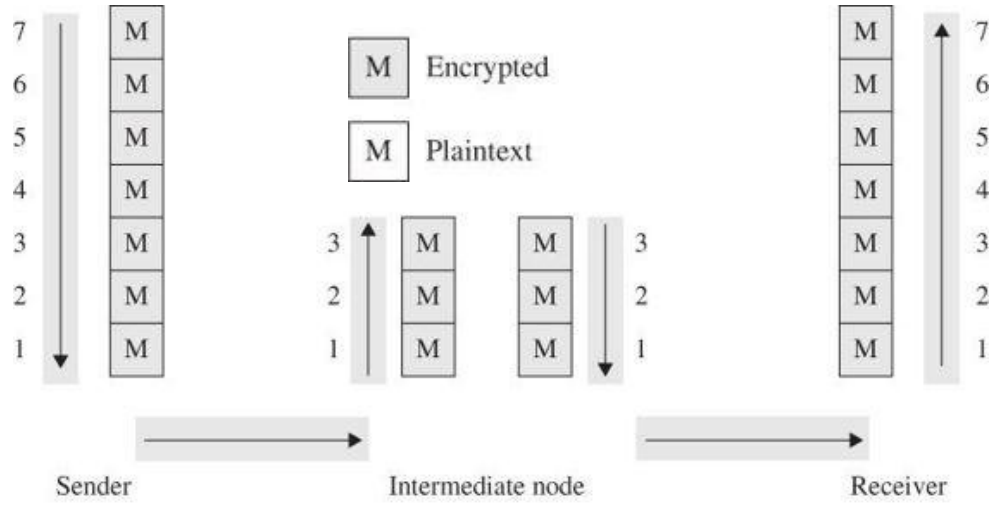
Link Encryption

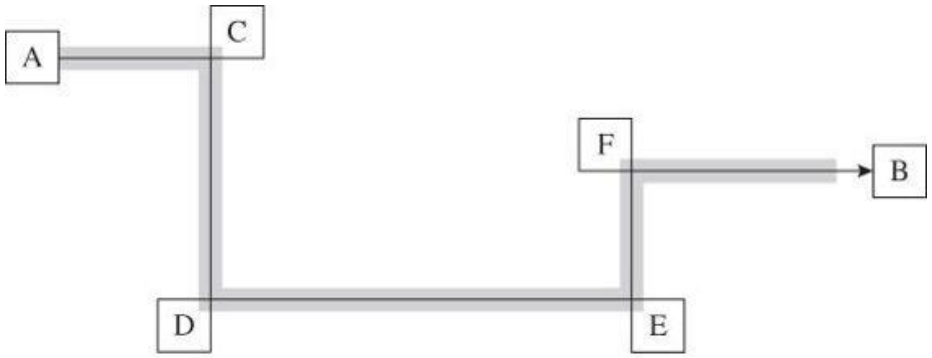


- Data is encrypted just before it's put on the physical network
- Encryption occurs at layer 1 or 2 in OSI network model
- Link encryption covers the communication from one node to next on the path to destination
- Message remains plaintext within the hosts
- Data is encrypted while it travels on network.
  - When date reaches a router or another intermediate device, data gets decrypted
  - This is to allow the intermediator knows which way to send it next.

Useful when all hosts are reasonably secure but communication line is not

End to End Encryption





- Encryption is applied between two users
- Encryption is performed at highest level of network layers
- Data confidentiality is maintained even if a lower layer fails or communication passes thru unsecure nodes
- Only the communicating users can read the messages.
- Prevents potential eavesdroppers including telecoms, ISPs and other intermediaries.

Browser Encryption

- Browsers can encrypt data during transmission.
- Browser negotiates with the server an algorithm for encryption
- SSH (Secure Shell):
  - Provides authentication and encryption service to Shell or OS commands
  - Replaces telnet, rlogin, rsh for remote access
  - Protects against spoofing and data modification during transmission
  - Usage algorithm (DES, AES etc) for encryption and (Public keys, Kerberos etc) for authentication
- SSL/TLS (Secure Socket Layer/Transport Layer Security):
  - SSL has 3 version 1.0, 2.0. 3.0. Version 3.1 is known as TLS
  - Implemented at layer 4 (transport layer)
  - SSL operates at application level
  - Provides server authentication, optionally client authentication and encrypted communication channel between client and server

Cipher Suite

- Cipher suite is client & server negotiated encryption algorithm for authentication, session encryption and hashing
  - Diffie-Hellman
  - DES
  - AES
  - RC4
  - RSA
  - ….
- Server sends a set of records listing cypher suite identifiers it can use
- Client responds with the preferred choices from the shared set

SSH (Secure Shell)

- SSH or Secure Shell or Secure Socket Shell is a network protocol that helps us securely accessing and communicating with remote servers.
- SSH uses a client-server architecture for secured communication over the network by connecting an ssh client with the ssh server.
- By default, ssh server listens to the standard TCP port 22.
- SSH uses a public-key cryptography technique to authenticate between client and server.
- SSH uses strong symmetric encryption & hashing algorithms for the exchange of messages between client and server to ensure privacy and data integrity.

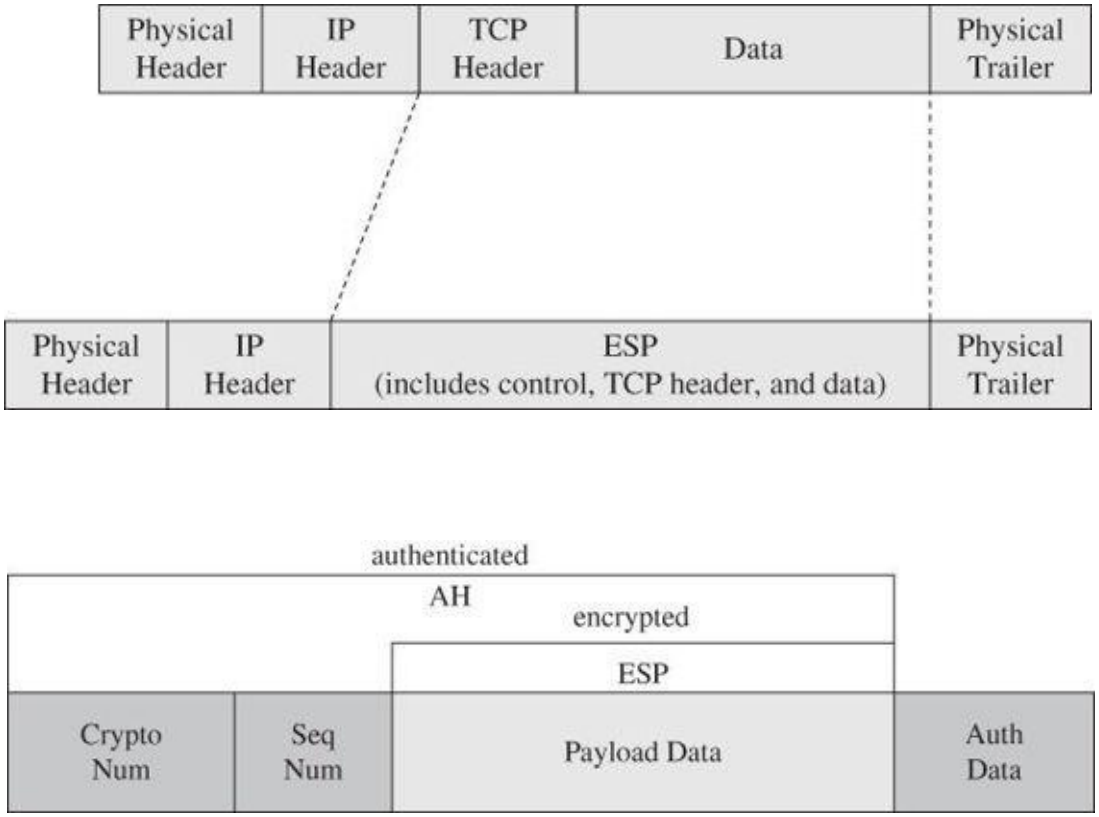
SSL (HTTPS)

