



BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP



SSZG681: Cyber Security

Lecture No: 05

Strategic Defense

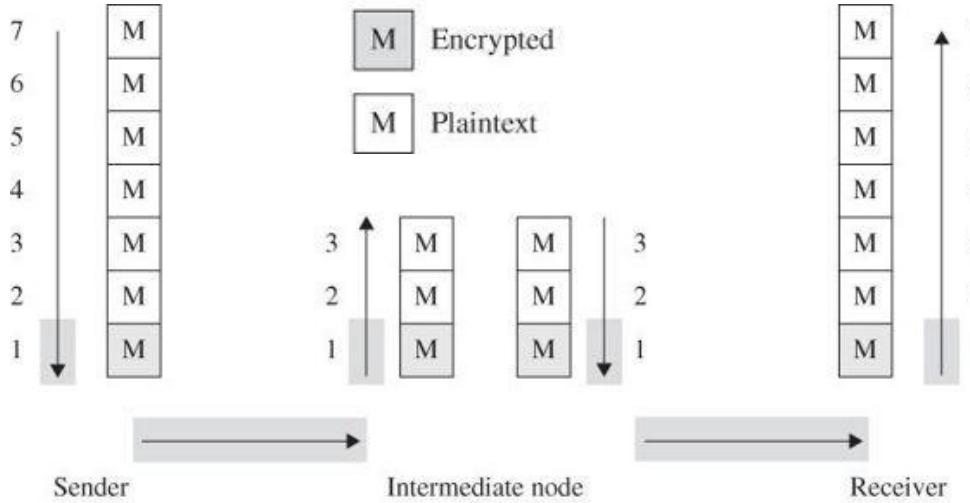
Agenda

- Network Security Strategies
 - Network & Browser Encryption
 - The Onion Routing (TOR)
 - IP Security Protocol Suite
 - Virtual Private Networks
 - Network Architecture
- Firewalls
 - What is a firewall
 - Design of firewall
 - Types of firewall
 - Comparison of firewall types
 - Firewall configuration
 - Network address translation
 - Data Loss Prevention

Network Encryption

- Encryption protects only what is encrypted. At sender or receiver end once data is decrypted, it's exposed to threats
- Encryption algorithm design is work of professionals
- Encryption is no more secure than its key management. Once key is revealed, encryption is of no use
- Encryption is not cure for all ailments. A flawed system design with super encryption is still a flawed system
- Encryption types:
 - **Link encryption:** Host to Host
 - **End to end encryption:** Application to Application

