Parul® University

Network Defense tools

Prof. Rameez Raja
Cyber security trainer

Parul®
University

DIGITAL LEARNING CONTENT

CHAPTER-3

Network Defense tools

Parul® University

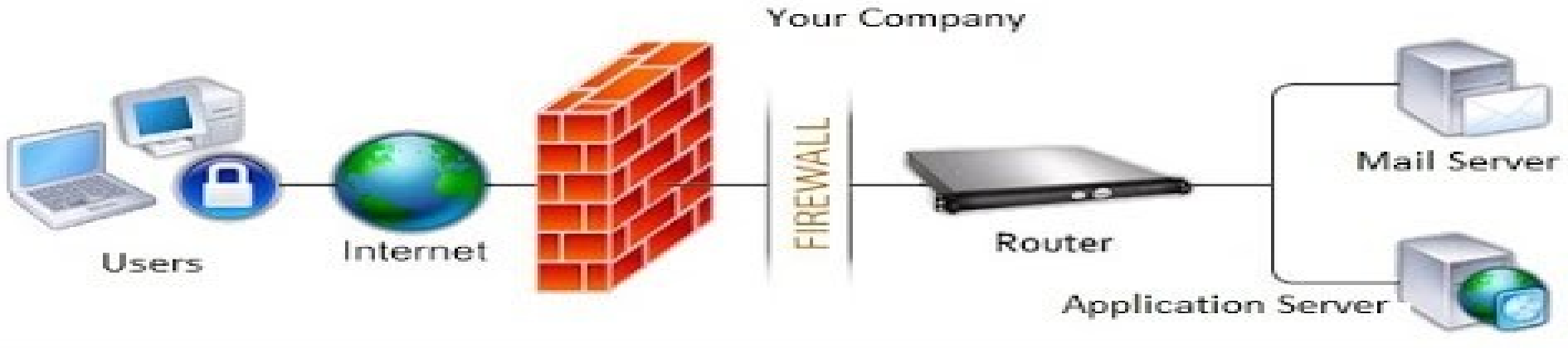
Network Defense tools

Network defense tools play a crucial role in protecting computer networks from various cyber threats and attacks. These tools help organizations monitor, detect, and respond to security incidents, ensuring the integrity, confidentiality, and availability of their network resources.

Example:

- **Antivirus and Anti-malware Software** (McAfee, Windows Defender).
- **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)** (Snort, Suricata, Cisco Firepower)
- **Firewalls** (Cisco ASA, Palo Alto Networks, pfSense).
- **Virtual Private Network** (VPN) (OpenVPN, Cisco AnyConnect, Palo Alto GlobalProtect).

What is a Firewall?

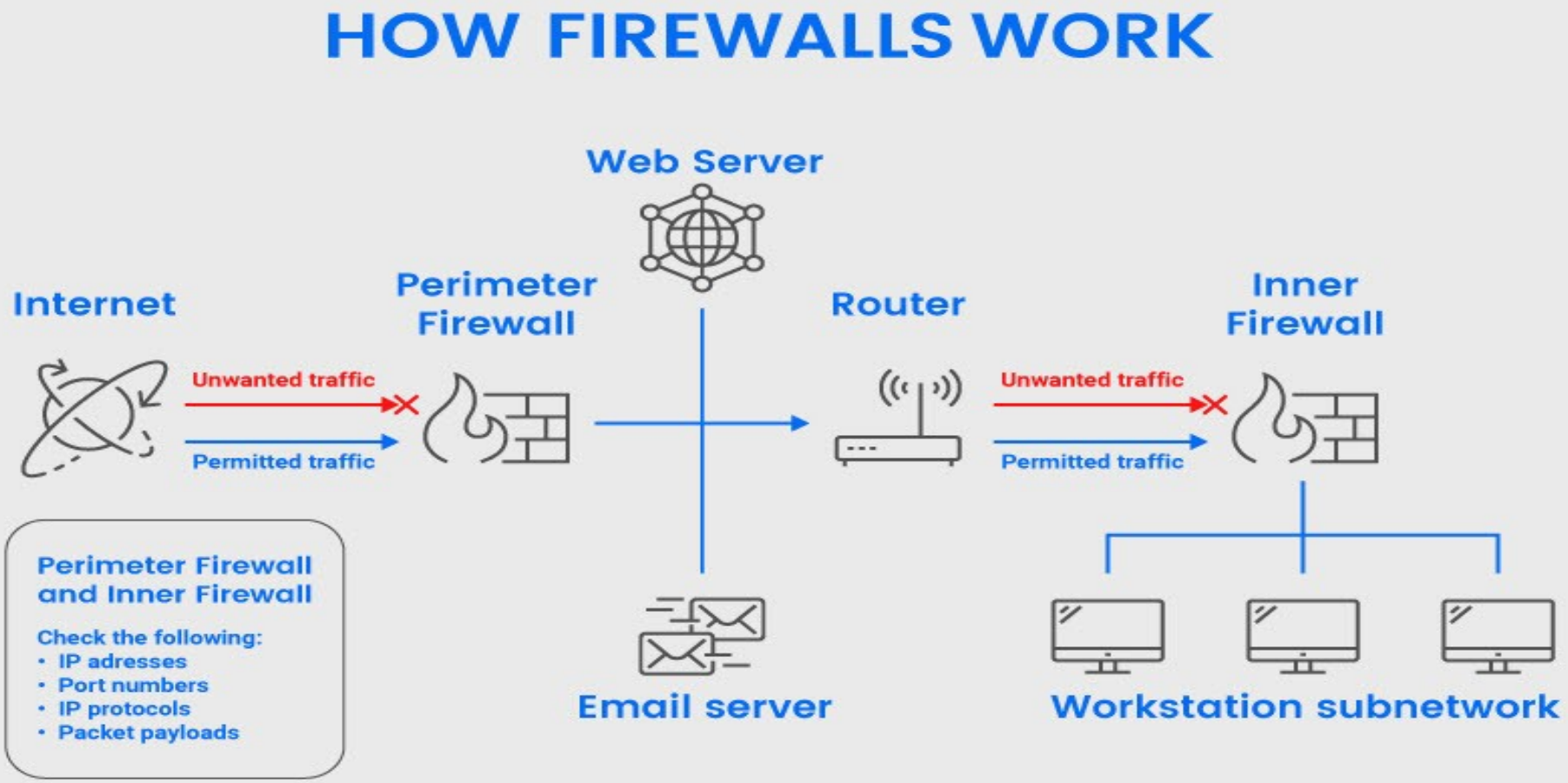


What is a Firewall?

- Firewalls act as a barrier between a trusted internal network and untrusted external networks, controlling the flow of network traffic based on predetermined security rules.

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules making our network secure and more reliable.

How Firewalls Work?



Key Functions of Firewalls:

1.Packet Filtering:

Firewalls inspect individual data packets and make decisions about whether to allow or block them based on pre-defined rules.

2.Stateful Inspection:

Stateful inspection, also known as dynamic packet filtering, keeps track of the state of active connections and makes decisions based on the context of the traffic.