- SSL encrypts data that is transmitted across the web.
- Anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.
- SSL initiates an **authentication** process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL digitally signs data in order to provide **data integrity**, verifying that the data is not tampered with before reaching its intended recipient.

IP Security (IPSec)

- IPSec is implemented at OSI layer 2 (data layer)
- Implements encryption and authentication
- Allows two communicating parties to agree on mutually supported set of protocols
- **Security Association (SA):** a set of security parameter for a secured communication channel
- SA includes:
  - Encryption algorithm, key and mode
  - Encryption parameters like initialization vector
  - Authentication protocol and key
  - Life span of the SA
  - Address of opposite end of association
  - Sensitivity level of protected data (used for classified information)
- A host (network server or firewall) may have multiple SAs in operation at any given point of time

Headers and Data

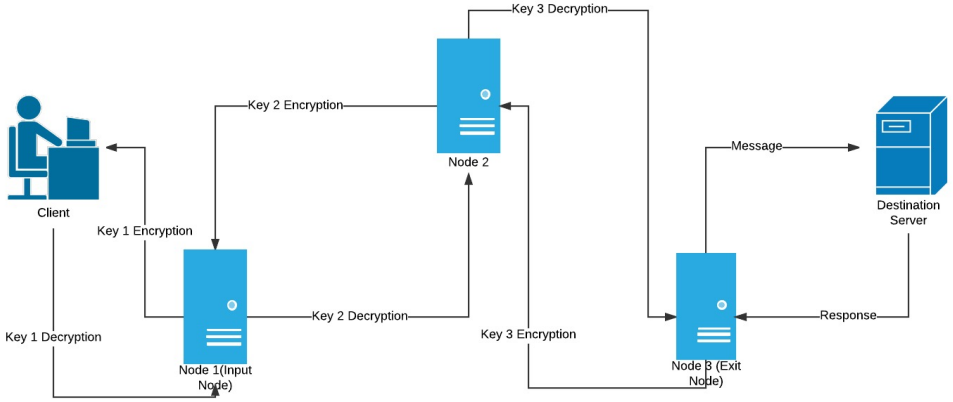


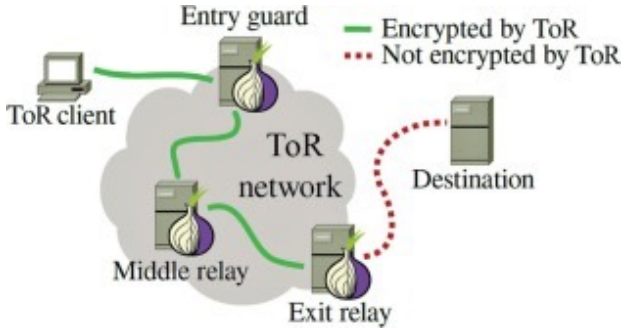
- IPSec has two fundamental data structure:
  - Authentication Header (AH)
  - Encapsulated Security Payload (ESP) – replaces TCP header & data portion of packet
  - Sequence number is incremented by 1 for each packet transmitted
- IPSec encapsulated security payload contains descriptors to tell a recipient how to interpret encrypted content

The Onion Routing (TOR)

- Link & End to end encryption data is encrypted but client & server address remain exposed
- TOR prevents an eavesdropper from learning source, destination, or content of data in transit
- Protection is achieved by transferring communication around a network of computer before delivery to receiver
- Ex: A needs to send a packet to B. It routes it thru X, Y & Z.
  - A encrypts the packet with B's public key and appends a header from Z to B
  - Then A encrypts the result with Z's public key and appends a header from Y to Z
  - Then A encrypts the result with Y's public key and appends a header from X to Y
  - Then A encrypts the result with X's public key and appends a header from A to X
  - Upon receipt of the packet, intermediate nodes only know the previous and next nodes for the packet and not the whole path
- Used in covert mails, private browsing, dark web etc
- Browsers: TOR, Orfox, Epic, Comodo Ics Dragon

The Onion Routing (TOR)





- The client with access to all the encryption keys i.e **key 1, key 2 & key 3** encrypts the message (get request) thrice wrapping it under 3 layers like an onion which have to be peeled one at a time.
- This **triple encrypted message** is then sent to the first server i.e. **Node 1(Input Node).**
- **Node 1** only has the address of **Node 2** and **Key 1**. So it **decrypts** the message using **Key 1** and realises that it doesn't make any sense since it still has 2 layers of encryption so it passes it on to **Node 2**
- **Node 2** has **Key 2** and the addresses of the **input & exit nodes.** So it **decrypts** the message using **Key 2** realises that its still **encrypted** and passes it onto the **exit node**
- **Node 3 (exit node)** peels of the last layer of encryption and finds a **GET request** for youtube.com and passes it onto the **destination server**
- The server processes the request and serves up the desired webpage as a **response.** The response passes through the same nodes in the reverse direction where each node puts on a **layer of encryption** using their specific key
- It finally reaches the client in the form of a **triple encrypted** response which can be decrypted since the client has access to all the keys

Firewalls

What is a Firewall?

- Firewalls are network security devices which protect a subnet (mainly internal) from harm by another subnet (mainly external)
  - Filters traffic between a protected (inside) network and less trustworthy (outside) network
  - Firewall is a traffic cop that permits or block data flow between two parts of a network architecture
  - Firewalls enforce pre-determined rules (security policies) to govern traffic flow
  - Two rules commonly used – default permit and default deny
- Can also be used to separate the sensitive segments of a network i.e. R&D
- Firewalls run on dedicated systems for performance and security reasons
- Firewall system typically doesn't have:
  - Compilers, linkers, loaders, text editors, debuggers, libraries or other tools
  - An attacker can take advantage of these tools

How Does Firewall Work?