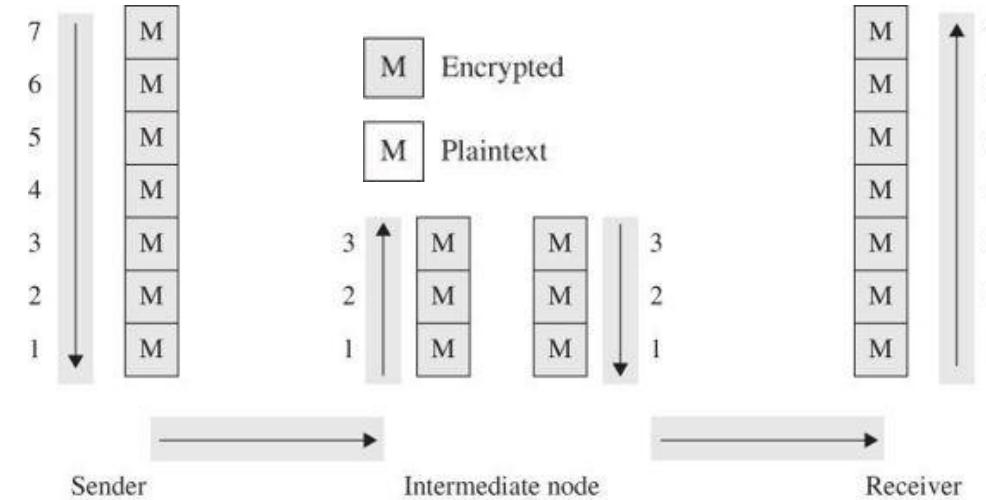
Link Encryption



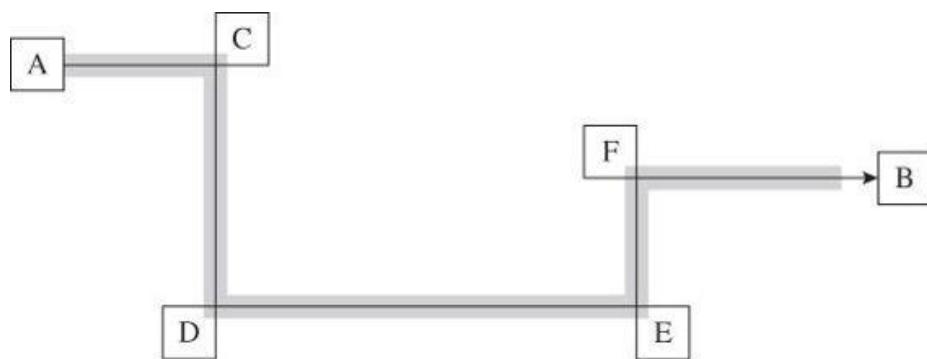
- Data is encrypted just before it's put on the physical network
- Encryption occurs at layer 1 or 2 in OSI network model
- Link encryption covers the communication from one node to next on the path to destination
- Message remains plaintext within the hosts
- Data is in an encrypted state while it travels on its communication path. However, when it reaches a router or another intermediate device, it gets decrypted so that the mediator 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. In principle, it prevents potential eavesdroppers – including telecoms, ISPs and other intermediaries.



Link v/s End-to-End Encryption

Link Encryption	End-to-End Encryption
Security within hosts	
Data partially exposed in sending host	Data protected in sending host
Data partially exposed in intermediate nodes	Data protected through intermediate nodes
Role of user	
Applied by sending host	Applied by user application
Invisible to user	User application encrypts
Host administrators select encryption	User selects algorithm
One facility for all users	Each user selects
Can be done in software or hardware	Usually software implementation; occasionally performed by user add-on hardware
All or no data encrypted	User can selectively encrypt individual data items
Implementation considerations	
Requires one key per pair of hosts	Requires one key per pair of users
Provides node authentication	Provides user authentication

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

Cypher Suite

- Cypher 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
-

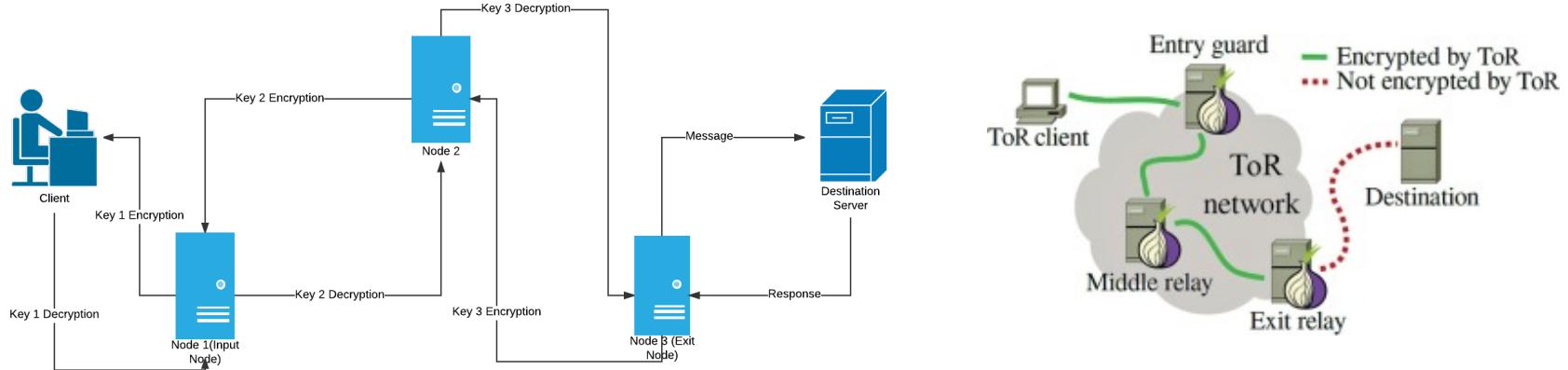
SSL (HTTPS) Session

- Client requests an SSL session
- Client sends a symmetric session key encrypted using server's public key
- Server decrypts the session key and responds back to client
- Both server and client compute session key and initiate encrypted communication
- Details of the session can be viewed in the browser
- SSL certificates are signed by Certified Authorities
- SSL protects data from client browser to server's decryption point
- Keystroke logger and man in browser can still access plaintext data
- LocalSSL provides the local environment protection

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)