Key Functions of Firewalls:

3. Proxying:

Proxies act as intermediaries between internal and external systems. They can enhance security by filtering and forwarding requests and responses.

4. Network Address Translation (NAT):

Firewalls often use NAT to modify network address information in packet headers while in transit, helping conceal internal IP addresses. Example: A firewall with a proxy server may receive an HTTP request from an internal user, then forward that request to the internet on behalf of the user, masking the user's internal IP address.

Key Functions of Firewalls:

4. **Virtual Private Network (VPN) Support:**
   Firewalls can facilitate secure communication over the internet by supporting VPNs, which encrypt data as it travels between networks.
   Example: Allowing employees to connect securely to the corporate network from remote locations using VPN protocols like IPsec or SSL/TLS.
5. **Logging and Auditing:**
   Firewalls maintain logs of network traffic and security events, allowing administrators to monitor and analyze activity for security purposes.

Types of Firewall

01 Packet-filtering firewall

02 Stateful Multi-Layer Inspection (SMLI)

03 Stateless firewall

04 Application-level gateway (Proxy firewall)

05 Circuit-level gateway

06 Next-Generation Firewall (NGFW)

07 Cloud firewall

1. Packet Filtering Firewalls

Definition: Packet filtering firewalls operate at the network layer (Layer 3) of the OSI model. They examine each packet of data entering or leaving the network and decide whether to allow or block it based on predefined rules.

Uses: Packet filtering is often used to control access based on IP addresses, protocols, and port numbers.

Example: iptables on Linux is a popular packet filtering firewall

Parul® University

Parameters for filtering

1.Packet Inspection:

1. Packet filtering firewalls inspect individual packets of data as they pass through the network.
2. Each packet is examined based on specific criteria defined by rules.

2.Rule-Based Filtering:

1. Packet filtering is rule-based, where administrators define rules to dictate which packets are allowed and which are denied.
2. Rules are typically based on attributes such as source and destination IP addresses, source and destination port numbers, and the protocol type.

Parul® University

Parameters for filtering Contd.

3.Filtering Criteria:

1. **Source IP Address:** The IP address of the sender or originator of the packet.
2. **Destination IP Address:** The IP address of the intended recipient of the packet.
3. **Source and Destination Port Numbers:** Identifies the specific application or service using the port numbers.
4. **Protocol Type:** Specifies the communication protocol (e.g., TCP, UDP, ICMP).

4. Access Control Lists (ACLs):

5. Rules are often implemented using Access Control Lists (ACLs), which are lists of rules that define what kind of traffic is allowed or denied.
6. ACLs can be configured to permit or deny traffic based on the defined criteria.

2. Stateful Multi-Layer Inspection (SMLI)

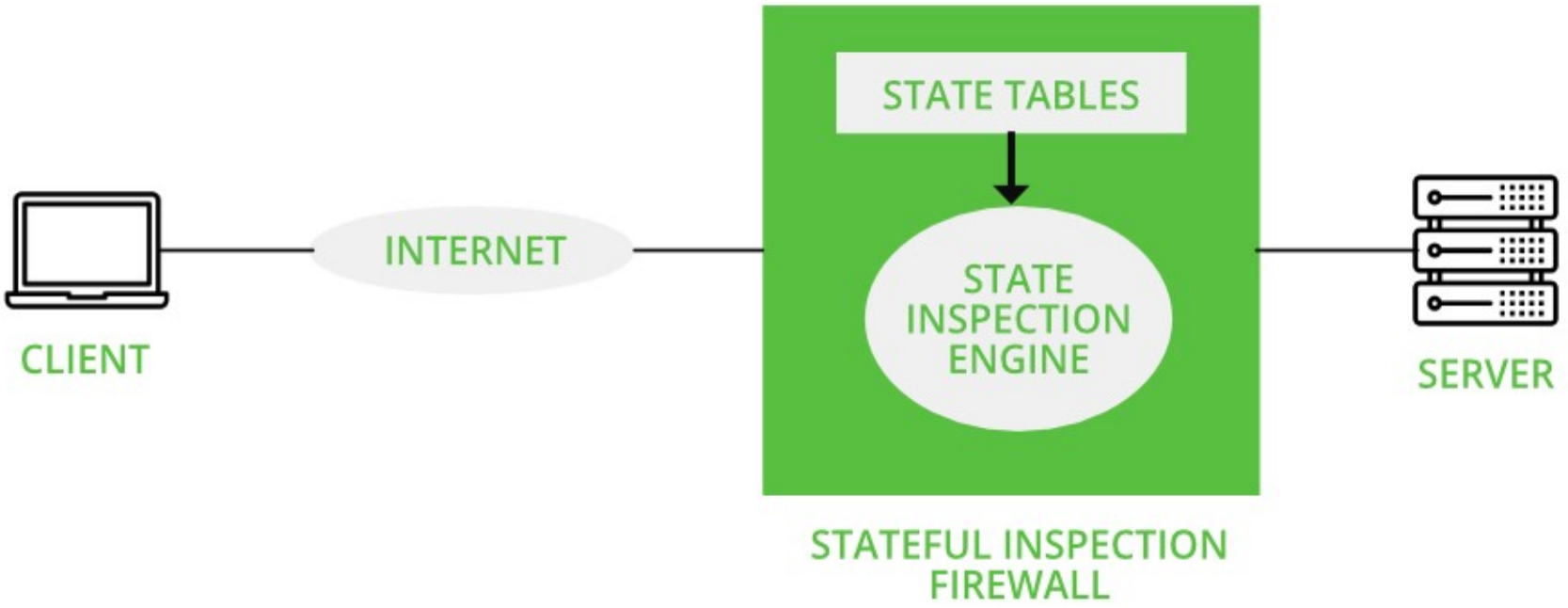
Stateful Multi-Layer Inspection (SMLI) is an advanced security approach that combines stateful inspection with multiple layers of analysis to provide a more comprehensive and effective means of protecting computer networks. This approach goes beyond traditional packet filtering and stateless inspection to consider the context and content of network traffic. The detailed concept of Stateful Multi-Layer Inspection is available on next slide

Example: Cisco ASA , Fortinet FortiGate.

Stateful Multi-Layer Inspection (SMLI)

1. **Stateful Inspection:**
    1. **Connection Tracking:** Stateful inspection involves tracking the state of active connections and making decisions based on the context of the traffic.
    2. **Session Awareness:** It understands the state of network connections and can differentiate between new connection requests and established sessions.
2. **Multi-Layer Inspection:**
    1. **Network Layer:** Analyzes traffic at the network layer (Layer 3), considering source and destination IP addresses, as well as protocol types (e.g., TCP, UDP).
    2. **Transport Layer:** Examines transport layer information, such as source and destination port numbers, to identify the specific application or service.
    3. **Application Layer:** Goes beyond the network and transport layers to inspect the actual content of the data payload at the application layer (Layer 7). This allows the firewall to understand the context and nature of the traffic, including the applications being used.

Working of Stateful Inspection



Working of Stateful Inspection

1. Stateful inspection detects communications packets over a period of time and examines both incoming and outgoing packets.