Rule	Type	Source Address	Destination Address	Destination Port	Action
1	TCP	*	192.168.1.*	25	Permit
2	UDP	*	192.168.1.*	69	Permit
3	TCP	192.168.1.*	*	80	Permit
4	TCP	*	192.168.1.18	80	Permit
5	TCP	*	192.168.1.*	*	Deny
6	UDP	*	192.168.1.*	*	Deny

- **Security Policy:** Set of rules that define what traffic can or can not pass thru the firewall
- Firewalls enforce pre-determined rules (security policies) to govern traffic flow

- **Rule 1:** Allow traffic from any outside host to 192.168.1 subnet on port 25 (mail transfer)
- **Rule 2:** Allow traffic from any outside host to 192.168.1 subnet on port 69 (file transfer)
- **Rule 3:** Allow traffic from 192.168.1 subnet to any outside host on port 80 (web pages)
- **Rule 4:** Allow traffic from any outside host to 192.168.1.18 on port 80 (web server)
- **Rule 5 & Rule 6:** Deny all other traffic (inbound or outbound)

Firewall Rules

- Firewalls can enforce pre-determined rules for:
  - IP Address
  - Domain name
  - Protocols
  - Programs
  - Ports
  - Key words
- Firewall Types
  - Host based (software firewall) - Windows firewall
  - Network based (hardware+software firewall)

Firewall Categories

- **First Generation:** Packet filtering gateways or screening routers
- **Second Generation:** Stateful inspection firewalls
- **Third Generation:**
  - Application Proxy Firewall
  - Circuit level gateways
  - Guard Firewall
  - Personal firewall
- Network Address Translation (NAT) Firewall
- Next Generation Firewall (NGFW)

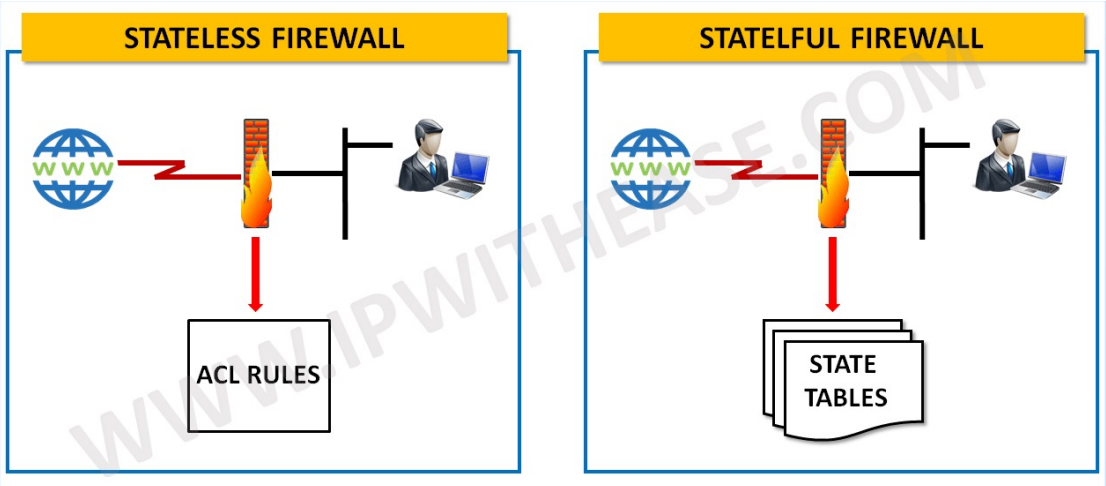
Packet Filtering Firewall

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

- Simplest form of firewalls
- Controls access based on packet address (source or destination) or specific transport protocol type (HTTP, Telnet)
- Doesn't inspect data inside packet and treats each packet in isolation. It has no ability to judge whether a packet is part of an existing stream of traffic.
- Can detect outside traffic with a forged source header
- Usage separate interface cards for inside and outside
- Can not implement complex rules

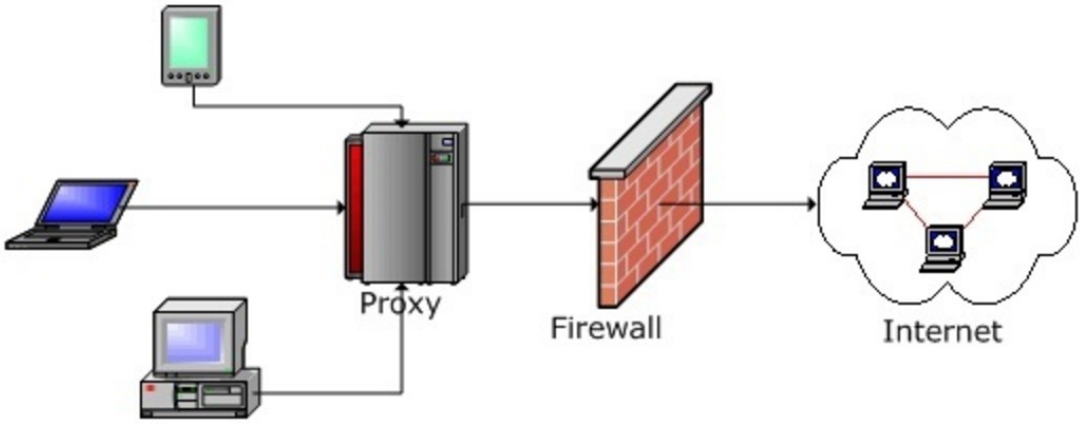
Stateful Inspection Firewall



- Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet which makes it more efficient.
- It keeps track of the state of networks connection travelling across it, such as TCP streams.
- Filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

- Stateful inspection firewalls judge traffic based on information from multiple packets
- If someone is trying to scan ports in a short time, firewall will block that host
- Ex: first attempt (port 1) from 10.1.3.1 will be allowed but access time recorded, port 2 allowed, port 3 allowed but at port 4 the abnormal behavior is noticed and dis-allowed