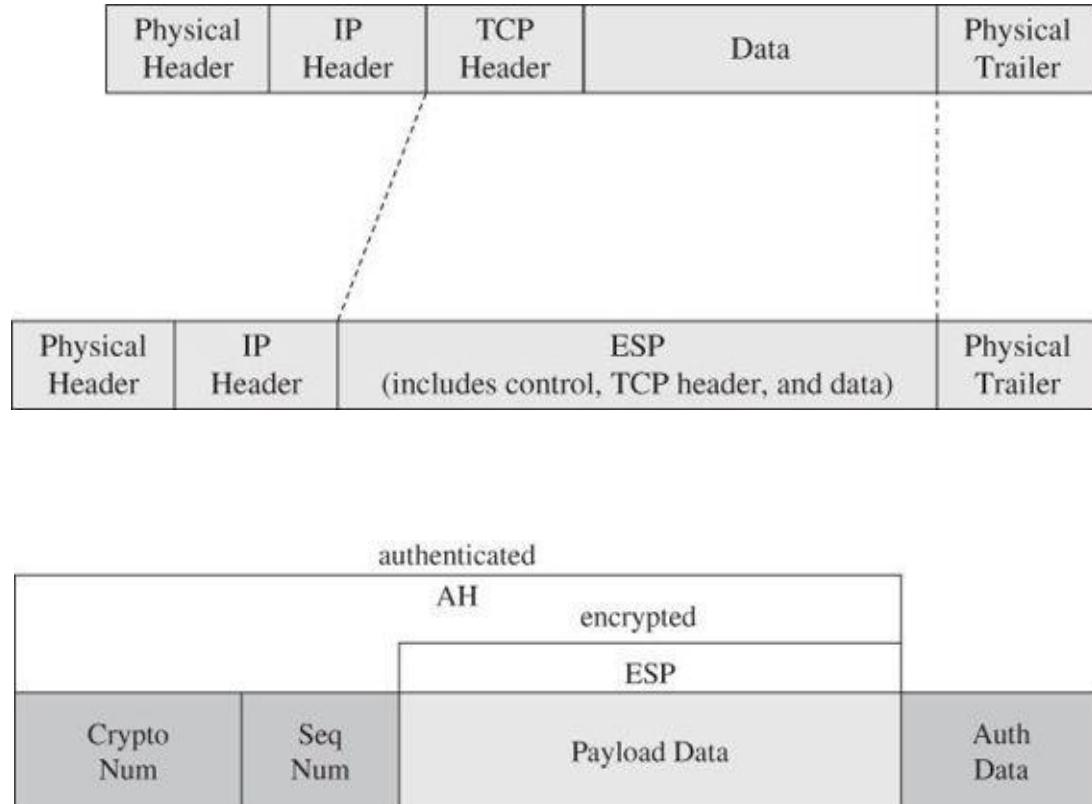


- The client with access to all the encryption keys i.e **key 1, key 2 & key 3** encrypts the message (get request) thrice wrapping it under 3 layers like an onion which have to be peeled one at a time.
- This **triple encrypted message** is then sent to the first server i.e. **Node 1(Input Node)**.
- 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 off 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

IP Security Protocol (IPSec)

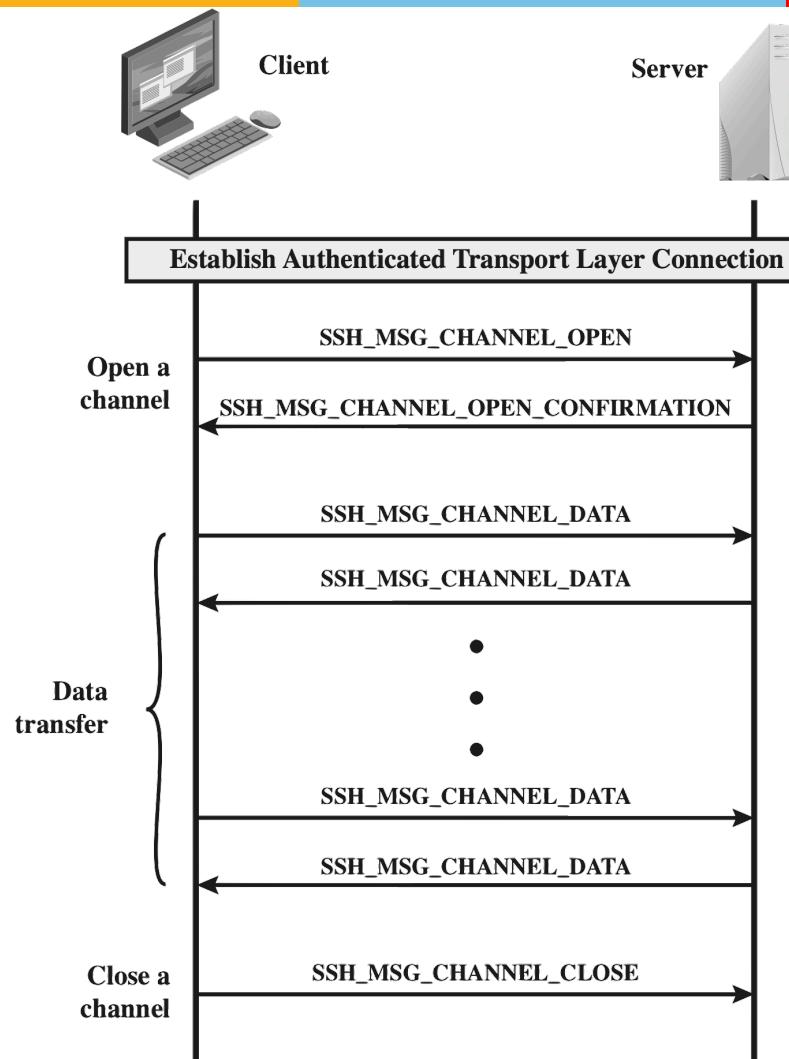
- IPSec implemented at OSI layer 2 (data layer)
- Implements encryption and authentication
- Allows two communicating parties to agree on mutually supported set of protocols
- Security Association (SA): a set of security parameter for a secured communication channel
- SA includes:
 - Encryption algorithm, 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