2. The firewall follows outgoing packets that request specific sorts of incoming packets and authorize incoming packets to undergo as long as they constitute an accurate response.

3. A stateful firewall monitors all sessions and verifies all packets, although the method it uses can vary counting on the firewall technology and therefore the communication protocol getting used.

Working of Stateful Inspection

4. For example, when the protocol is TCP, the firewall captures a packet's state and context information and compares it to the prevailing session data.
5. If an identical entry already exists, the packet is allowed to undergo the firewall.
6. If the match is not found, then the packet must undergo certain policy checks. At that time, if the packet meets the policy requirements, the firewall assumes that it's for a replacement connection and stores the session data within the appropriate tables. It then permits the packet to pass.
7. If the packet does not match the policy conditions, the packet is rejected.

3. Stateless firewall

A Stateless Firewall is a network security device that filters and controls network traffic based solely on the predefined rules and criteria, without considering the context or state of the connections. Unlike Stateful Firewalls, which maintain a table of active connections and make decisions based on the state of each connection, Stateless Firewalls treat each packet in isolation

example : Cisco IOS Access Control Lists (ACLs)

Stateless firewall

1. Packet-Level Filtering:

1. Stateless Firewalls operate at the network layer (Layer 3) of the OSI model and inspect individual packets of data.
2. Filtering decisions are based on specific attributes of each packet, such as source and destination IP addresses, source and destination port numbers, and protocol type (e.g., TCP, UDP, ICMP).

2. Rule-Based Filtering:

3. Administrators define rules that dictate which packets are allowed and which are denied.
4. Rules are typically based on static criteria, such as IP addresses and port numbers, without considering the state of connections.

Stateless firewall

3. No Connection Tracking:

1. Unlike Stateful Firewalls, Stateless Firewalls do not maintain a table of active connections or sessions.
2. Each packet is evaluated independently of previous or subsequent packets.

4. Efficiency:

3. Stateless Firewalls are generally more efficient than Stateful Firewalls in terms of processing speed because they don't have to keep track of connection states.
4. This makes them suitable for high-speed networks and environments where minimal latency is crucial.

4. Application-level gateway (Proxy firewall)

An Application Layer Gateway (ALG) firewall, also known as a proxy firewall, operates at the application layer (Layer 7) of the OSI model. Unlike traditional firewalls that work at lower layers and filter traffic based on IP addresses and port numbers, ALG firewalls understand specific application protocols and can make decisions based on the content of the data being transmitted. ALG firewalls act as intermediaries between clients and servers, providing enhanced security features.
Example : Squid Proxy Server.

Benefits of Application-level gateways

- Safest firewall
- Deep packet inspection
- Significant slowdowns
- Safeguard resource identity and location

5. Circuit-level gateway

A Circuit-Level Gateway (CLG) is a type of firewall that operates at the session layer (Layer 5) of the OSI model. Unlike stateful firewalls or application layer gateways that inspect and filter packets at higher layers, circuit-level gateways focus on controlling sessions and connections at a more basic level. The primary function of a circuit-level gateway is to determine whether a given communication session is allowed based on network-level information.
Example : Microsoft Forefront Threat Management Gateway (TMG)

Benefits of Circuit-level gateway

- Simple and inexpensive
- A single form of protection is insufficient
- Setup and management are simple

6. Cloud firewall

A cloud firewall is a network security solution that is specifically designed to protect cloud-based resources and applications. It serves as a barrier between an organization's infrastructure hosted in the cloud and external threats, such as unauthorized access, malicious attacks, and data breaches. Cloud firewalls provide security for virtualized environments and are often an integral part of cloud security strategies.
Example: AWS WAF, Azure Firewall, Google Cloud Armor , Cloudflare Firewall

Benefits of Cloud firewall

- Unified security policy
- Flexible deployment
- Simplified deployment and maintenance
- Improved scalability
- Automatic updates

7. Next-Generation Firewall (NGFW)

The most common type of firewall available today is the Next-Generation Firewall (NGFW), which provides higher security levels than packet-filtering and stateful inspection firewalls. An NGFW is a deep-packet inspection firewall with additional features such as application awareness and control, integrated intrusion prevention, advanced visibility of their network, and cloud-delivered threat intelligence. This type of firewall is typically defined as a security device that combines the features and functionalities of multiple firewalls.
Example: Palo Alto NGFW , Cisco Firepower NGFW, Fortinet FortiGate.

Benefits of Next-Generation Firewall

- Block malware
- Recognizing Advanced Persistent Threats (APTs)
- Financially beneficial

Feature	Packet Filtering Firewall	Stateful Inspection Firewall	Proxy (Application Layer) Firewall	Circuit-Level Gateway Firewall	Next-Generation Firewall (NGFW)	Cloud Firewall
Layer of Operation	Network/ Transport	Network/ Transport	Application	Session	Network/ Transport/ Application	Network/ Transport
Decision Basis	IP addresses, ports,	Context of connections	Application content	Session state	Application awareness	IP addresses, ports, protocols
protocols				User identity awareness		
Granularity of Control	Low	Medium	High	Low	High	Medium to High
Functionality	Filtering at packet level	Filtering and context-aware	Application-level filtering	Session-level filtering	Advanced threat protection	Cloud resource protection
Examples	iptables, pfSense	Cisco ASA, Check Point	Squid Proxy Server	Microsoft Forefront TMG	Palo Alto Networks, Cisco Firepower	AWS WAF, Azure Firewall, GCP Cloud Armor