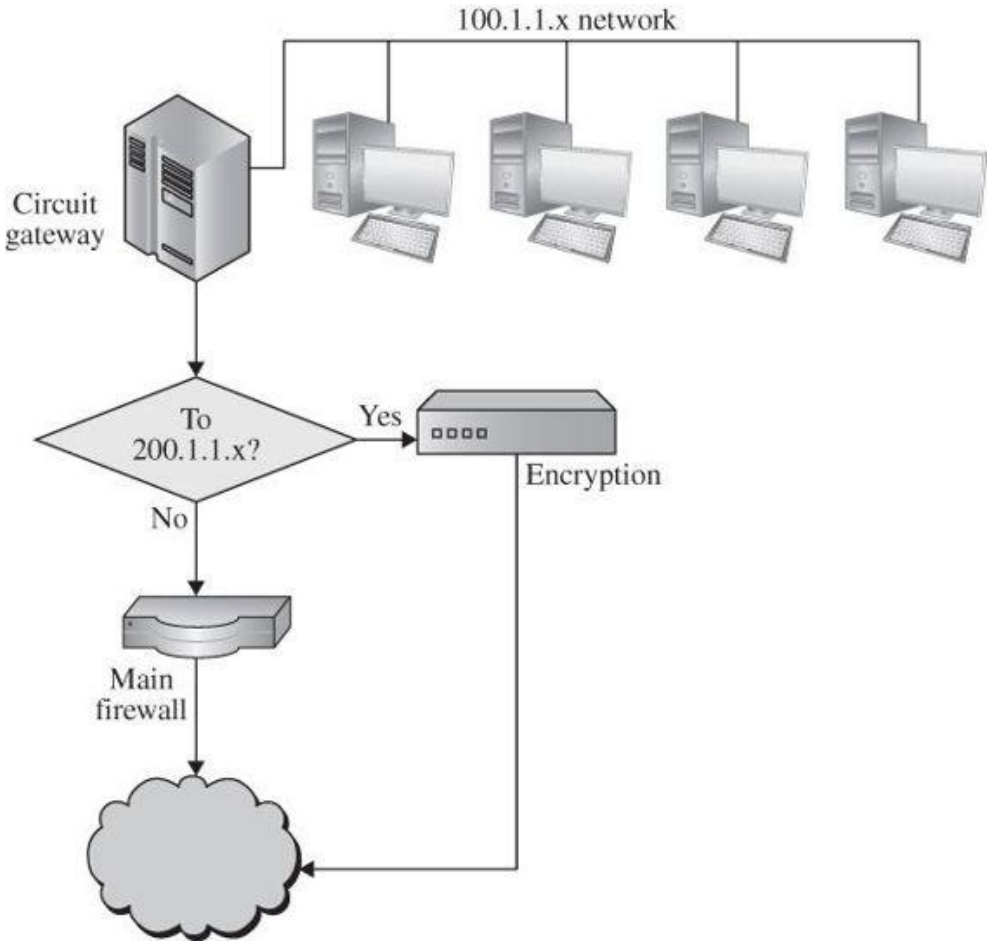
Application Proxy Firewall



- Proxy acts an intermediary between two end systems. Can filter traffic at application level.
- The client must send a request to the firewall, where it is then evaluated against a set of security rules and then permitted or blocked.
- Proxy firewalls monitor traffic for layer 7 protocols (HTTP, FTP etc) and use both stateful and deep packet inspection to detect malicious traffic.

- Application proxy firewall simulates the behavior of a protected application on the inside network, allowing in only safe data
- Application proxy intrudes in the middle of protocol between sender and receiver, similar to man in the middle
- Proxy interprets the protocol stream as an application would and takes control action based on things visible inside the protocol

Circuit Level Gateway



- This firewall allows one network to be extension of another network and functions as a virtual gateway between two networks
- Firewall verifies the circuit at time of creation after which data transfer is normal
- VPNs are implemented thru circuit level gateways

Guard Firewall

- A guard is a proxy type firewall
- A guard implements programmable set of conditions, even if the program conditions become very sophisticated
- Great firewall of China (Golden Shield Program) is a guard firewall. It filters content based on government restrictions/ rules.
  - Initiated, developed, and operated by the Ministry of Public Security (MPS)
  - Blocks politically inconvenient incoming data from foreign countries
  - Web sites belonging to "outlawed" or suppressed groups, such as pro-democracy activists

Personal Firewall

- Personal firewall is program that runs on a single host to monitor and control traffic to that host
- It works in conjunction with support from operating system
- Ex: SaaS Endpoint Protection (McAfee), F-Secure Internet Security, Microsoft Windows Firewall, Zone Alarm, Checkpoint
- Personal firewalls:
  - List of safe/unsafe sites
  - Policy to download code/files
  - Unrestricted data sharing
  - Management access from corporate but not from outside
  - Combine action with anti-virus software

Network Address Translation (NAT)

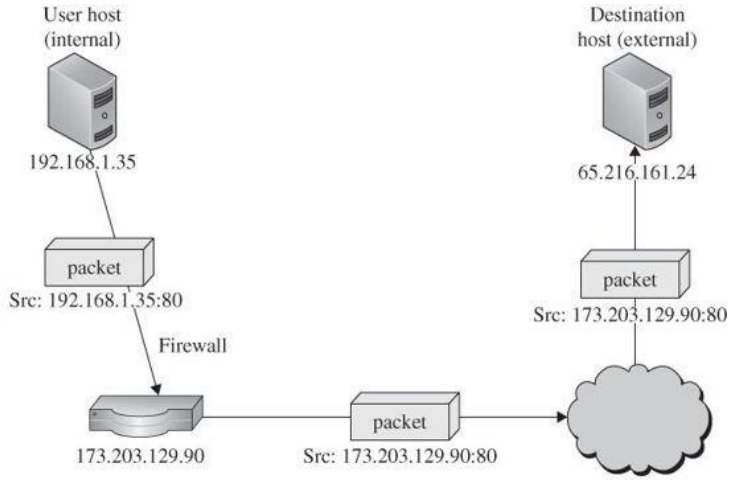


Table of translations performed	
Source	Dest
192.168.1.35:80	65.216.161.24:80

- Allow multiple devices with independent network addresses to connect to the internet using a single IP address, keeping individual IP addresses hidden.
- Hence, attackers scanning a network for IP addresses can't capture specific details, providing greater security against attacks.
- NAT firewalls are similar to proxy firewalls in that they act as an intermediary between a group of computers and outside traffic.

- Every packet between two hosts contains source address & port and destination address & port
- NAT firewall conceals real internal addresses from outsiders who don’t know the real addresses and can not access these real addresses directly
- Firewall replaces source address by its own address and keeps entries of original source address & port and destination address & port in a mapping table.

Next Generation Firewalls (NGFW)

- Combines traditional firewall technology with additional functionality, such as encrypted traffic inspection, intrusion prevention systems, anti-virus etc.
- Has capability to deep packet inspection (DPI).
  - While basic firewalls only look at packet headers, deep packet inspection examines the data within the packet itself, enabling users to more effectively identify, categorize, or stop packets with malicious traffic
- TCP handshake checks
- Surface level packet inspection
- May also include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against network

Next Generation Firewalls (NGFW)

- According to Gartner, a next-generation firewall must include:
  - Standard firewall capabilities like stateful inspection
  - Integrated intrusion prevention
  - Application awareness and control to see and block risky apps
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats
- **Examples:** FortiGate (Fortinet), Cisco ASA, Cisco Meraki MX, Sophos XG, SonicWall TZ, CheckPoint, Palo Alto, Juniper etc

Threat Focused NGFW

innovate achieve lead

- These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation.
- A threat-focused NGFW can:
  - Know which assets are most at risk with complete context awareness
  - Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
  - Better detect evasive or suspicious activity with network and endpoint event correlation
  - Greatly decrease the time from detection to clean-up with retrospective security that continuously monitors for suspicious activity and behaviour even after initial inspection
  - Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

NGFW Features

- Breach prevention and advanced security
  - Prevention to stop attacks before they get inside
  - A best-of-breed next-generation IPS built-in to spot stealthy threats and stop them fast
  - URL filtering to enforce policies on hundreds of millions of URLs
  - Built-in sandboxing and advanced malware protection that continuously analyzes file behavior to quickly detect and eliminate threats
  - A world-class threat intelligence organization that provides the firewall with the latest intelligence to stop emerging threats
- Comprehensive network visibility
  - Threat activity across users, hosts, networks, and devices
  - Where and when a threat originated, where else it has been across your extended network, and what it is doing now
  - Active applications and websites
  - Communications between virtual machines, file transfers, and more

