GuiNet Technologies

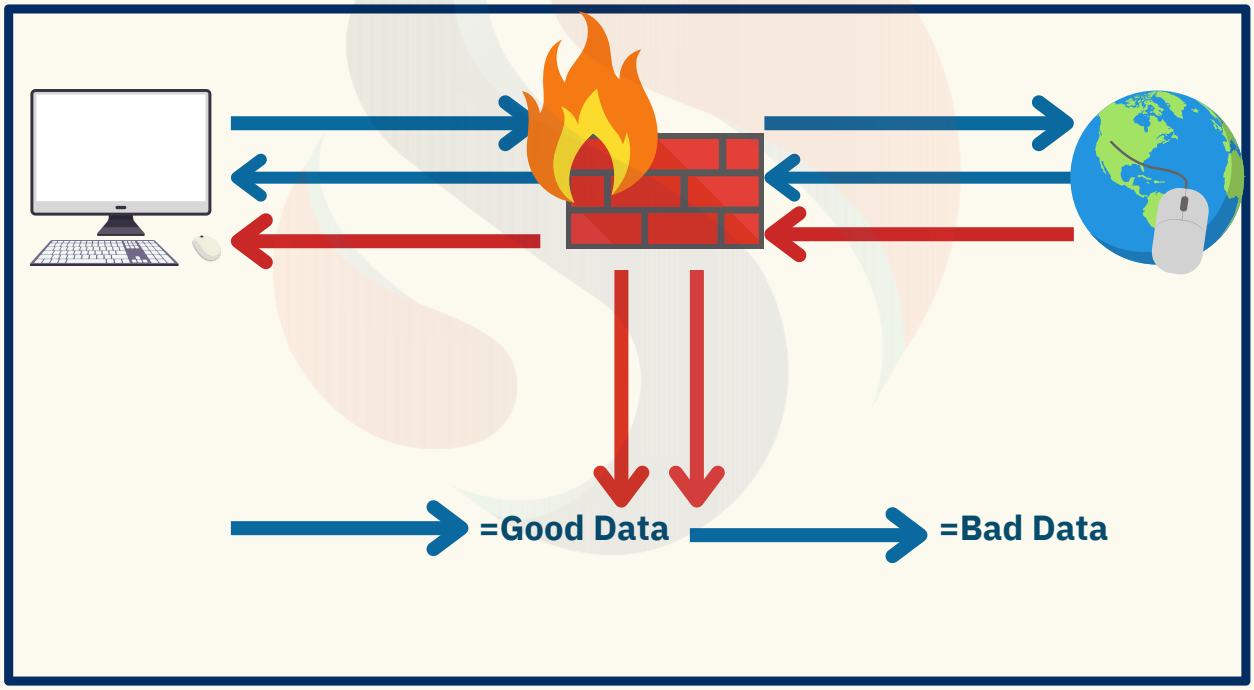
Firewall Technologies

Beyond the Firewall: A Security Deep Dive and Essential Guide to Modern Firewall Architectures & Deployment

www.guinett.com

Firewall Technologies

- The word firewall commonly describes a system or device or Software.
- Firewall is placed between a trusted network and an untrusted network.
- A firewall is security devices used to stop or mitigate unauthorized access.
- The only traffic allowed on the network is defined via the firewall policies.
- It grants or rejects access to traffic flows between untrusted & trusted zone.
- A firewall monitors and check incoming and outgoing network related traffic.
- It decides to allow or block specific traffic based on defined set of security rules.
- A firewall can be hardware, software, or both or can be Cloud-based or Virtual.
- The first generation of firewall technology consisted of packet filters techniques.
- The second generation of firewall started with application layers technologies.
- The third generation of firewall had “Stateful” filters inspection also called NGFW.
- Firewalls are relied upon to secure home and corporate networks from any attacks.