Parul®
University

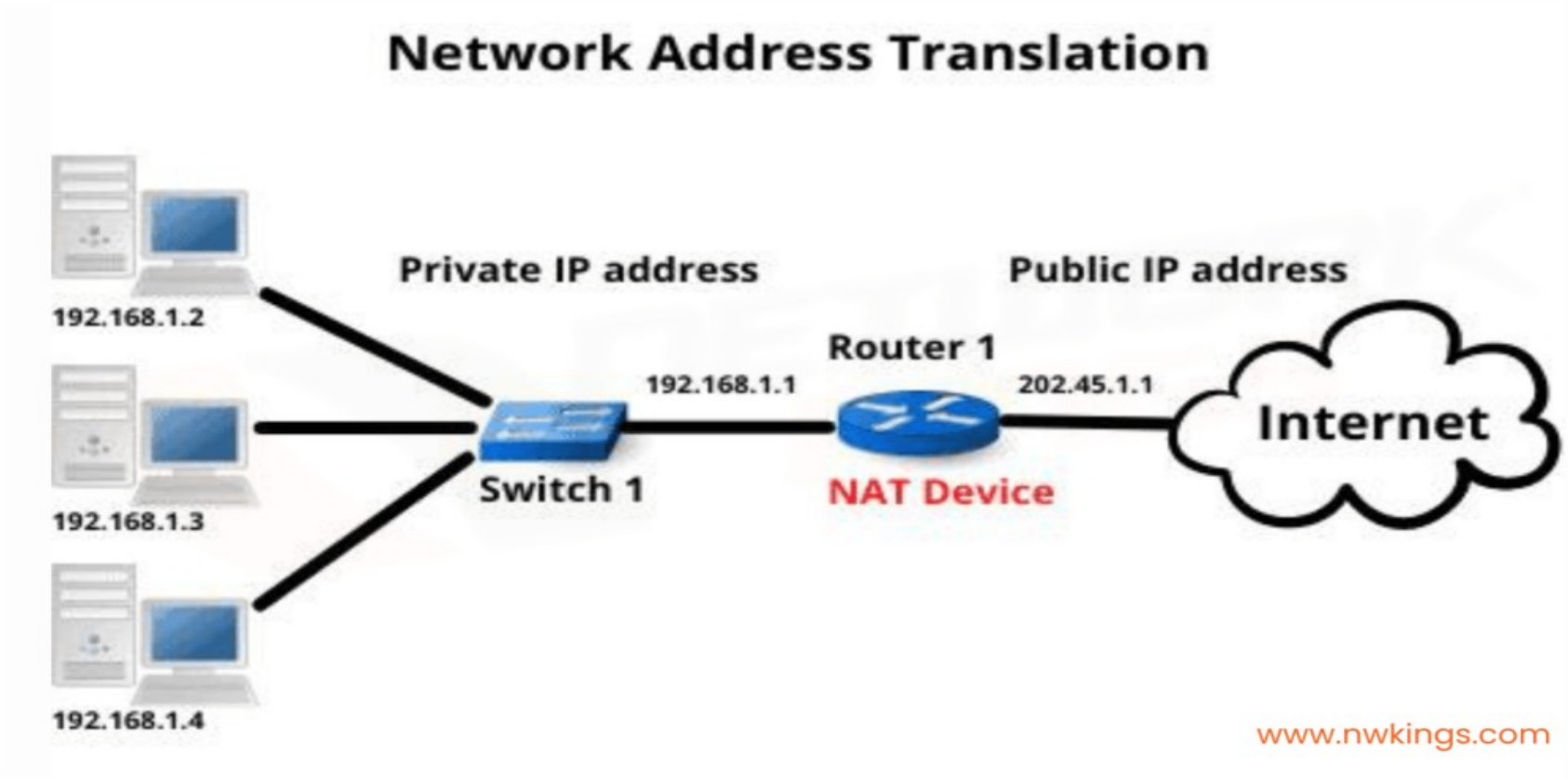
DIGITAL LEARNING CONTENT

Network Address Translation (NAT)

Definition

NAT stands for Network Address Translation, is a technology used in computer networking to enable multiple devices within a local network to share a single public IP (Internet Protocol) address when connecting to the internet. This is particularly useful due to the limited availability of IPv4 addresses.

Contd..


Network Address Translation
Private IP address
Public IP address
192.168.1.2
192.168.1.3
192.168.1.4
Switch 1
192.168.1.1
Router 1
NAT Device
202.45.1.1
Internet
www.nwkings.com

Working of NAT

Local Network: In a typical home or office network, multiple devices (such as computers, smartphones, or other networked devices) share a private IP address range, like those defined in the RFC 1918 standards (e.g., 192.168.x.x).

Public IP Address: The router or gateway device that connects the local network to the internet has a public IP address, which is unique and routable on the internet. However, this public IP address is limited in number, and there aren't enough of them to assign a unique public IP to every device in every local network.

Contd..

Translation: When a device within the local network wants to communicate with a server on the internet, NAT translates the private IP address of the device into the public IP address of the router. It also assigns a unique port number to each communication session.

Maintaining State: The NAT device keeps track of the translation in a NAT table, which maintains a mapping between private and public IP addresses and port numbers. This allows incoming packets from the internet to be correctly directed to the appropriate device within the local network.

Modes of NAT (Static NAT)

Static NAT: it involves mapping a private IP address to a specific public IP address on a one-to-one basis. This creates a permanent association between a private and public IP address.

Example:

Private IP: 192.168.1.10

Public IP: 203.0.113.5

Static NAT mapping: 192.168.1.10 (private) -> 203.0.113.5 (public)

Use: Static NAT is often used when a server inside a private network needs to be accessible from the internet, such as a web server or an FTP server.

Modes of NAT (Dynamic NAT)

Dynamic NAT: it assigns public IP addresses from a pool to private IP addresses on a first-come, first-serve basis. The mapping is temporary and depends on the availability of public IP addresses in the pool.

Example:

Private IP range: 192.168.1.0/24

Public IP pool: 203.0.113.1 to 203.0.113.10

Dynamic NAT mapping: Private IP 192.168.1.15 -> Public IP 203.0.113.3

Use: Dynamic NAT is suitable for scenarios where multiple devices in a private network need occasional access to the internet but do not require a permanent public IP address.

Modes of NAT (Port Address Translation)

PAT (Port Address Translation) or NAT Overload: PAT maps multiple private IP addresses to a single public IP address using different port numbers for each connection. This allows many devices to share the same public IP address simultaneously.

Example:

Private IP 1: 192.168.1.100

Private IP 2: 192.168.1.101

Public IP: 203.0.113.2

PAT mapping: Private IP 1 -> 203.0.113.2:5001, Private IP 2 -> 203.0.113.2:5002

Use Case: PAT is commonly used in home or small office networks where multiple devices share a single public IP address to access the internet simultaneously.

Parul®
University

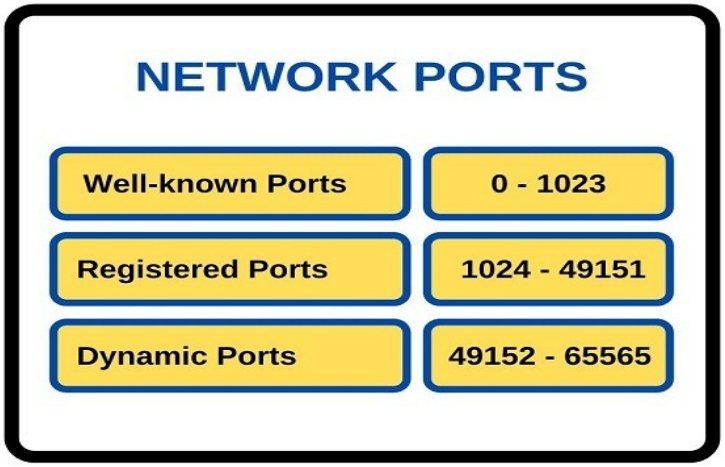
DIGITAL LEARNING CONTENT

Port Forwarding

Parul® University

What is Port?