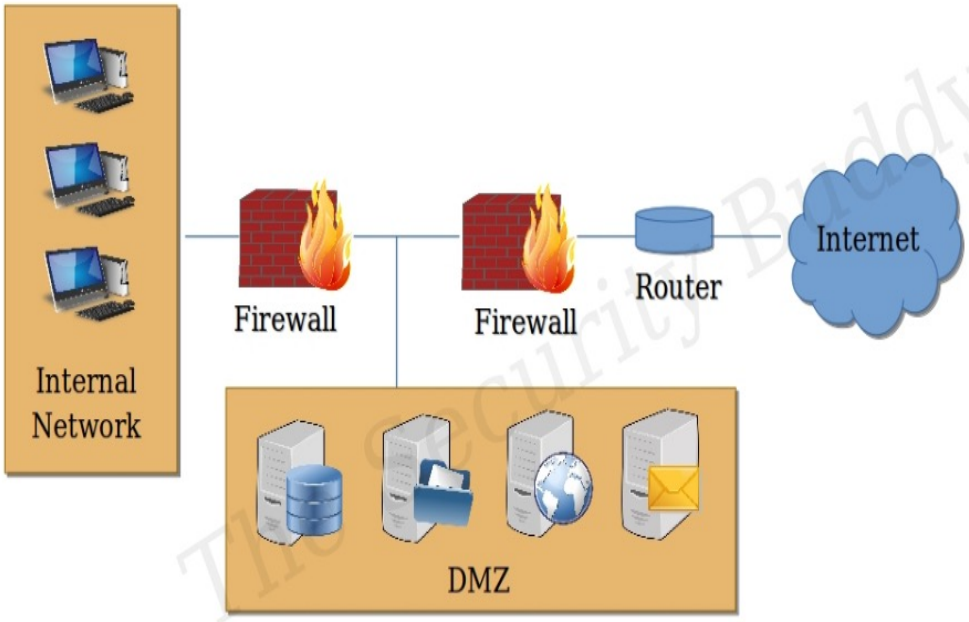
NGFW Features

- Flexible management and deployment options
  - Management for every use case--choose from an on-box manager or centralized management across all appliances
  - Deploy on-premises or in the cloud via a virtual firewall
  - Customize with features that meet your needs--simply turn on subscriptions to get advanced capabilities
  - Choose from a wide range of throughput speeds
- Fastest time to detection
  - Detect threats in seconds
  - Detect the presence of a successful breach within hours or minutes
  - Prioritize alerts so you can take swift and precise action to eliminate threats
  - Make your life easier by deploying consistent policy that's easy to maintain, with automatic enforcement across all the different facets of your organization

NGFW Features

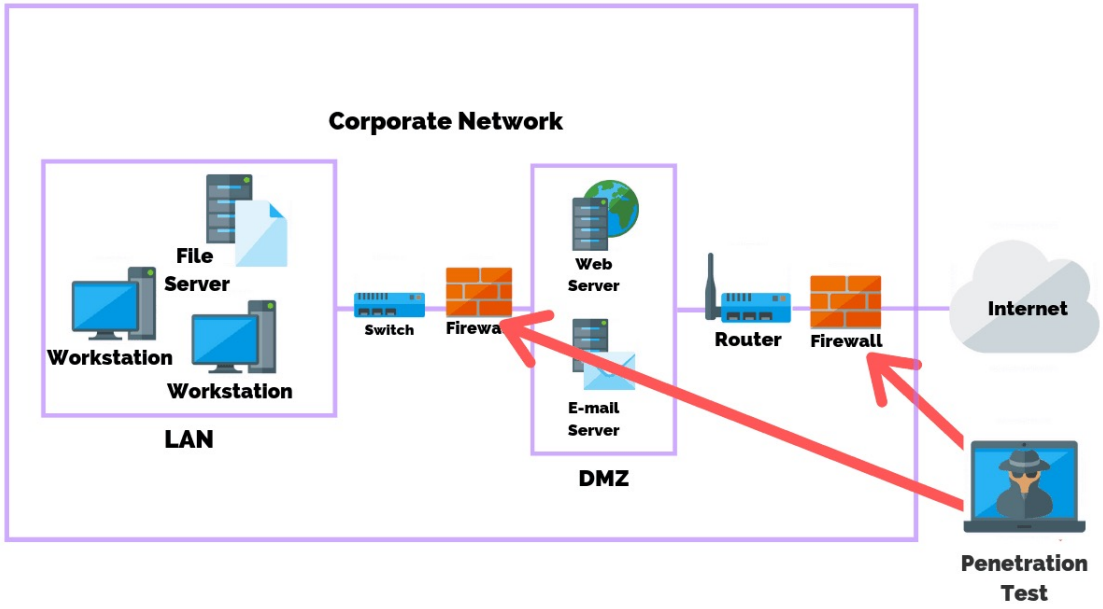
- Automation and product integrations
  - Seamlessly integrates with other tools from the same vendor
  - Automatically shares threat information, event data, policy, and contextual information with email, web, endpoint, and network security tools
  - Automates security tasks like impact assessment, policy management and tuning, and user identification
- Leading Firewalls
  - Fortinet Fortigate
  - Cisco ASA NGFW
  - pfSense
  - Sophos UTM
  - WatchGuard Firebox
  - Meraki MX Firewalls
  - Juniper SRX
  - Palo Alto Network VM-Series

DMZ (De-Militarized Zone)



- A DMZ Network functions as a subnet containing an organization's exposed, outward-facing services.
- DMZ adds an extra layer of security to an organization's local area network.
  - A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ
  - Rest of the organization's network is safe behind a firewall.
- A DMZ provides extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Firewall Penetration Testing Steps



1. Locate firewall
2. Conduct traceroute
3. Port scan
4. Banner grab
5. Access control enumeration
6. Identifying firewall architecture
7. Testing firewall policies
8. Firewalking
9. Port redirection
10. External and internal testing
11. Test for covert channels
12. HTTP Tunneling
13. Identify firewall specific vulnerabilities

Firewall Penetration Testing Steps

- Step 1. Locating The Firewall
  - Every firewall penetration test will begin with locating the firewall.
  - Using any packet crafting software, the tester crafts specific IP packets containing UDP, TCP or ICMP payloads.
  - Common firewall pen-testing tools used are Hping and Nmap.
    - Both tools have similar functionality with one small difference.
    - Hping can only scan 1 IP address at a time compared to Nmap, which can scan a range of IP addresses.
  - Hping is a better choice to avoid any abnormal activity from being detected.
  - By repeating the scanning process, one can map the list of allowed services in the firewall.

Firewall Penetration Testing Steps

- Step 2. Conducting Traceroute
  - Network range can be identified by running a tracert command against the firewall located in the previous step.
  - This step will also provide information regarding the route packets take between systems and determine all routers and devices that are involved in the connection establishing process.
  - Certain information pertaining to devices that filter traffic and protocols used can also be obtained.