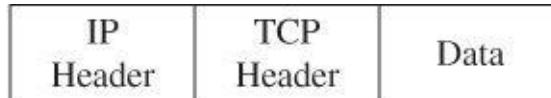
Communication Setup Between Sender & Receiver



Key Management

- Managed thru Internet Security Association Key Management Protocol (ISAKMP)
- Distinct key for each security association
- Key exchange between sender and receiver implemented thru ISAKMP Key Exchange (IKE)
- Usage Diffie-Hellman scheme to generate a mutually shared secret key to be used for encryption
- IPSec enforces both confidentiality (thru symmetric encryption) and authentication (thru asymmetric algorithm for signing with private key)
- A hash function can also be used to protect against modifications (integrity)

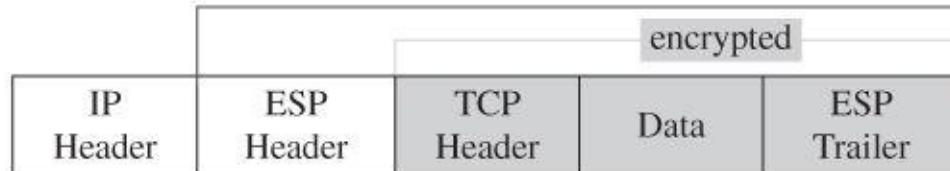
Modes of Operation



(a) Original Packet

authenticated

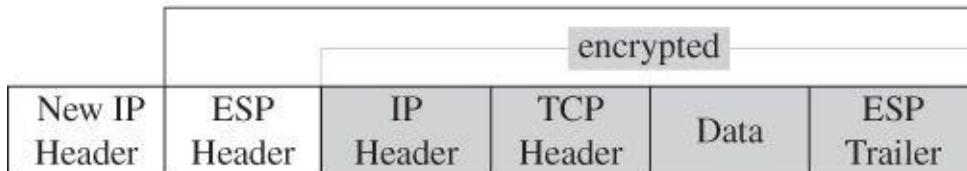
encrypted



(b) Transport Mode

authenticated

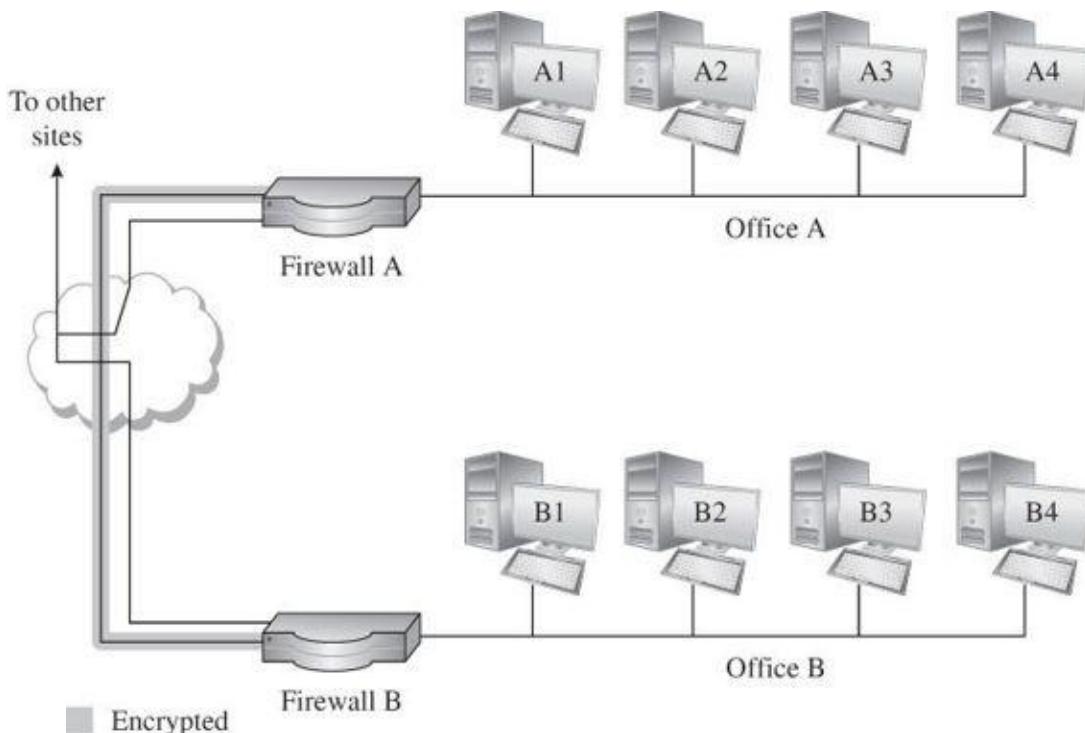
encrypted



(c) Tunnel Mode

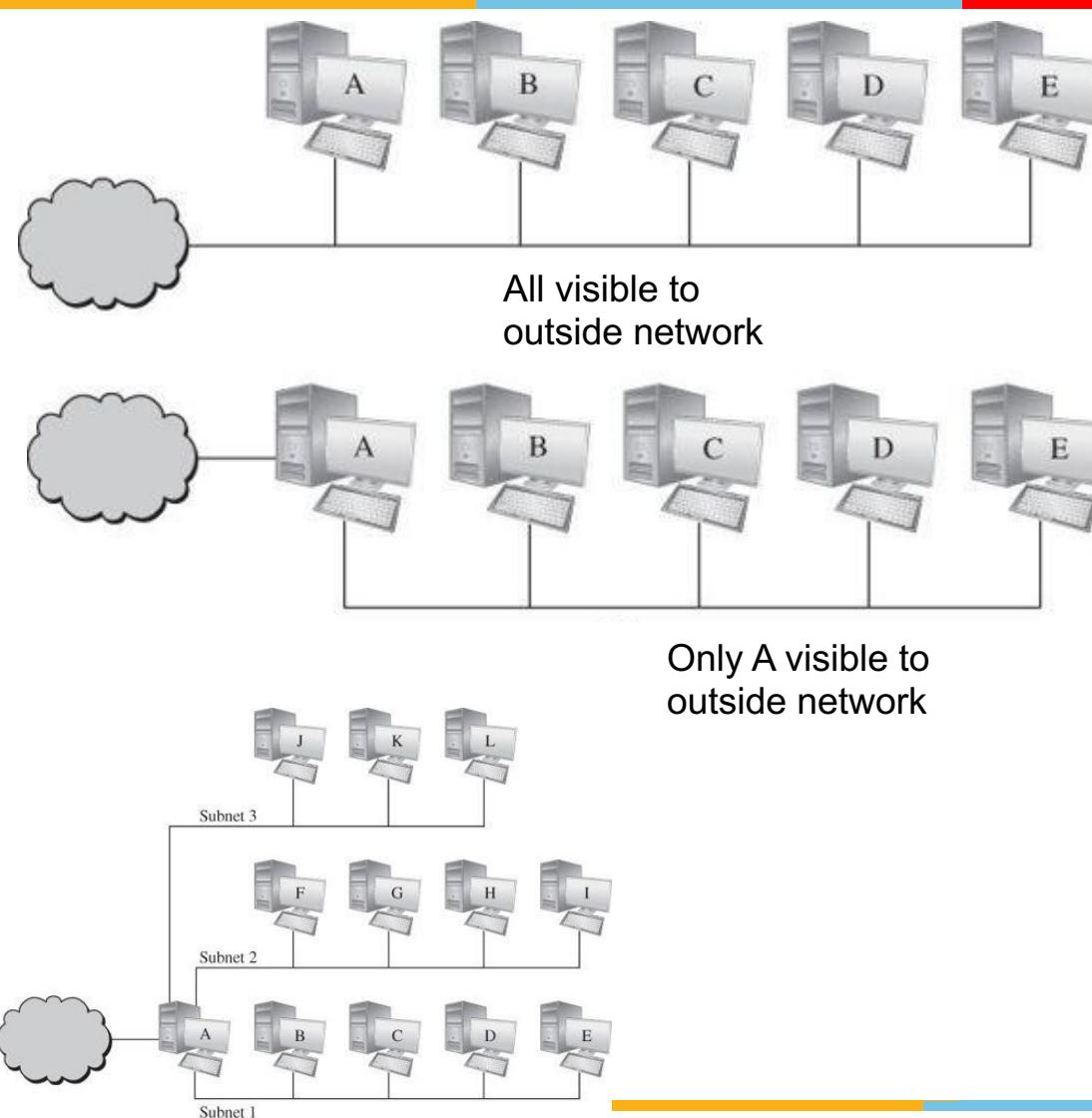
- **Transport mode:** Normal mode where IP address header is unencrypted
- **Tunnel mode:** Recipient address is concealed thru encryption, IPSec substitutes address of a remote device like firewall, that will receive the packet and remove IPSec encryption.