In computer networking, ports are virtual endpoints for communication. They allow different services or applications on a single device to share the network connection. Ports are identified by numbers ranging from 0 to 65535



Port-No.	Service/Protocol
20/21	FTP - File Transfer Protocol. Transmission of files between the network participants
23	Telnet – Terminal access to distant system
25	SMTP – Simple Mail Transfer Protocol Sending of electronic mail
80	HTTP – Hypertext Transfer Protocol Transmission of HTML-files
443	HTTPS – HTTP over Secure Socket Layer

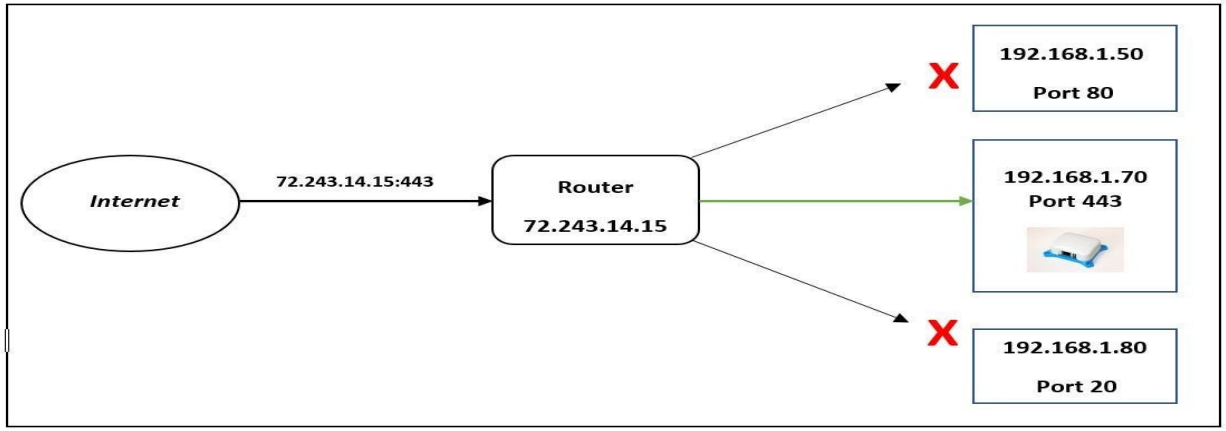
Port Forwarding Definition

Port forwarding allows you to make services or applications hosted on devices within a private network accessible from the internet. By configuring port forwarding rules on your router, you can selectively redirect incoming traffic to specific devices and ports, enabling external access to services like web servers, game servers, FTP servers, and more.

Port forwarding allows the router to redirect specific incoming traffic to a designated device on the private network.

Contd..

Example: Suppose you have a web server running on a computer within your home network, and you want to make it accessible from the internet. By default, incoming traffic on port 80 (HTTP) is blocked by your router's firewall. To allow external users to access your web server, you configure your router to forward incoming traffic on port 80 to the internal IP address of your web server.



Applications of Port Forwarding

Web Servers: Port forwarding allows hosting websites from home or office networks by redirecting incoming HTTP (port 80) or HTTPS (port 443) traffic to the web server.

Remote Desktop Access: Port forwarding facilitates accessing computers remotely by redirecting Remote Desktop Protocol (RDP) traffic (port 3389) to the target machine.

Gaming Servers: Hosting game servers for multiplayer gaming requires port forwarding to direct incoming game traffic to the hosting computer.

Contd..

File Transfer: Port forwarding enables secure file transfer by redirecting FTP (port 21) or Secure FTP (SFTP - port 22) traffic to a designated server.

Video Streaming: Services like media servers or IP cameras can be accessed remotely through port forwarding, allowing users to view live video streams.

Parul®
University

DIGITAL LEARNING CONTENT

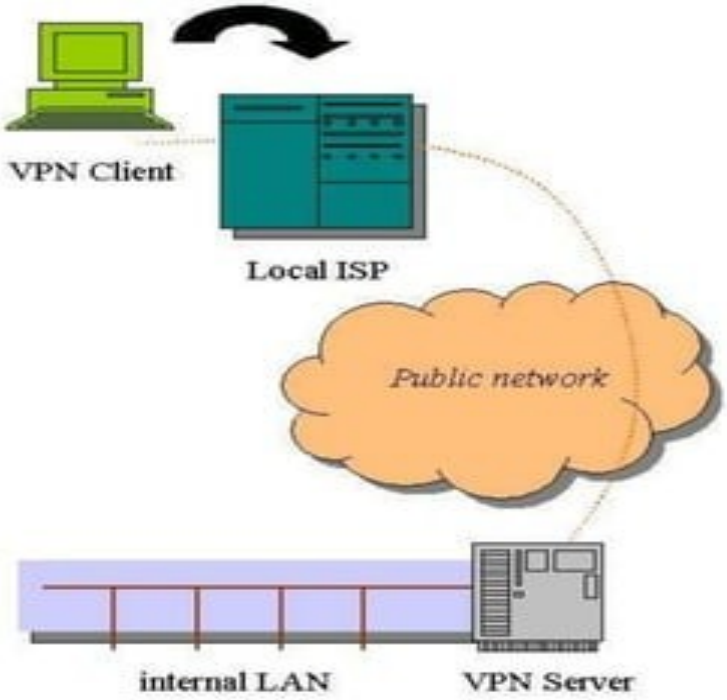
Virtual Private Networks

Content

- What is VPN
- Types of VPN's
- How does it work?
- Protocols
- Security: Firewalls
- VPN Devices
- Advantages
- Disadvantages
- Features
- Future
- Conclusion

What is VPN

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.
- Became popular as more employees worked in remote locations.
- Terminologies to understand how VPNs work.



Types of VPN's

- Remote-Access VPN
- Site-to-Site VPN (**Intranet-based**)
- Site-to-Site VPN (**Extranet-based**)