Firewall Penetration Testing Steps

- Step 3. Port Scanning
  - The most commonly used tool is Nmap due to the flexibility of its wide customization of scans one wishes to perform.
  - This step identifies open ports on the firewall and also identifies the corresponding services that are running on those open ports.
  - Using Nmap, one can craft a scan that encompasses the type of scan wanted, options for that specific scan type, the timing of the scan etc.
  - For example,
    - Nmap -sS -p 0-1024 x.x.x.x -T4
    - will send packets with a SYN flag raised, to the first 1024 ports using aggressive timing.
    - Depending on the preferences and requirements of the penetration tester, Nmap can export the results of the scan in different formats.

Firewall Penetration Testing Steps

- Step 3. Port Scanning

```
C:\Program Files (x86)\Nmap>nmap.exe -sS [redacted]137 -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:34 W. Europe Daylight Time
Nmap scan report for aib-of-wl[redacted] (10.[redacted])
Host is up (0.11s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
113/tcp  closed ident
135/tcp  open   msrpc
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2701/tcp open   sms-rcinfo
3389/tcp open   ms-wbt-server
6129/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 36.46 seconds
```

  - After mapping all necessary ports and determining the ones that are in an open state, the penetration testers can run another Nmap scan on the open ports to determine which services are running.
  - Running the following Nmap scan will provide that information:
  - Nmap -sV x.x.x.x -T1.
  - After crafting and running different Nmap scans, the penetration tester will have a basic overview of the firewall, open ports, and services running on those ports.

Firewall Penetration Testing Steps

- Step 4. Banner Grabbing
  - Banner grabbing on the firewall will provide information on the version of the firewall in use. This information can be used to find available exploits that can potentially compromise the firewall.
  - Netcat is used to craft a connection request which will provide the tester with the right information.
  - For example, let's say that we identified port 80 on the firewall as open. The following Netcat command will retrieve the firewall banner and the webserver version:
  - nc-nvv 10.0.0.1 80.

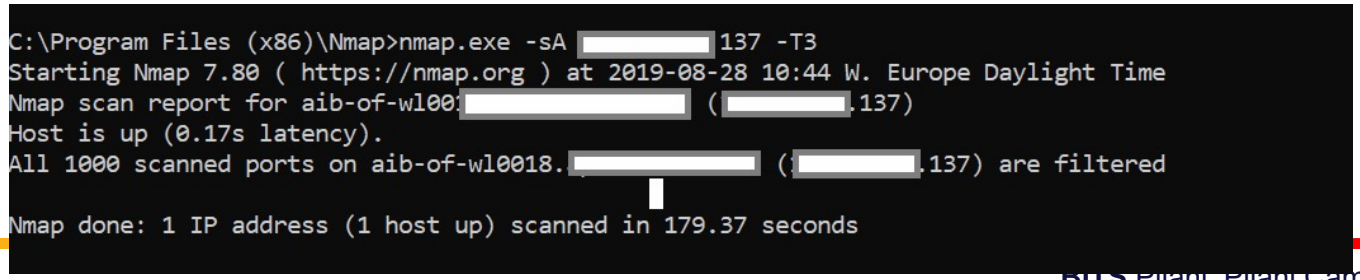
```
C:\Program Files (x86)\Nmap>nmap.exe -sV 10[redacted] -T3
Starting Nmap 7.80 ( https://nmap.org ) at 2019-08-28 10:37 W. Europe Daylight Time
Nmap scan report for [redacted].int ([redacted].137)
Host is up (0.067s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE       VERSION
113/tcp  closed ident
135/tcp  open   msrpc?
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds?
2701/tcp open   cmrcservice   Microsoft Configuration Manager Remote Control service (CmRcService.exe)
3389/tcp open   ms-wbt-server Microsoft Terminal Services
6129/tcp open   damewaremr    DameWare Mini Remote Control
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 245.09 seconds
```

Firewall Penetration Testing Steps

- Step 4. Banner Grabbing
  - Next step is crafting and scanning the firewall using custom made packets.
  - The purpose of this is to elicit different firewall responses and determine which type of firewall you are trying to bypass.
  - Using Hping or Nmap, a penetration tester should try many different variations of the scan in order to gather as much information as possible.
  - Each scan should use different flags (SYN, ACK, FIN etc.) and different protocols (TCP, UDP) in order to attempt connection establishment.
  - Testing different protocols with different connection attributes will elicit the most useful responses from the firewall.

Firewall Penetration Testing Steps

- Step 5. Access Control Enumeration
  - A firewall employs access control lists in order to determine which traffic to allow or deny from the internal network.
  - The only indicator a penetration tester can observe while enumerating the access control list is the state of ports on the firewall.
  - Nmap can also be used to accomplish this step with the following command; Nmap -sA x.x.x.x.
  - Nmap will send packets to the first 1024 ports with the ACK flag raised.
  - This will return results indicating if the port is open, filtered or unfiltered.
  - If the port is in an “Open” state, it is in listening mode.
  - If the state of the port Is “filtered”, it indicates the port is blocked by the firewall.
  - if the port is “unfiltered”, the firewall is passing traffic through the port, but the port is not open.



Firewall Penetration Testing Steps

- Step 6. Identifying Firewall Architecture
  - Sending crafted packets to firewall ports that were already identified will provide a penetration tester with a complete list of port status.
  - By eliciting responses from the firewall on specific ports, the tester will be able to determine the firewall reaction and aid in mapping open ports.
  - Responses from the firewall will let the tester know if the connection was rejected, dropped or blocked.
  - Hping, Hping2 or Nmap can be used to accomplish this task.
  - After initiating the scan, the firewall will send back specific packets indicating the action it took against the scan.
  - If the firewall returns a SYN/ACK packet, the port is in an “Open” state.
  - If the firewall returns a RST/ACK packet, it means the firewall rejected the crafted packet from the tester’s scanner.
  - If no response is received, the firewall dropped the crafted packet indicating a filtered port.
  - If the firewall returns an ICMP type 3 code 13 packet, the connection attempt was simply blocked.

Firewall Penetration Testing Steps

- Step 7. Testing The Firewall Policy
  - Testing of firewall policies can be done in two ways.
  - The penetration tester will either compare hard copies of the extracted firewall policy configuration and the expected configuration in order to identify potential gaps
  - The tester will perform actions on the firewall in order to confirm the expected configuration.

Firewall Penetration Testing Steps

- Step 8. Firewalking
  - Firewalking is a method of mapping the network devices that sit behind the firewall.
  - The Firewalk network auditing tool analyzes packets returned by the firewall with the use of traceroute techniques.
  - It will determine open ports on the firewall by checking devices behind the firewall and thus identify which traffic is able to pass the firewall.
  - The Firewalk tool is considered to perform advanced network mapping and is able to paint a picture of the network topology.
  - By crafting packets with certain TTL values, the penetration tester can identify open ports if the return message is received with the exceeded TTL.
  - If no response is received, it can be concluded that the firewall filtered the packet and blocked the connection.

