paloalto NETWORKS

PALO-ALTO

BASIC TO ADVANCED

vishwajeet.it.net@outlook.com

ABOUT PALO-ALTO

Palo Alto Networks is a leading **cybersecurity company**, founded in **2005** by **Nir Zuk**, a well-known expert in network security.

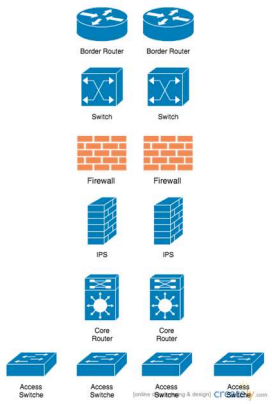
Next-generation firewalls (NGFWs), which are advanced security devices that can **identify and control over 1,900 applications**, not just ports and protocols like traditional firewalls.

Key Innovations:

- ✓ **App-ID™** – Identifies applications, regardless of port, protocol, or encryption.
- ✓ **User-ID™** – Connects network activity to specific users, not just IP addresses.
- ✓ **Content-ID™** – Scans content for threats like malware, viruses, and data leaks.

Global Presence:

- ✓ **12,500+ customers**
- ✓ Spread across **55+ countries**
- ✓ Offers **24/7 support** worldwide



Why the Firewall is Placed at the Trust Border:

The **gateway** or firewall is placed at the **boundary between trusted (internal) and untrusted (external) networks**. This is called the **"trust border"**.

- ✓ **Monitor all traffic** coming in and going out
- ✓ **Enforce security policies**, like blocking harmful applications or allowing only certain users access to specific resources

By seeing **everything at this boundary**, Palo Alto firewalls can make smart decisions about what to **allow**, **block**, or **inspect**.

But Today's Applications Have Changed...

In the past, firewalls could control traffic just based on:

- **Ports** (e.g., TCP 21 for FTP)
- **IP addresses**
- **Packets**

But now, that's not enough.

Modern applications can:

- **Use any port**
- **Hide inside encrypted traffic**
- **Mimic other apps to bypass security**
- **Move across different users and devices**

So instead of just looking at **port numbers** and **IP addresses**, *Palo Alto firewalls focus on:*

- **Applications** instead of ports
- **Users** instead of IPs
- **Content** instead of raw packets

The Problem with Traditional Firewalls (and Their Helpers)

Standard firewalls aren't enough to stop modern cyber threats. So, companies started adding **extra tools**, or "**firewall helpers**," to try to fill the gaps.

These "helpers" include:

- ✓ **IPS (Intrusion Prevention System)**
  – Detects and blocks attacks and harmful applications.
- ✓ **Proxy servers with or without Web Filters**
  – Controls which websites users can access, but only works well on standard ports like HTTP/HTTPS.
- ✓ **Network Anti-Virus (AV)**
  – Scans for and blocks malware (viruses, trojans, etc.).
- ✓ **QoS (Quality of Service)**
  – Helps prioritize important traffic like voice or video.

But There's a Catch…

Adding all these tools creates **complexity**:

- Each tool only sees **part of the traffic**, so no single tool has a full picture.
- It's **expensive** to buy and maintain all these separate systems.
- They don't work well together—**more tools = more problems**.
- Putting all of this into one device (like a traditional firewall) makes it **slow** and **inefficient**.

Just adding more tools doesn't fix the problem.
What's needed is a **single, smart security solution** that can:

- See everything
- Understand applications, users, and content
- Stop threats in real time

That's exactly what **Palo Alto Networks' next-gen firewall** is designed to do.

Next-Generation Firewall – Easy Breakdown

A **Next-Gen Firewall (NGFW)** is much **smarter** than old-style firewalls. It doesn't just block or allow traffic based on ports and IPs—it understands what's **actually happening in the traffic**.

✅ 1. Application Awareness & Full Visibility

- It sees **what applications** are being used (e.g., YouTube, Skype, Dropbox), even if they try to hide.
- This is done with a feature called **App-ID**, which can identify and control over **1,300+ applications**, not just ports.

✅ 2. Built-in Intrusion Prevention (IPS)

- Traditional firewalls need a separate IPS tool.
- Palo Alto includes **Content-ID**, which gives **full threat protection (IPS)** inside the firewall **without slowing it down**.
- It blocks malware, exploits, and malicious files in real time.

✅ 3. User Awareness (User-ID)

- It doesn't just see IP addresses—it knows **who the user is**.
- It connects to **Active Directory (AD)** to apply policies based on **users or groups**, like "only HR can access systems."