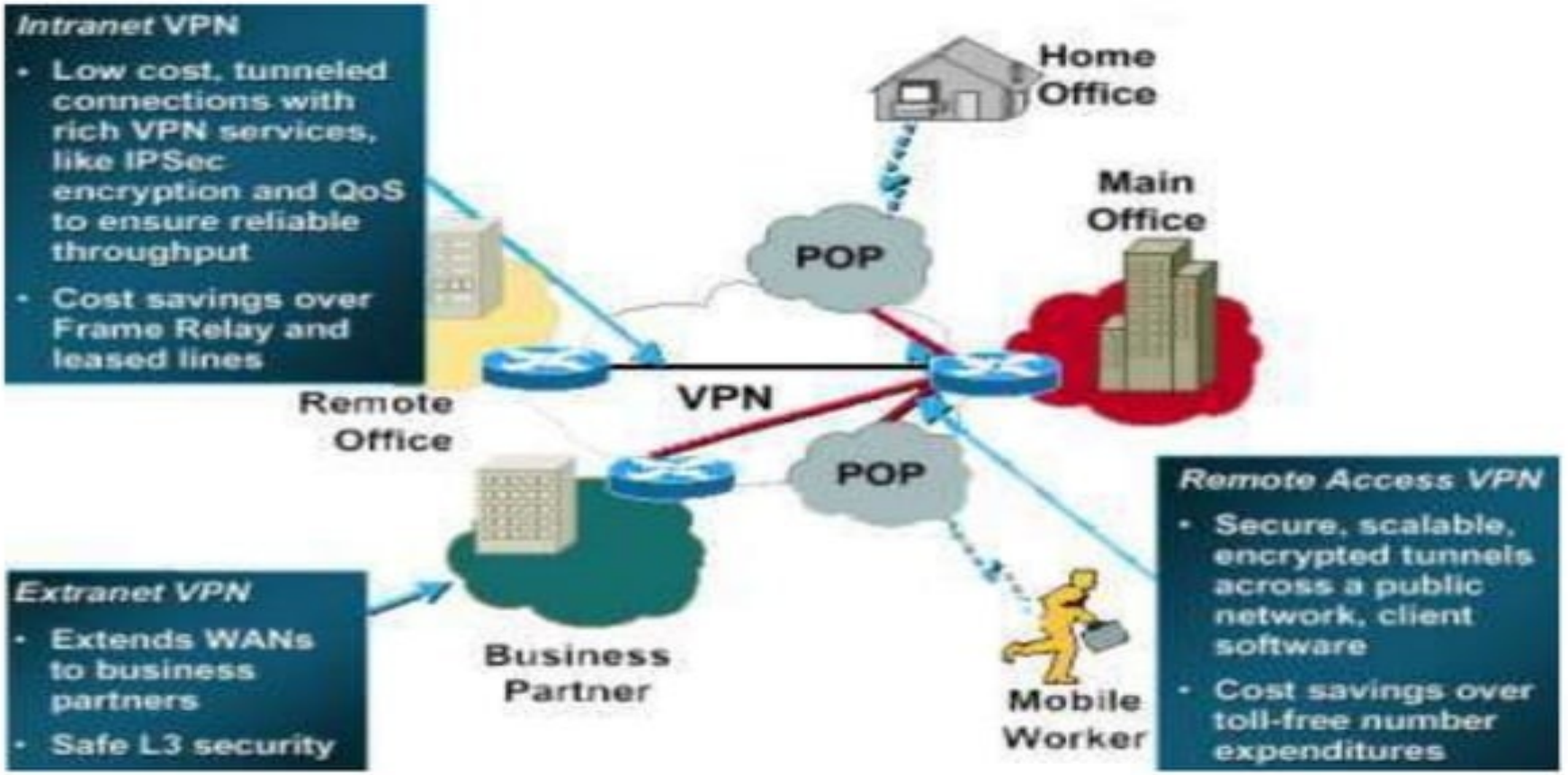
Remote-Access VPN

- A remote access VPN is for home or travelling users who need to access their central LAN from a remote location.
- They dial their ISP and connect over the internet to the LAN.
- This is made possible by installing a client software program on the remote user's laptop or PC that deals with the encryption and decryption of the VPN traffic between itself and the VPN gateway on the central LAN.

Site-to-Site VPN

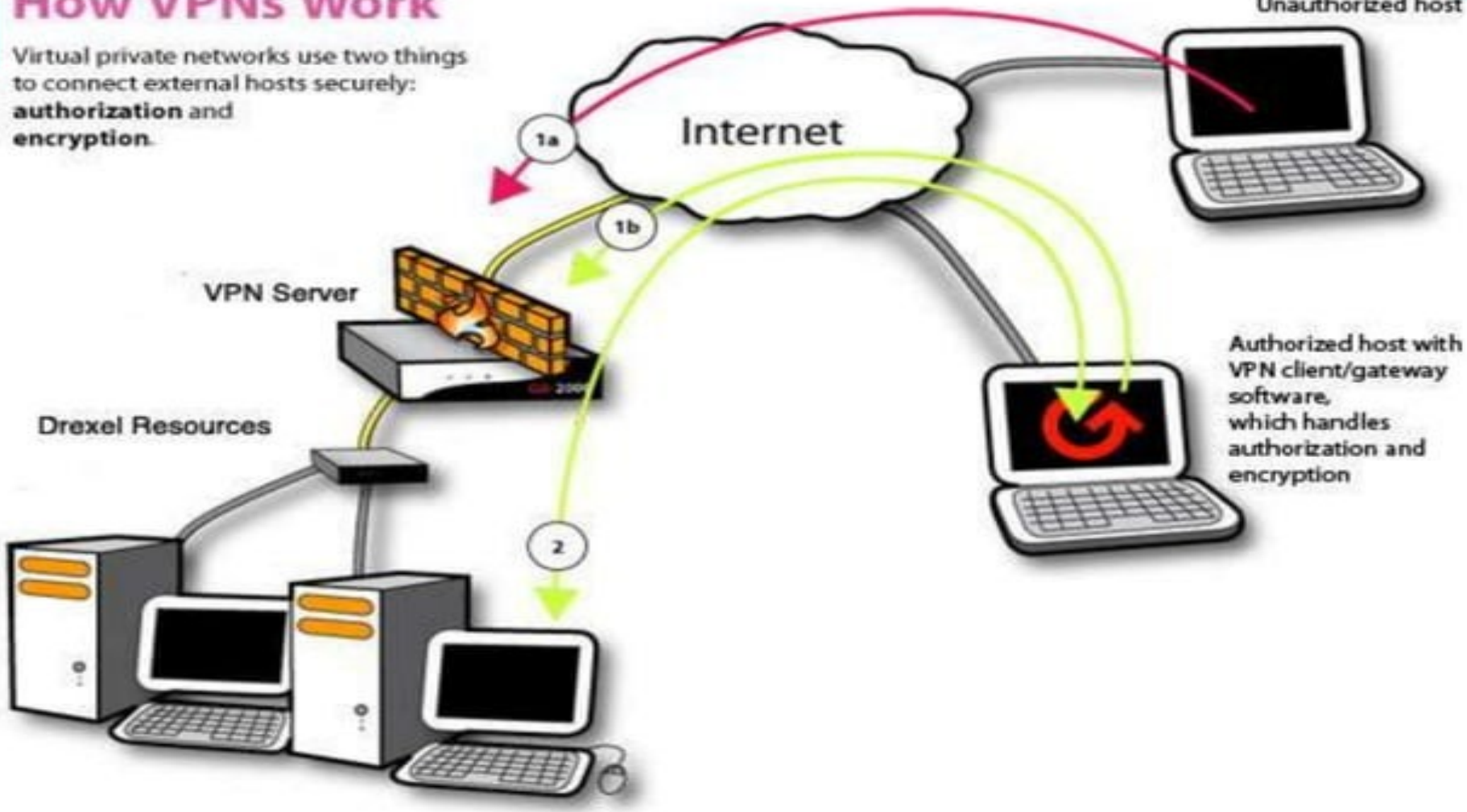
- **Intranet-based** - If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect LAN to LAN.
- **Extranet-based** - When a company has a close relationship with another company (for example, a partner, supplier or customer), they can build an extranet VPN that connects LAN to LAN, and that allows all of the various companies to work in a shared environment.

All 3 types of VPN



How VPNs Work

Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**.



Protocols used in VPN

- PPTP - Point-to-point tunneling protocol
- L2Tp – Layers to Tunneling Protocol
- IPSec - Internet protocol security
- SSL – is not used as much as the ones above.
- Encryption

VPN Security: Firewall

A well-designed VPN uses several methods for keeping your connection and data secure:

- **Firewalls**
- **Encryption**
- **IPSec**
- **AAA Server**

- You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through.