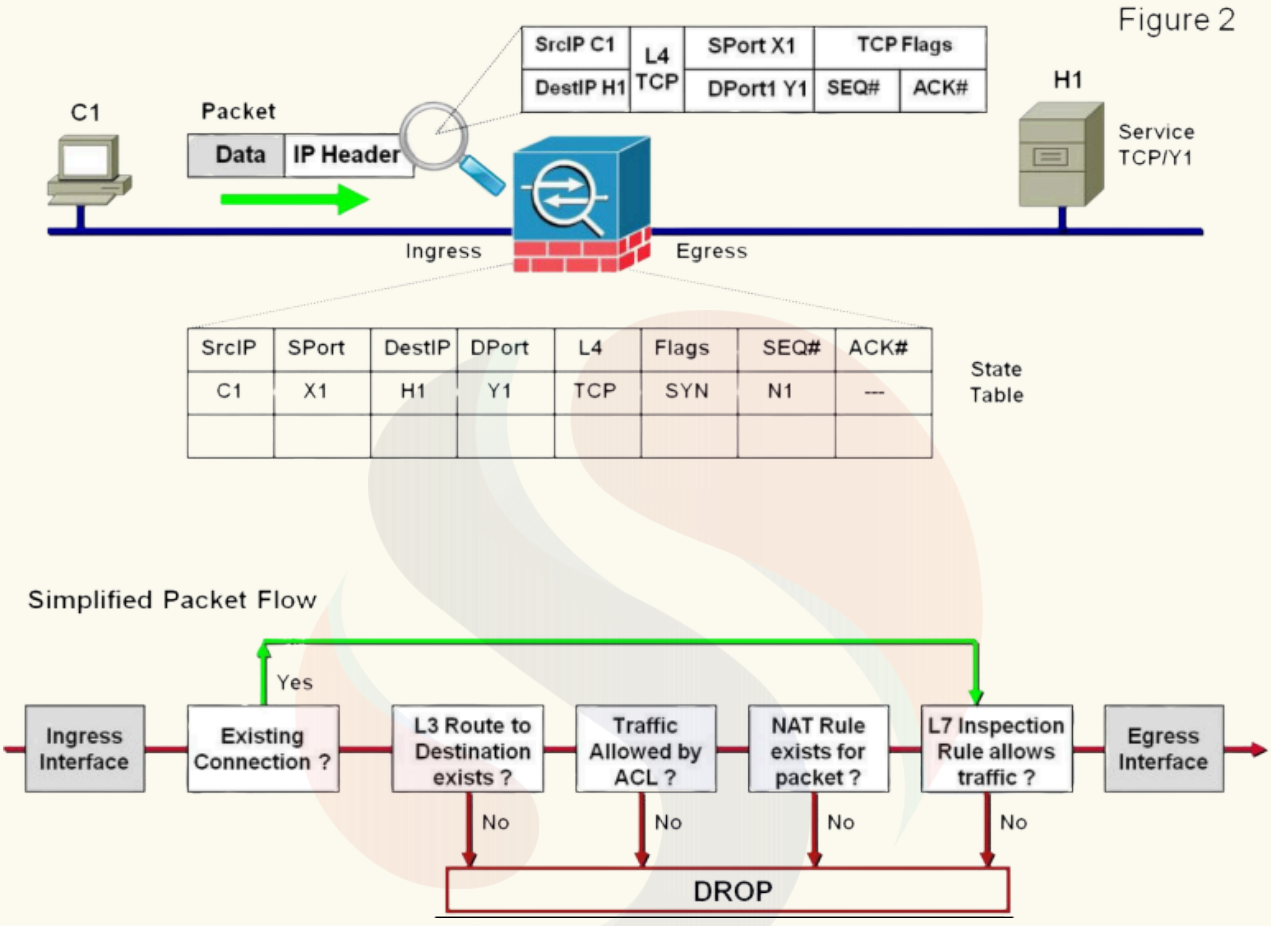


SONICWALL
WatchGuard
paloalto NETWORKS
FORTINET
Juniper NETWORKS
STONESOFT Real World Business Security
CISCO
Check Point SOFTWARE TECHNOLOGIES LTD.