Virtual Private Networks (VPNs)



- A VPN simulates the security of a dedicated, protected communication line on a shared network
- Link encryption between two secure sites can provide a VPN between two distant sites
- Firewalls used to establish VPN connections
- Can also be used for communication between office and home users

Network Architecture



- Network architecture can be designed to protect a set of computers from outside network access
- Something similar to limited direct inward dialing feature of a hospital telephone system
- Protected subnets are created for this implementation
- Protected subnets can separate departments, projects, clients, areas, any sub-group requiring controlled access to data or communication

Firewalls

What is a Firewall?

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

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 Trust

- Firewall is a reference monitor, positioned to monitor all traffic, is not accessible to outside attacks, and implements only access control
- Firewall is positioned as single physical point of connection between protected and uncontrolled networks. This placement ensures firewall is invoked always
- Typically implemented on a separate & dedicated computer with stripped down operating system running minimal utilities hence making it temper proof. Even firewall traffic audit logs need to be transported to another machine for reading purpose
- Firewall are simple and small with bare minimum functionality

Firewall Generation

- **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)

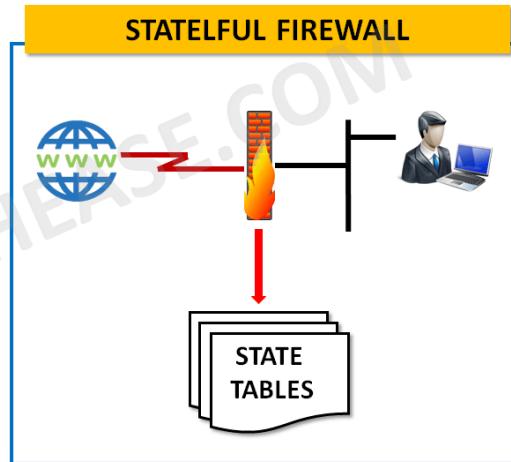
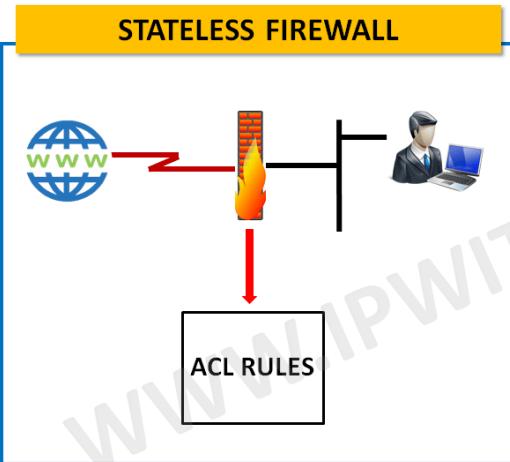
Packet Filtering Firewall