✅ 4. Standard Firewall Features Still Included

- It still does all the basics you expect from a firewall:
  - **Packet filtering**
  - **Stateful inspection**

- **NAT (Network Address Translation)**
- **VPNs** (IPsec and SSL)

✅ 5. Easy Deployment Options ("Bump in the Wire")

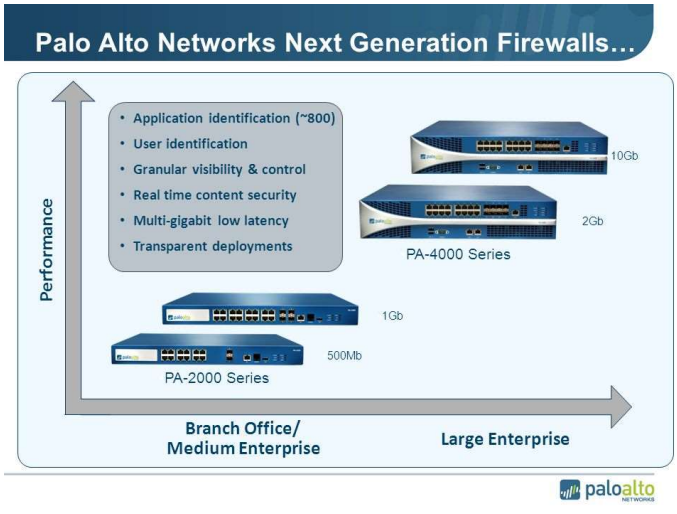
- Can be added to your network **without major changes**.
- Works in **transparent mode**, so it fits behind existing firewalls or routers—great for upgrading security without redesigning the whole network.

📌 In Short:

Palo Alto's Next-Gen Firewall is **a powerful all-in-one box** that:

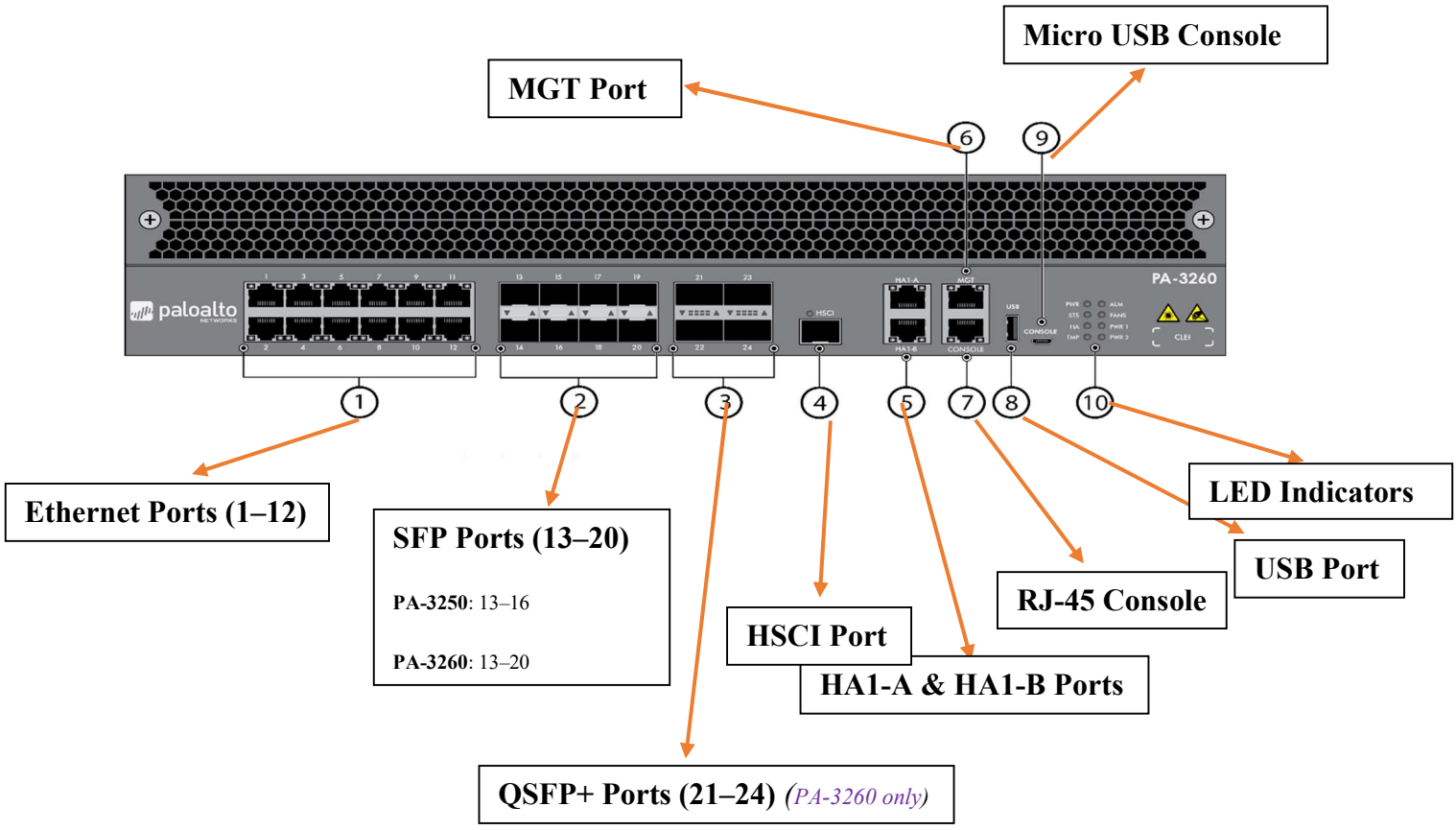
- ✓ Knows **which apps** are being used
- ✓ Sees **who's using them**
- ✓ Scans **everything** for threats
- ✓ Applies **smart policies**
- ✓ Still does all the basic firewall stuff