Stateful Firewall:

- It maintain the state of connection when packet is travelling for the appliance.
- State Full Firewall maintain the state of connection in the state table of Firewall.
- After adding information in state table, it forwards the packet to the destination.
- When it receive the reply-packet, it match the packet information to state-table.
- If Firewall receive the reply packet if match packet is accepted otherwise drop.

Figure 2

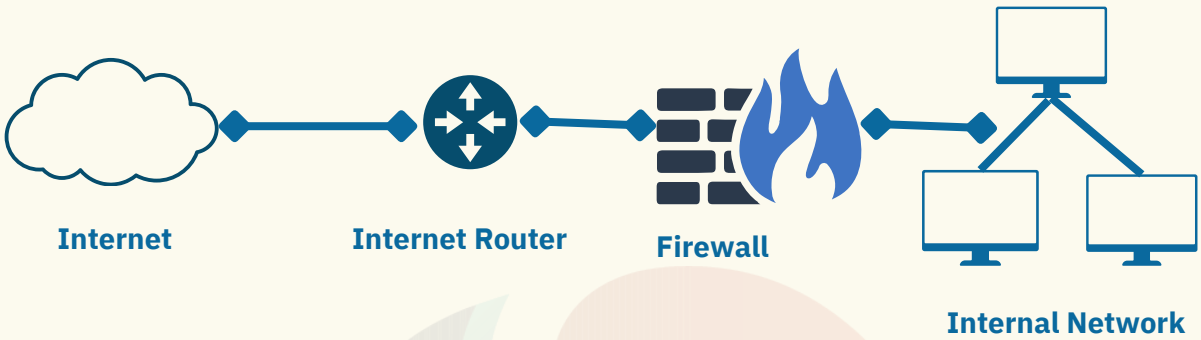


Stateless Firewalls:

- Stateless Firewalls watch network traffic and restrict or block the packets.
- This Firewalls restrict or block packet based on source & destination addresses.
- Stateless Firewalls also restrict or block packet based on other static values.
- Stateless Firewalls are not 'aware' of the traffic patterns or the data flows.
- A stateless firewall filter, also known as an Access Control List or (ACL).
- Stateless Firewall does not state fully inspect the traffic to keep the records.
- It evaluates packet contents statically and does not keep track of connection state.
- An example of a packet filtering firewall is the Extended ACL on Cisco Routers.

Packet Filtering Firewall:

- In Packet, filtering firewall packets are filtered using the Access-List (ACL).
- Packet Filtering Firewall is vulnerable to IP spoofing network attack easily.
- Cisco IOS use Standard or Extended ACL, Named ACL etc to filter the traffic.
- Limits info is allowed into a network based on the destination and source address.
- Packet Filtering Firewall can only be implemented on Network & Transport Layers.
- Packet Filtering Firewall filters packets based on address and port number only.

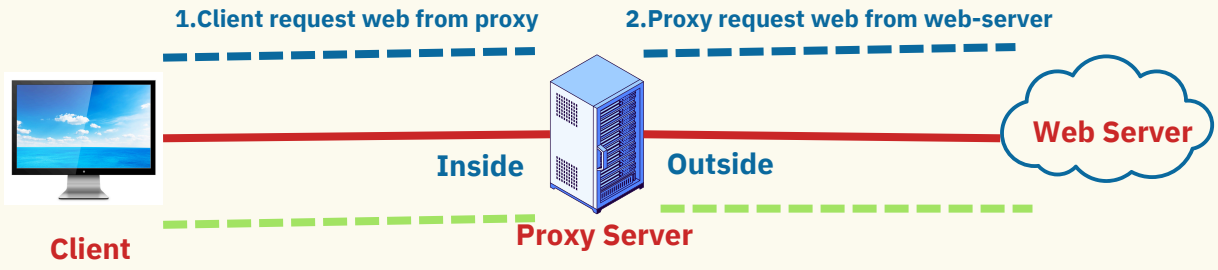


Injection Table

SRC IP	DST IP	DST Port	Protocol	Action
10.1.1.0/24	8.8.8.8	53	UDP	Allow
10.1.1.0/24	0.0.0.0/0	25	TCP	Allow
Deny Any				