Firewall Penetration Testing Steps

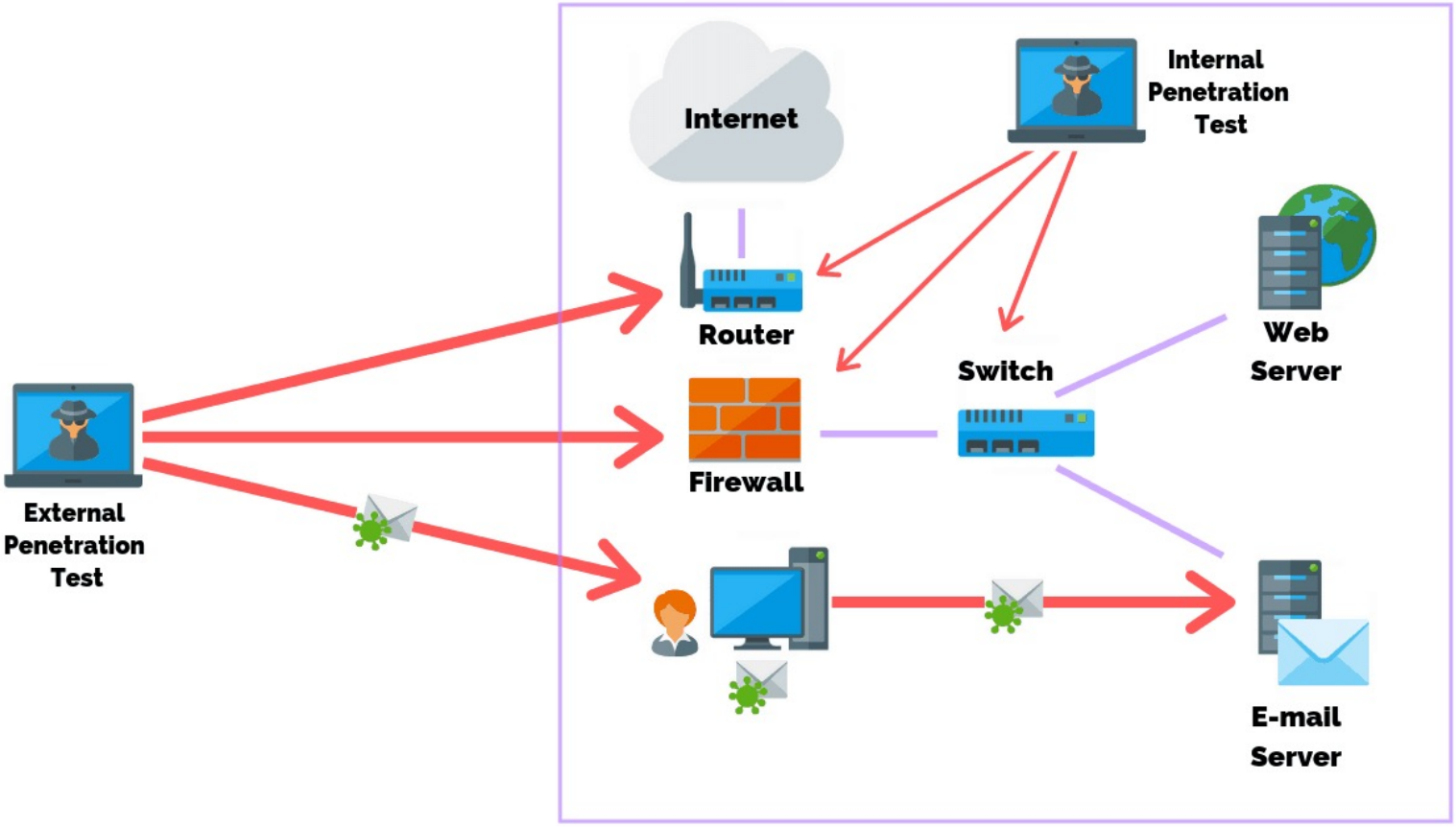
- Step 9. Port Redirection
  - Testing for port redirection is an important step that can allow further compromise of a given network. If a desired port is not accessible directly, port redirection techniques can be used to circumvent the denial of access.
  - If the tester manages to compromise a target system and wants to bypass the firewall, he or she can install a port redirecting tools such as Fpipe or Datapipe and listen to certain port numbers.
  - Once the traffic to the ports is sniffed, it can be redirected to the compromised machine.

```
fpipe -l 53 -s 53 -r 80 192.168.1.101

This would set the program to listen for connections on port 53 and
when a local connection is detected a further connection will be
made to port 80 of the remote machine at 192.168.1.101 with the
source port for that outbound connection being set to 53 also.
Data sent to and from the connected machines will be passed through.
```

Firewall Penetration Testing Steps

- Step 10: External And Internal Testing
  - Performing external and internal penetration tests is not always required when testing the firewall, however, it does provide a more realistic approach of how a malicious actor may attack your systems.
  - An external penetration test researches and attempts to exploit vulnerabilities that could be performed by an external user without proper access and permissions.
  - An internal penetration test is similar to a vulnerability assessment, however, it takes a scan one step further by attempting to exploit the vulnerabilities and determine what information is actually exposed.
  - In order to cover both sides, the tester will send packets from outside of the network and analyze the received packets inside the network.