	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

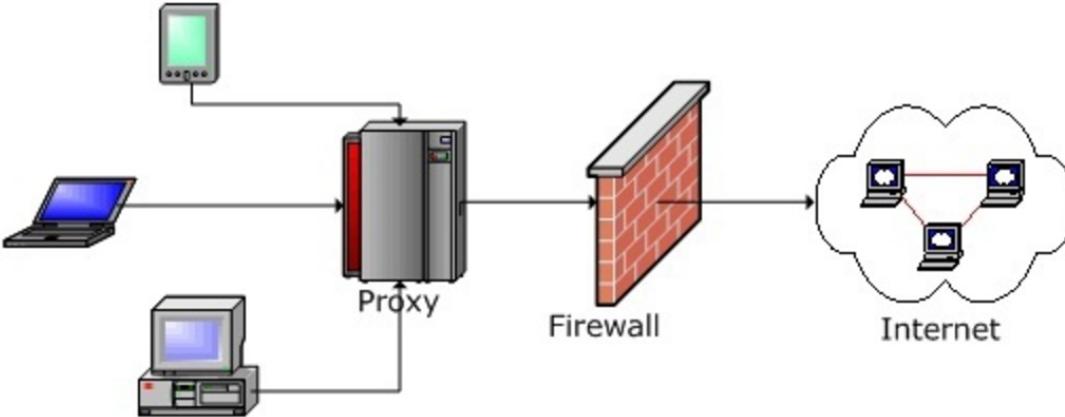
Stateful Inspection Firewall



- 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 disallowed

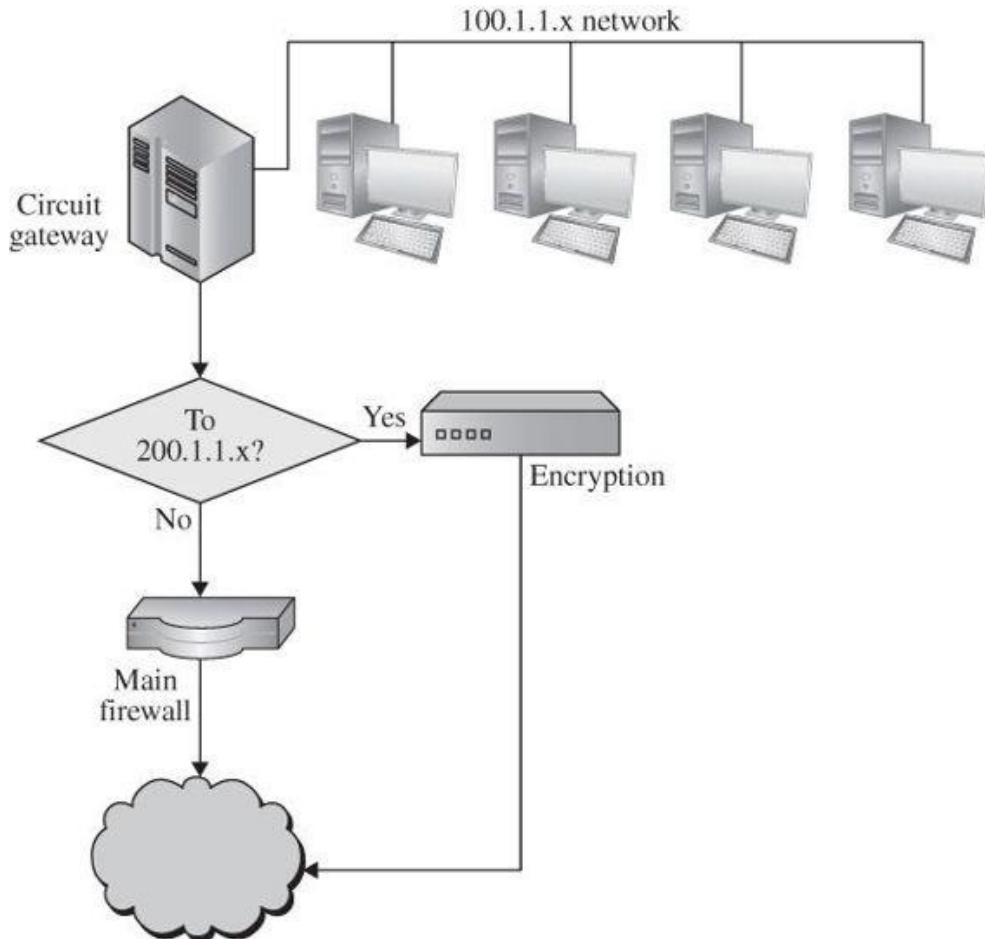
Application Proxy Firewall



- Proxy acts as 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

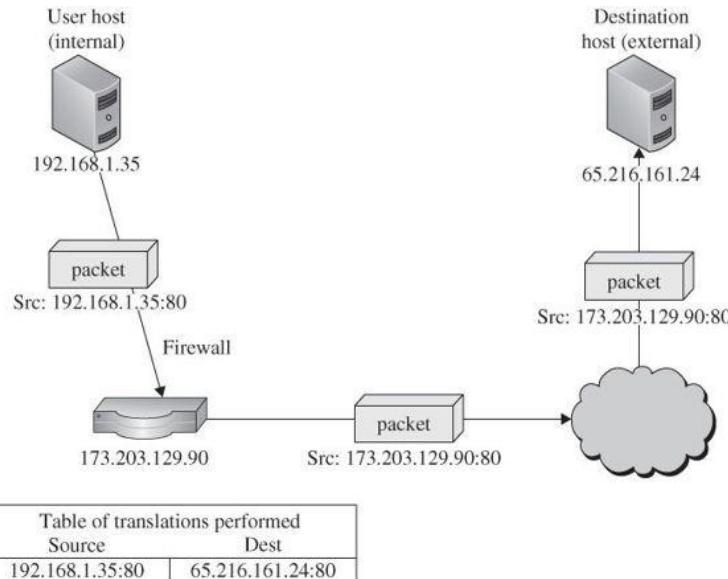
Guard Firewall

- 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)



- 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

- These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you 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