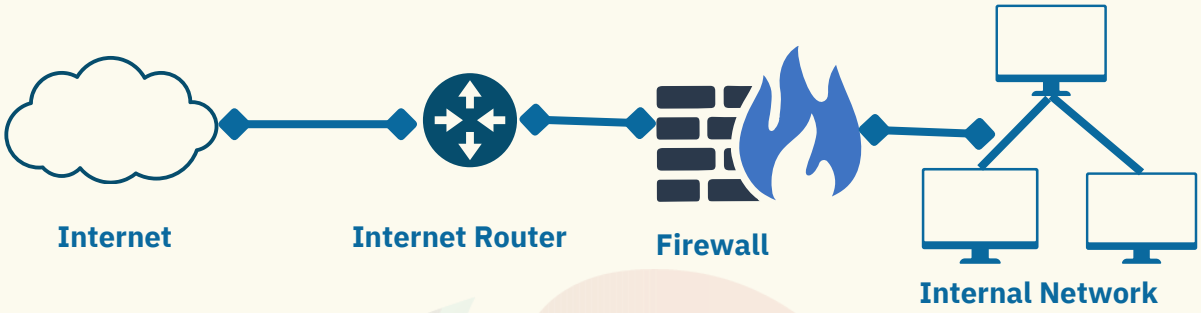
Proxy Firewall:

- Proxy Firewall works as a proxy for clients of Internal LAN users.
- No direct communication occurs between client & destination server.
- Takes requests from a client, puts that client on hold for a moment.
- Makes the requests as if it is its own request out to the final destination.
- Proxy Firewall is Memory and disk intensive at the proxy server or device.
- Proxy Firewall could potentially be a single point of failure in the network.



Application Firewall:

- Application level gateways works on the Application Layer of the OSI reference Model.
- Application Firewall you can block or control the traffic generated by any applications.
- Application Firewalls can also be configured as Caching Servers to increase performance.
- Application Level gateway Firewall is more processor intensive but have very tight control.
- Application Firewall is the ability to analyze traffic all the way up to the Application Layer



Injection Table

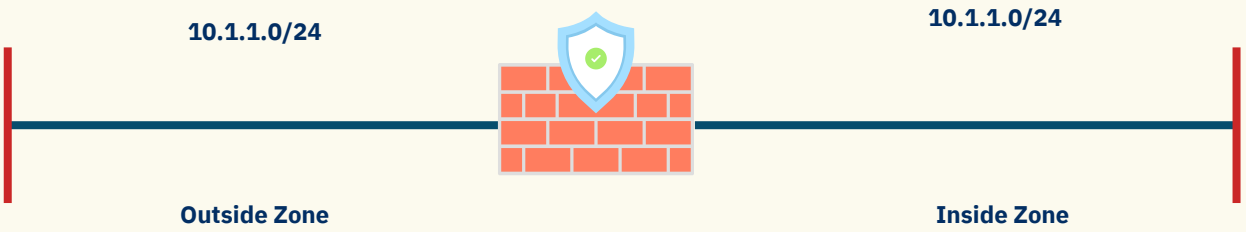
SRC IP	DST IP	DST Application	Protocol	Action
10.1.1.0/24	8.8.8.8	DNS	UDP	Allow
10.1.1.0/24	0.0.0.0/0	SMTP	TCP	Allow
Deny Any				

Personal Firewall

- Personal Firewall is typically software application that is installed on endpoint device.
- Personal Firewall protect the device itself from unauthorized intrusions or access.
- Most operating systems such as windows or Linux have integrated personal firewalls.
- Personal Firewalls protect a single host or device only in the network.
- Personal Firewalls control traffic arriving at and leaving individual hosts.
- Personal Firewalls have the ability to permit and deny traffic based on the application.
- Personal Firewalls have also the ability to define policies for different classes of network.