VPN Devices

- Hardware
- Firewall
- Software

VPN Advantages

- Multiple telephone lines and banks of modems at the central site are not required.
- A reduction in the overall telecommunication infrastructure – as the ISP provides the bulk of the network.
- Reduced cost of management, maintenance of equipment and technical support.
- Simplifies network topology by eliminating modem pools and a private network infrastructure.
- VPN functionality is already present in some IT equipment.

VPN Disadvantage

- If the ISP or Internet connection is down, so is the VPN.
- The central site must have a permanent internet connection so that remote clients and other sites can connect at anytime.
- VPNs may provide each user with less bandwidth than a dedicated line solution.
- Existing firewalls, proxies, routers and hubs may not support VPN transmissions.

VPN Features

- **Security** – tunneling support between sites with at least 128bit encryption of the data.
- **Scalability** – extra users and bandwidth can be added easily to adapt to new requirements.
- **Services** – quality of service features, including bandwidth, management and traffic shaping, are important to avoid congestion.
- **Management** – reports on user activity, management of user policies and monitoring of the VPN as a whole.

Future of VPN

- VPN popularity
  - Companies choosing VPN
  - Cost efficient?
  - New way of communicating?

Conclusion

- As we have gone through all possible details we conclude that VPN is the best option for the corporate networking.
- As many companies need to have access to Internet and hence security is also the main concern.
- VPN provides best possible combination of security and private network capabilities with adequate cost – saving to the companies who are presently working with leased lines.

Parul® University

DIGITAL LEARNING CONTENT

SNORT: INTRUSION DETECTION SYSTEM

- **SNORT** is a network based intrusion detection system which is written in C programming language. It was developed in 1998 by Martin Roesch. Now it is developed by Cisco. It is free open-source software.
- Snort is a network monitoring tool that watches traffic for signs of malicious activity (e.g., buffer overflows being executed against a service, command and control traffic from malware), suspicious activity (e.g., port scans and service enumeration) etc.
- Snort is a robust IDS that runs on Unix-based and Windows systems. It is also completely free.
- It is an open source intrusion prevention system capable of realtime traffic analysis and packet logging.

Parul®
University

DIGITAL LEARNING CONTENT

SNORT

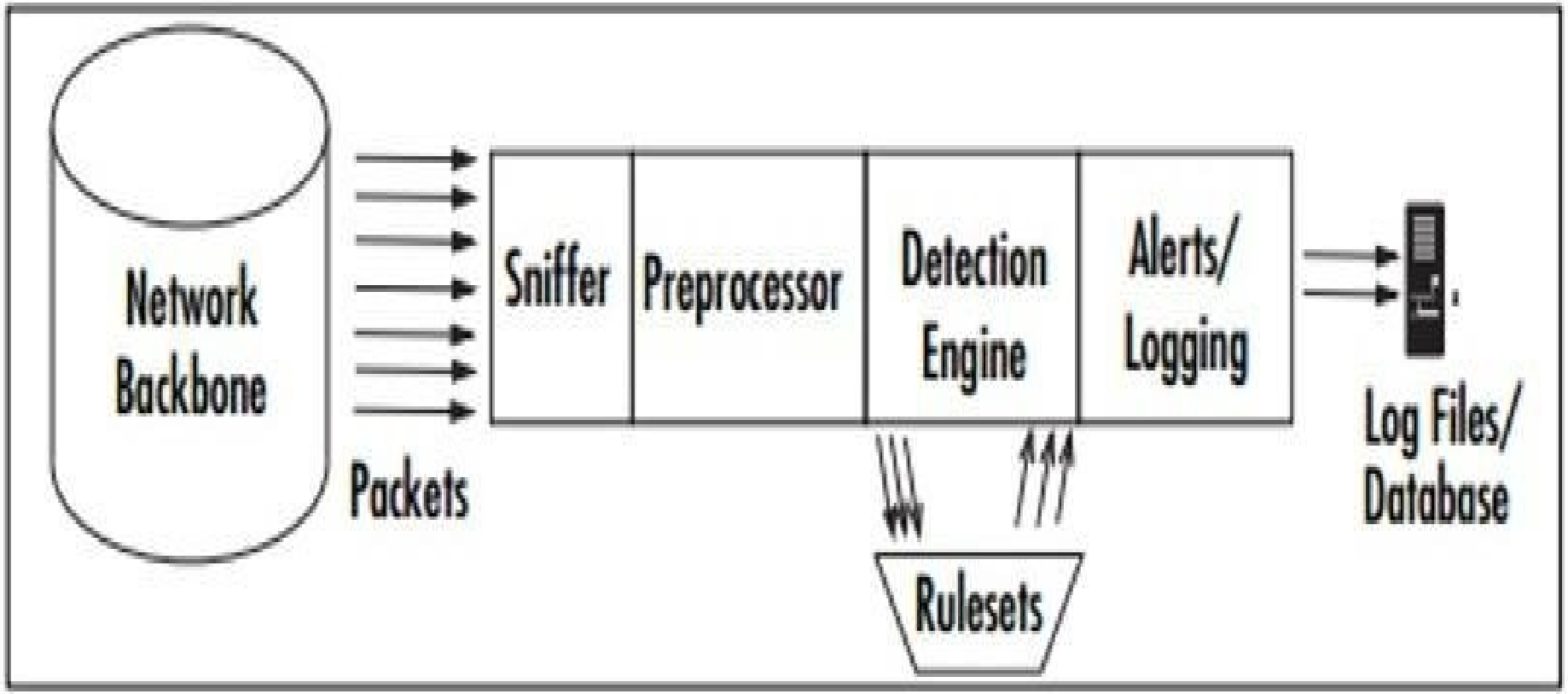
- snort is based on libpcap(for library packet capture), a tool that is widely used in TCP/IP traffic sniffers and analyzers
- Through protocol analysis and content searching and matching , snort detects attacks methods including denial of services, buffer overflow, CGI attacks, stealth port scans, and SMB probes. When suspicious behaviour is detected, snort sends a real-time alert to syslog, a separate 'alerts' file, or to a pop-up windows.
- A rule may be used to generate an alert message, log a message, or in terms of snort, pass the data packets drop it silently
- The word pass here is not equivalent to the traditional meaning of pass as used in firewalls and routers. In firewalls and routers, pass and drop are opposite to each other.

Parul®
University

SNORT

- Snort rules are written in an easy to understand syntax. Most of the rules are written in a single line. However you can also extend rules to multiple lines by using a backslash character at the end of lines.
- Rules are usually placed in configuration files, typically snort.conf.you can also use multiple files by including them in a main configuration file.
- A rule may be used to generate an alert message, log a message, or, in terms of snort , pass the data the packet ,i.e drop silently

SNORT


Network Backbone
Packets
Sniffer
Preprocessor
Detection Engine
Alerts/ Logging
Log Files/ Database
Rulesets

Parul®
University

Snort modes

- **Sniffer**:- Simply reads the packets off of the network and displays them for you in a continuous stream on the console (screen).
- **Packet logger**:- Logs the packets to disk.
- **Network intrusion detection**:- Performs detection and analysis on network traffic. This is the most complex and configurable mode.