Firewall Penetration Testing Steps

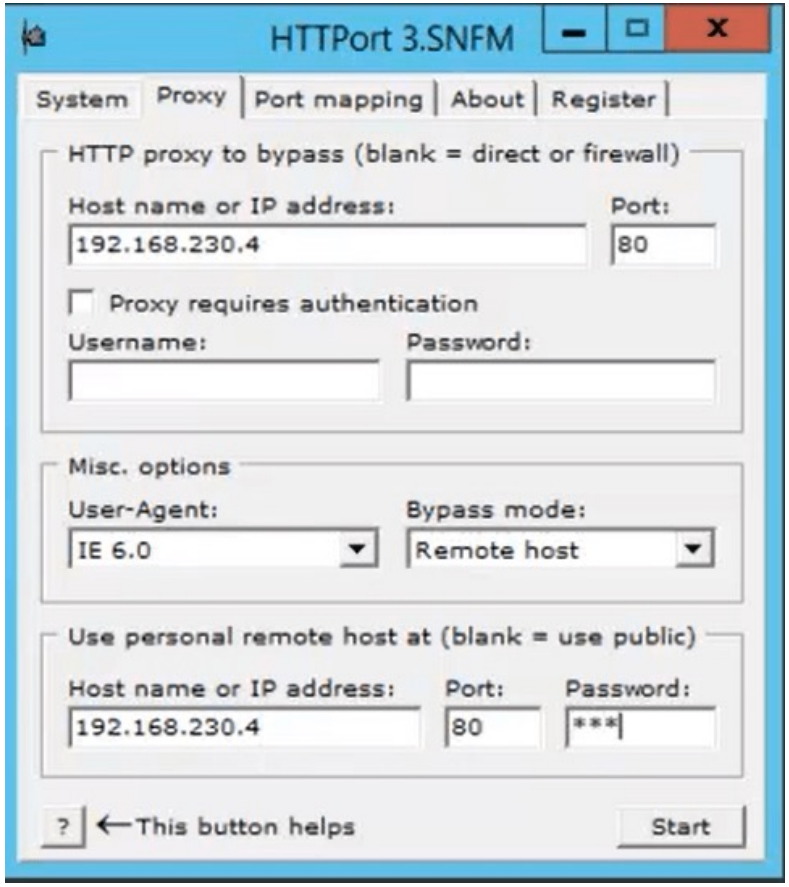


Firewall Penetration Testing Steps

- Step 11. Test For Covert Channels
  - A covert channel is a hidden communication connection that allows hackers to remain stealthy.
  - Mostly used for concealing activities and extracting valuable or sensitive data from a company, covert channels are created by installing a backdoor on a compromised machine inside the network.
  - Once installed, a reverse shell can be created to establish a connection with the outside machine belonging to the hacker.
    - One way of doing this is with the use of the popular hacking platform Metasploit.
  - To test whether establishing a covert channel is doable, the penetration tester will:
    - Identify firewall rules with the help of Firewalk.
    - Attempt to reach systems behind the firewall.
    - Examine the response of the arriving packets.

Firewall Penetration Testing Steps

- Step 12. HTTP Tunneling
  - HTTP tunnelling method consists of encapsulating traffic with HTTP protocol and is often used when there is restricted access to a device that sits behind a firewall or a proxy.
  - In this scenario, HTTPort tool can be used to send POST requests to the HTTP server by specifying hostname, port number and path. As the nature of HTTPort's functionality has the ability to bypass HTTP proxies, the only obstacle left is the enabled connect methods on the proxy itself.
  - If the CONNECT HTTP method is enabled, creating a HTTP tunnel is easy. However, if the CONNECT method is disabled, a remote host mode must be used but requires a significant amount of effort to accomplish.



Firewall Penetration Testing Steps

- 13. Identify Firewall Specific Vulnerabilities
  - If you were wondering how to ensure there are no vulnerabilities in your firewall, the answer is making sure no misconfigurations are present. As this is the main reason hackers manage to penetrate the network, configuring your firewall properly is the most important step you can take.
  - In some cases, printing or file-sharing services are left enabled on certain open ports and allow hackers to bypass the firewall through that vector. Disabling services that are not needed and checking firewall configuration is the only way to ensure safety.

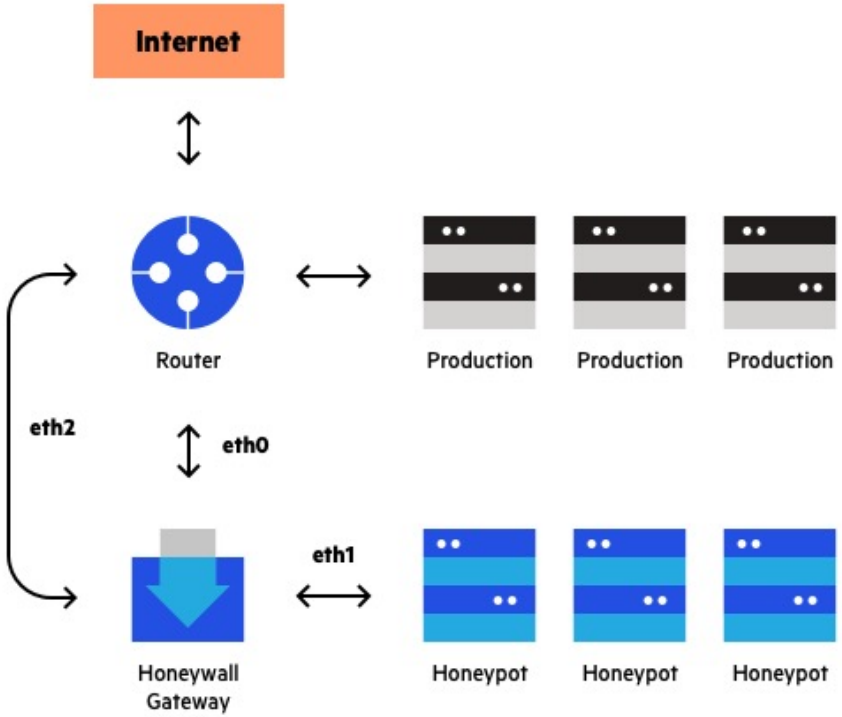
Firewall Penetration Testing: Demo

- Firewall Penetration Testing Demo
  https://youtu.be/0Izu0J6iSoM

- How to bypass Firewall
  https://www.youtube.com/watch?v=cypK0d8wTDs

Honeypots

Honeypots



- A cyber honeypot is a baiting trap for hackers.
- It's a sacrificial computer system to attract cyberattacks, like a decoy.
- Honeypots are filled with fabricated information
- Any access to honeypots triggers monitoring and logging actions
- An attack against a honeypot is made to seem successful
- It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals
- It finds the way hackers operate or distract them from actual targets.

How a Honeypot Works?

- A honeypot looks like a real computer system, with applications and data, fooling cybercriminals into thinking it's a legitimate target.
- Once the hackers are in, they can be tracked, and their behavior assessed for clues on how to make the real network more secure.
- Honeypots are made attractive to attackers by building in deliberate security vulnerabilities.
- Vulnerable ports might be left open to entice attackers into the honeypot environment, rather than the more secure live network.
- A honeypot is an information tool that helps understand existing threats to business and spot the emergence of new threats.
- With the intelligence obtained from a honeypot, security efforts can be prioritized and focused.

Honeypot Level of Interaction

- Low interaction
  - Simple to install
  - Only provides few fake services – port emulation
  - No real operating system that an attacker can operate on
- Medium interaction
  - Provides more interaction
  - Services are still emulated
  - Scripts used to provide more interaction
  - Requires higher skills to deploy
- High interaction
  - Actual operating system in place for interacting with attacker
  - Potential to gather more information
  - Higher risk

Honeypots Uses

- By monitoring traffic coming into the honeypot system, one can assess:
  - where the cybercriminals are coming from
  - the level of threat
  - what modus operandi they are using
  - what data or applications they are interested in
  - how well your security measures are working to stop cyberattacks

Types of Honeypots

- Email traps
- Database decoys
- Malware honeypot
- Spider honeypot

Popular Honeypot Products

- KFSensor – High interaction
- Honeyd – Low to Medium interaction
- Back Office Friendly (BOF) – Low interaction
- Argos
- HoneyBOT
- NetBAIT

Demo

- Hacking for Beginers:
  https://www.youtube.com/watch?v=B7tTQ272OHE
- Honeypots
  https://www.youtube.com/watch?v=fQqWe8br2Gw
- Burp Suite Demo
  https://www.youtube.com/watch?v=G3hpAeoZ4ek
- Cisco NGFW Firepower
  https://www.youtube.com/watch?v=e-CtcCPIy04

Thank You