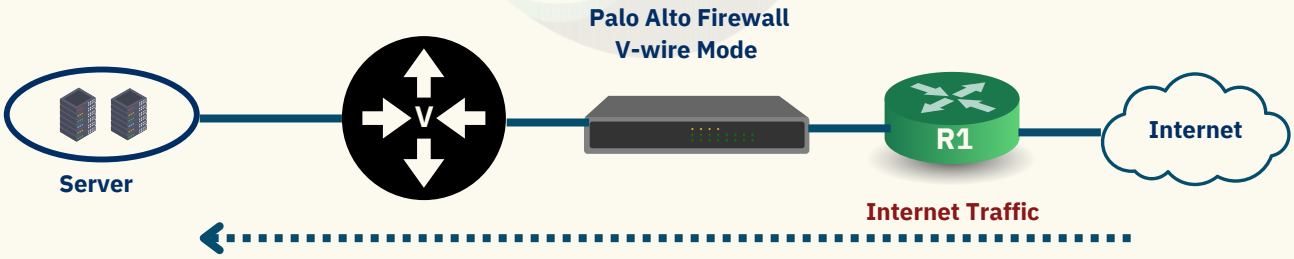
Transparent Firewall:

- It works at layer 2, or it forwards the frames based on destination MAC.
- It has the capabilities to filter the traffic from layer 2 to layer 7 of OSI Model.
- Transparent Firewall is invisible to devices on both sides of protected network.
- Transparent mode does not support dynamic routing protocols or more stuff.



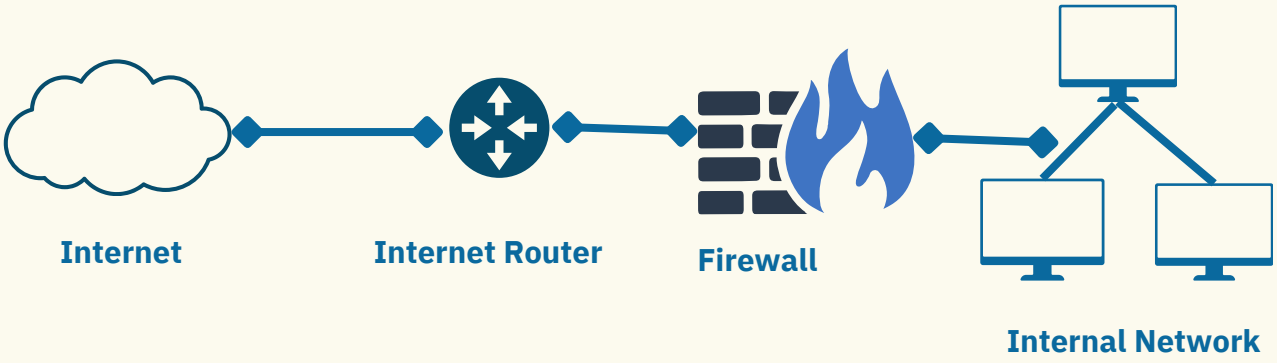
Virtual Wire Firewall:

- Virtual Wire Firewall mode logically binds two Ethernet interfaces together.
- Virtual Wire Firewall mode allowing for all traffic to pass between interfaces.
- Virtual Wire, also known V-Wire, deployment options use Virtual Wire interfaces.
- A virtual Wire Firewall mode requires no changes to adjacent network devices.
- A Virtual Wire interface supports App-ID, User-ID, Content-ID, NAT & decryption.
- Virtual Wire Firewall mode is typically used when no switching or routing is needed.



Traditional Network Firewall:

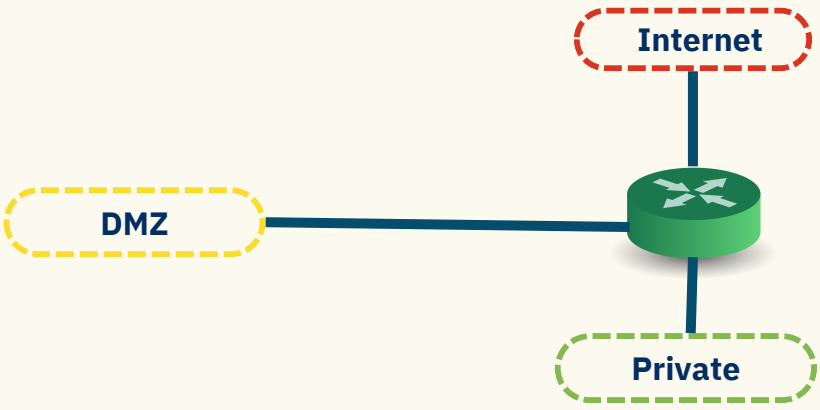
- Traditional firewalls work at the network & transport layer of OSI Model.
- Allow or block traffic based on criteria such as an IP address and/or port.