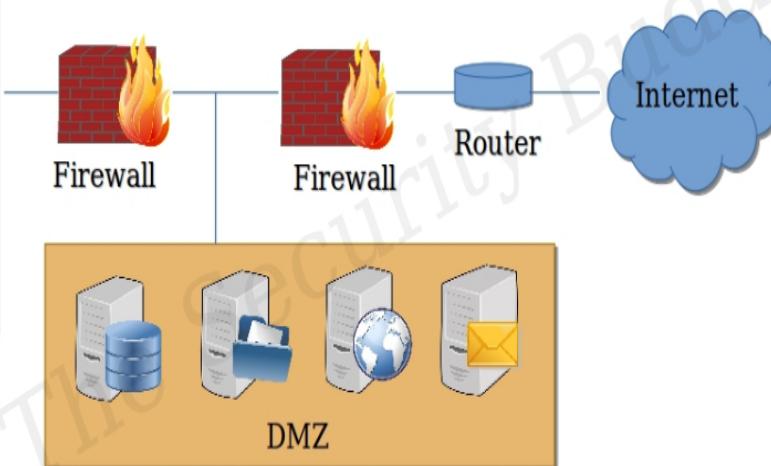
NGFW Features

- 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

Comparison of Firewalls

Packet Filter	Stateful Inspection	Application Proxy	Circuit Gateway	Guard	Personal Firewall
Simplest decision-making rules, packet by packet	Correlates data across packets	Simulates effect of an application program	Joins two subnetworks	Implements any conditions that can be programmed	Similar to packet filter, but getting more complex
Sees only addresses and service protocol type	Can see addresses and data	Sees and analyzes full data portion of pack	Sees addresses and data	Sees and analyzes full content of data	Can see full data portion
Auditing limited because of speed limitations	Auditing possible	Auditing likely	Auditing likely	Auditing likely	Auditing likely
Screens based on connection rules	Screens based on information across multiple packets—in either headers or data	Screens based on behavior of application	Screens based on address	Screens based on interpretation of content	Typically, screens based on content of each packet individually, based on address or content
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex decision rules, but proxies must be aware of application's behavior	Relatively simple addressing rules; make configuration straightforward	Complex guard functionality; can be difficult to define and program accurately	Usually starts in mode to deny all inbound traffic; adds addresses and functions to trust as they arise

DMZ (De-Militarized Zone)



- A DMZ Network (De-Militarized Zone) functions as a subnetwork containing an organization's exposed, outward-facing services.
- The goal of a DMZ is to add 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, while the rest of the organization's network is safe behind a firewall.
- A DMZ gives extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Objective of DMZ

- DMZ Network protects the host's most vulnerable to attack. These hosts usually involve services that extend to users outside of the local area network like email, web servers, and DNS servers.
 - Because of the increased potential for attack, they are placed into the monitored subnetwork to help protect the rest of the network if they become compromised.
 - Hosts in the DMZ have tightly controlled access permissions to other services within the internal network, because the data passed through the DMZ is not as secure.
 - All services accessible to users on communicating from an external network should be placed in the DMZ. The most common services are: Web Server, Mail Server, FTP Server etc.
-

Single Firewall DMZ

- Requires a single firewall and minimum of 3 network interfaces.
- DMZ is placed Inside of this firewall.
 - Tier of operations are as follows:
 - External network device makes the connection from the ISP
 - Internal network is connected by the second device
 - Connections within the DMZ is handled by the third network device.

Dual Firewall DMZ

- More secure approach is to use two firewalls to create a DMZ.
 - The first firewall (referred to as the “frontend” firewall) is configured to only allow traffic destined for the DMZ.
 - The second firewall (referred to as the “backend” firewall) is only responsible for the traffic that travels from the DMZ to the internal network.
 - An effective way of further increasing protection is to use firewalls built by separate vendors, because they are less likely to have the same security vulnerabilities.
 - While more effective, this scheme can be more costly to implement across a large network.
-

Firewall Limitations

- Firewall can protect an environment only if the firewall controls entire perimeter
 - Firewalls do not protect data outside perimeter
 - Firewalls are most visible part of an installation to outsiders and hence most attractive target for attack
 - Firewalls must be configured correctly and the configuration must be updated as the internal and external environment changes
 - Firewalls are targets for intruders, check firewall logs periodically for evidence of attempted or successful intrusions
 - Firewalls exercise only limited control over the content inside packet and hence may not be able to stop malicious code or inaccurate data completely
-

Data Loss Prevention (DLP)

- Set of technologies designed to detect and possibly prevent attempt to send data where it is not allowed to go
- Classified documents, proprietary information, personal information etc in light of Wiki leaks / Edward Snowden scandal
- Two implementation of DLP:
 - **Agent based:** Installed as a rootkit to monitor user behavior like network connections, file access, applications run etc
 - **Application based:** Software agents to monitor email, file transfer etc
- DLP looks for indicators:
 - **Keywords:** set of identified words in the data
 - **Traffic patterns:** bulk file transfer, file sharing, connection to outside email etc
 - **Encoding/encryption:** block outgoing files that they can't decode/decrypt



Leading Enterprise Firewall Products

- Fortinet Fortigate
- Cisco ASA NGFW
- pfSense
- Sophos UTM
- WatchGuard Firebox
- Meraki MX Firewalls
- Juniper SRX
- Palo Alto Network VM-Series



Thank You