Parul®
University

Exploring Snort.conf

- In the Snort source directory, there are 2 subdirectories of interest: etc and rules. The actual snort.conf file lives in etc.
- The first part of the snort.conf file lets you set some important global variables, indicating such things as your home subnet, your web servers, and your rule locations.
- The second part of the file lets us configure pre-processors. The pre-processors handle such things as fragmented packets, port scan detection, and stream reassembly.

Parul®
University

Snort Rules

- Snort has several types of rules that affect how it handles traffic:
- **Alert rules** - Log packets whose characteristics match a predefined suspicious pattern (e.g., generated by a common hacking tool, or contain a string indicative of a buffer overflow or web attack) or custom rules that monitor packets you determine to be prohibited or undesirable on your network (e.g., file sharing, gaming, etc.).
- **Pass rules** - Explicitly ignore packets. Traffic that matches these rules will not be logged.
- **Log rules** - Record packets but do not generate rules. This would be useful for diagnosing network problems, storing traffic for audits, or monitoring sensitive systems so that traffic can be analyzed in case a compromise is detected.

Parul®
University

Snort rules…

- **Activate rules -** Generate an alert for traffic that matches this rule's trigger, then activate a subsequent dynamic rule. (Until it is activated, a dynamic rule will not generate an alert even if traffic matches it.)
- **Dynamic rules -** Triggered by activate rules. This enables you to chain rules together in a way that makes inspection more efficient (don't run rules needlessly) and more effective (create complex chains). These are great mechanisms for gathering more information during an attack.

Parul®
University

snort Rules Syntax

- Snort comes with a standard ruleset that checks for activity such as Nmap stealth scans, vulnerability exploits, attempted buffer overflows, anonymous FTP access etc.
- By default, Snort checks the packet against alert rules first, followed by pass rules, and then log rules.
- Basic Snort rules consist of two parts: the header and the options.
- The first part of the header tells Snort what type of rule it is (such as alert, log, pass).
- The rest of the header indicates the protocol (ip, udp, icmp, or tcp), a directional operator (either -> to specify source to destination or <> to specify bidirectional), and the source and destination IP address and port.

testing rule (to check)

- **Rule:-**
  - **Alert ip any any → any any (msg;ip"ip packet detected';)**
- This is the worst rule ever written, but it does a very good job of testing if snort is working well and is able to generate alerts.
- You can use this rule at the end of the snort.conf file the first time you install snort. The rule will generate an alert message for every captured IP packet.
- This rule is bad because it does not convey any information. This should be your first test to make sure that snort is installed properly.

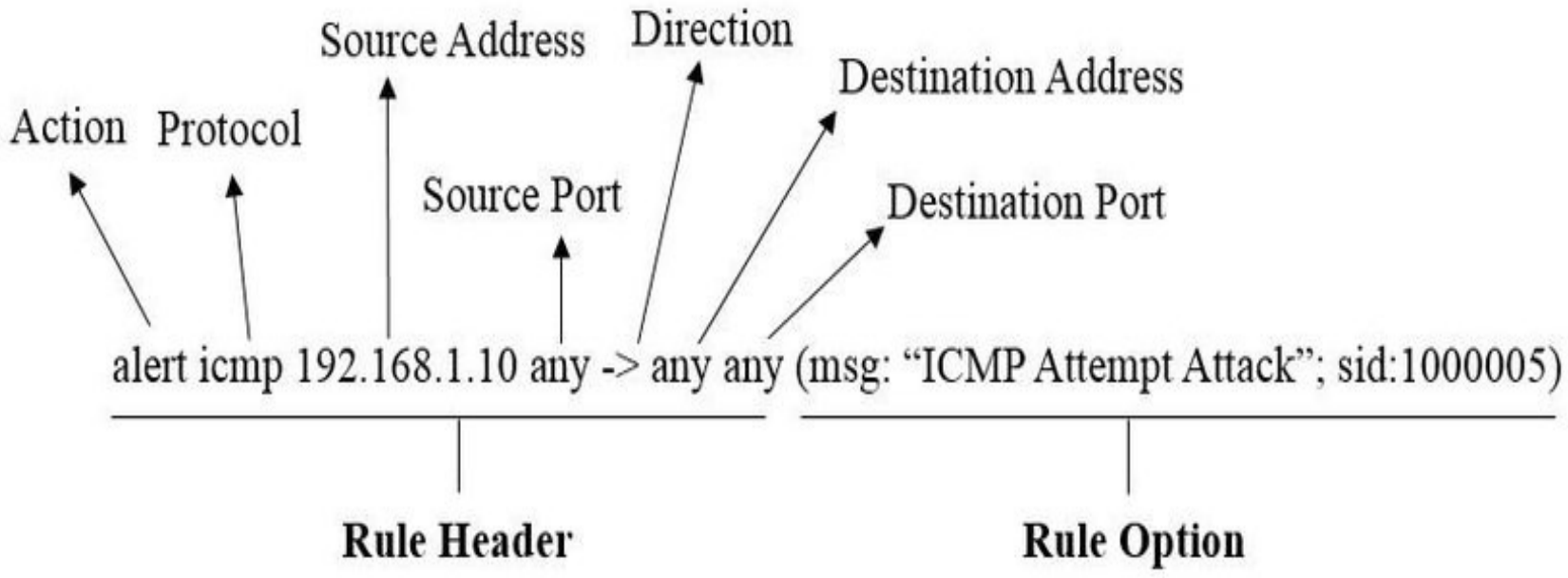
Parul®
University

DIGITAL LEARNING CONTENT

Structure of a rule

- All snort rules have two logical parts: rule header and rule options.
- The rule header contains information about what action a rule takes. It also contains criteria for matching a rule against data packets.
- The rule options part usually contains an alert message and information about which part of the packets should be used to generate the alert message.
- The options part contains additional criteria for matching a rule against data packets.
- A rule may detect one type or multiple types of intrusion activity

Snort rule (Structure of a snort rule)



Snort Plug-ins

- **Pre-processors :-** Pre-processors are set up in the snort.conf file using the pre-processor command. They operate on packets after they've been received and decoded by Snort but before it starts trying to match rules.
- **Output Modules:-**Output modules are also set up in the snort.conf file using the output command, which controls how, where, and in what format Snort stores the data it receives. Any rule types we define can be specified to use a particular kind of output plug-in

Basic usage

- **Packet Sniffing:** The way traffic is being transmitted can be thoroughly examined by gathering the individual packets that travel to and from devices on the network.
- **Generates Alerts:** It generates warnings based on the configuration file's rules when it discovers unusual or malicious activity, the possibility of a vulnerability being exploited, or a network threat that compromises the organization's security policy.
- **Debug Traffic:** After the traffic has been logged, any malicious packets and configuration problems are checked.

features

- Real-time traffic monitor
- Packet logging
- Analysis of protocol
- Content matching
- OS fingerprinting
- Can be installed in any network environment.
- Creates logs
- Open Source
- Rules are easy to implement

DIGITAL LEARNING CONTENT

Parul® University

www.paruluniversity.ac.in