Injection Table				
SRC IP	DST IP	DST Port	Protocol	Action
10.1.1.0/24	8.8.8.8	53	UDP	Allow
10.1.1.0/24	0.0.0.0/0	25	TCP	Allow
Deny Any				

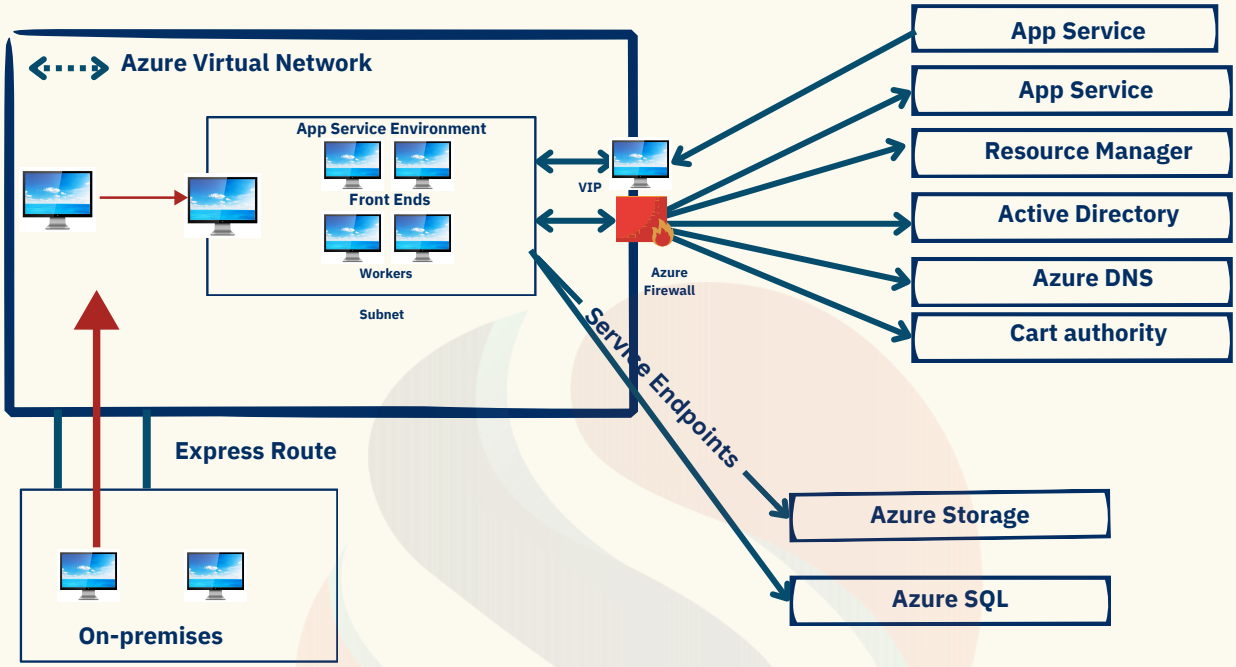
Zone-Based Firewall:

- Zone Based Firewall is the most advanced method of a Stateful Firewall.
- Zone Based Firewall is available on Cisco IOS Routers.
- The idea behind ZBF is that we do not assign access-lists to interfaces.
- In ZBF, different zones created & assigned Interfaces to different zones.
- In Zone Based Firewall security policies assigned to traffic between zones.



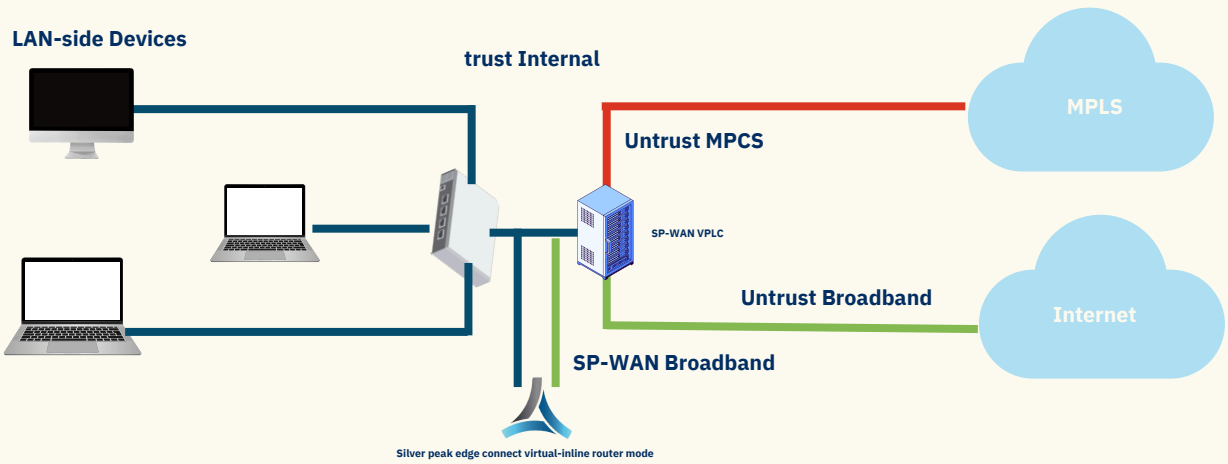
Could-Based Firewall:

- Cloud Firewalls are software-based, cloud deployed network devices.
- Cloud Firewalls built to stop or mitigate unwanted access to private networks.
- As Cloud Firewalls a new technology, they are designed for modern business needs.
- Cloud Firewalls are sit within online application environments to stop any attacks.
- Firewall-as-a-service (FWaaS), Security-as-a-service (SECaaS) are the examples.



Virtual Firewall:

- Virtual firewall is a firewall service or an application for virtualized environment.
- Virtual firewall provides packet filtering within a virtualized environment.
- Virtual firewalls are commonly used to protect virtualized environments only.
- Virtual firewall is often deployed as a software appliance in virtual environment.
- A virtual firewall manages and controls incoming and outgoing traffic.
- It works in conjunction with switches and servers similar to a physical firewall



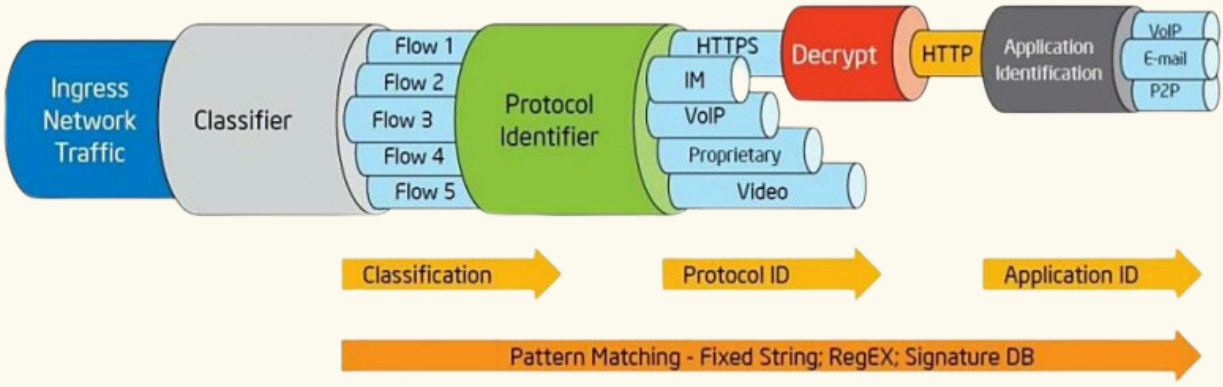
UTM Firewall:

- The term UTM firewall or simply UTM (Unified Threat Management) is the terminology.
- It is given to hardware or software device capable of assembling various security functions.
- Such as packet filtering, proxy, IDS & IPS, protection against malware, application control.
- UTM provides multiple security features & services in single device or service on network.
- UTM includes functions such as anti-virus, anti-spam, content filtering, & web filtering etc.
- UTM (Unified Threat Management) Firewall is not consider Next-Generation Firewall.

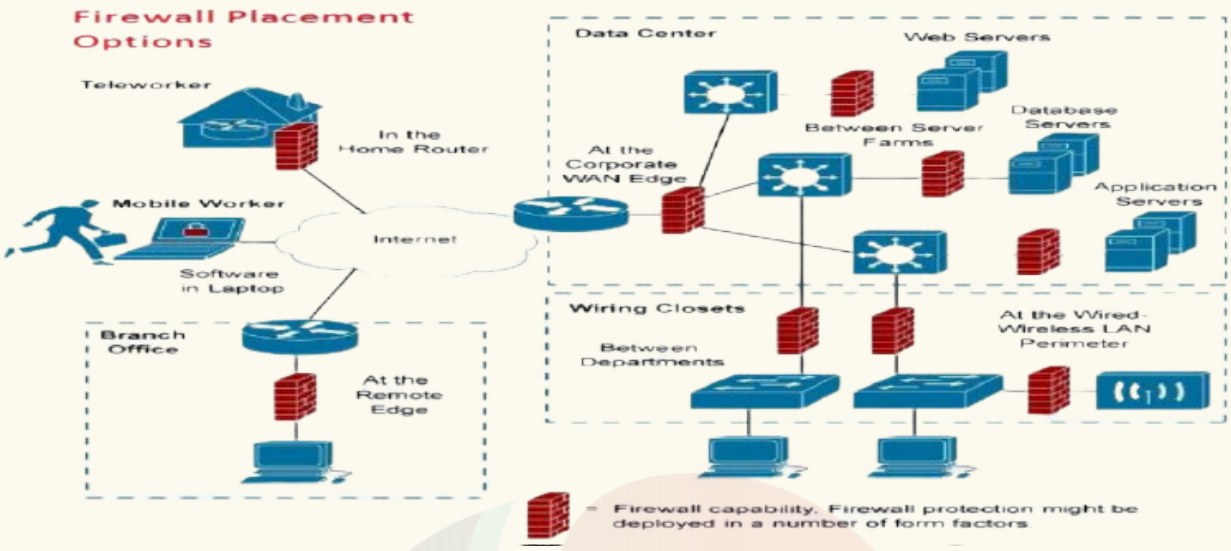
Next-Generation Firewall (NGFW):

- NGFW performs the role of a traditional firewall and adds NGIPS features.
- Next-Generation Firewall is part of the third generation of Firewall technology.
- All NGFWs offer two key features App Awareness & Control & ID Awareness.
- Next-Generation Firewall (NGFW) provide deep-packet inspection of traffic.
- Next-Generation Firewall add application-level inspection & Intrusion Prevention.
- Next-Generation Firewall provides all traditional IPS features with high performance.
- Next-Generation Firewall allow, and block traffic based on specific application as well.
- Next-Generation Firewall allow, and block traffic based on user information as well.
- Next-Generation Firewall (NGFW) provide both IPS and application control functions.
- There is no big difference between the UTM and Next-Generation Firewall (NGFW).
- Next-Generation Firewall provide high performance and Processing using to protect.

Deep packet Inspectionn



Basic firewall filtering is recommended at every trust boundary, externally and internally, throughout the enterprise network in data center, Perimeter or edge etc .



Innovating for a Smarter Future – GuiNet Technology!

Thank You

GuiNet Technologies

www.guinett.com

Mobile No: +91-9289682701, Email: info@guinett.com