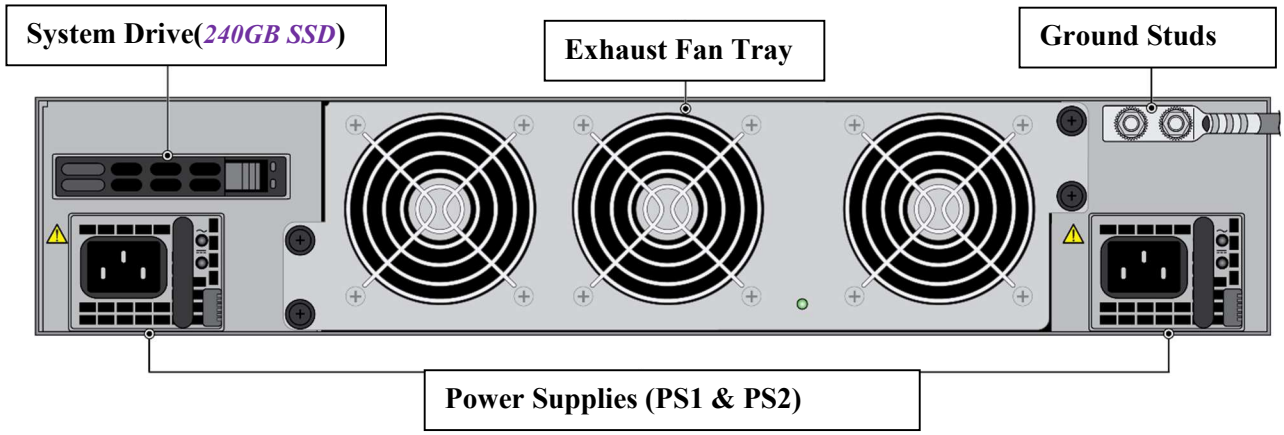
And it does all this **without slowing down your network**.



PA-3250 PHYSICAL LAYOUT

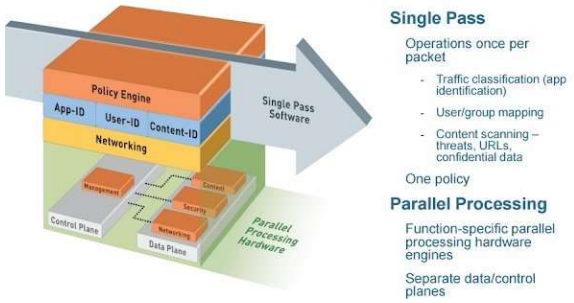
PA-3200 Series Firewall – Port Summary





Palo Alto Architecture

Palo Alto firewalls are designed to be **super fast and super smart** when it comes to securing your network. They use a special technology called **SP3 (Single Pass Parallel Processing)** architecture.



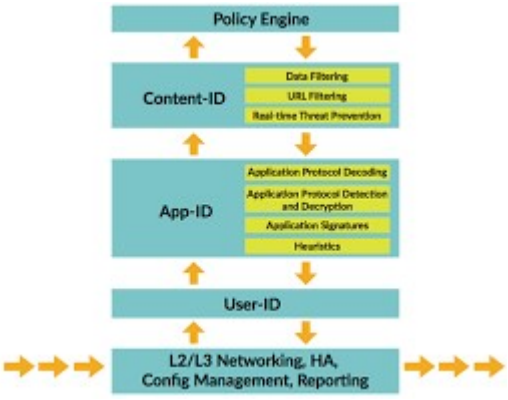
❖ *What is SP3? (Single Pass Parallel Processing)*

SP3 has **two main parts** that work together:

1. Single Pass Software (Fast & Smart Processing)

This software processes each network packet **only once** instead of multiple times.
During that single scan, it checks for:

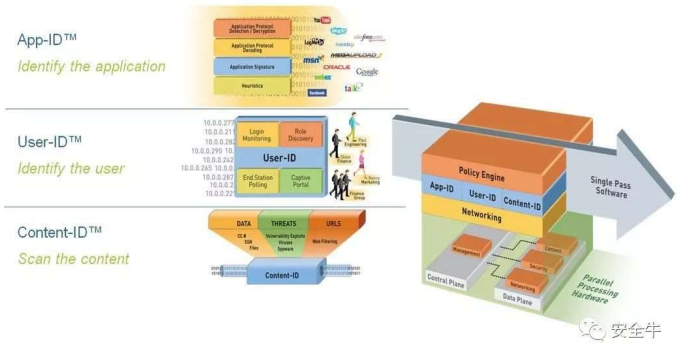
- ☑ ✅ **User-ID** – Who is sending the traffic
- ☑ ✅ **App-ID** – What application is being used
- ☑ ✅ **Content-ID** – Is there any virus or threat inside?
- ☑ ✅ **Policy Lookup** – Is this allowed based on firewall rules?
- ☑ ✅ **Decoding & Signature Matching** – Is it safe or suspicious?



🔄 **All this is done in one go!**
That means **less delay**, **less load**, and **faster results**.

2. Parallel Processing Hardware (Speed at Hardware Level)

While the software does the smart thinking, the **hardware handles everything in parallel**, using dedicated parts of the firewall. This boosts performance without slowing anything down.



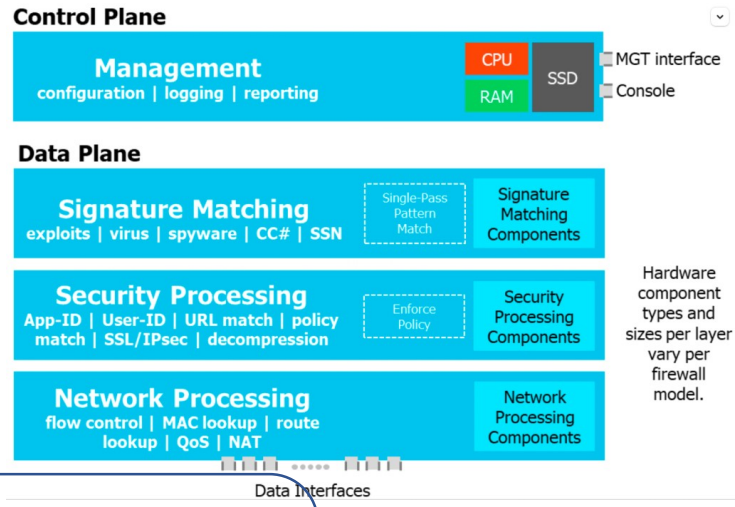
Separation of Planes = Smooth Performance

- **Control Plane** – Handles **management**, **policies**, and **configurations**.
- **Data Plane** – Handles **actual traffic** passing through the firewall.

These two planes are **separated**, so if you're doing heavy work in one (like updating policies), it **won't affect traffic flow**.

Inside the Data Plane – 3 Key Processors

1. **Signature/Content Processor**
   - Detects **viruses**, **malware**, **intrusions**, and does **App-ID** checks.
2. **Security Processor**
   - Handles **SSL decryption**, **policy enforcement**, and other **security tasks**.
3. **Network Processor**
   - Takes care of **routing**, **NAT**, and **layer 3 communication**.



Why It's So Good

- 🔁 **Processes each packet once** → Fast & efficient
- ⚡ **Parallel hardware processing** → High speed
- 🔒 **Advanced security checks** → Safer networks
- 🧩 **Separation of planes** → No performance drop under heavy load

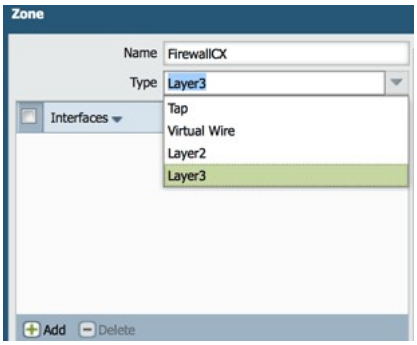
Palo Alto Networks – Security Zones)

What is a Security Zone?

Think of a **zone** as a **group** or **area** in your network that you want to apply specific rules to. Instead of creating rules for each **interface**, Palo Alto firewalls use **zones** to apply security policies.

- **Firewall rules** (like who can access what) are applied **between zones**, not interfaces.
- If an interface is not in a zone, **no traffic will pass through it**.

4 Main Types of Zones in Palo Alto

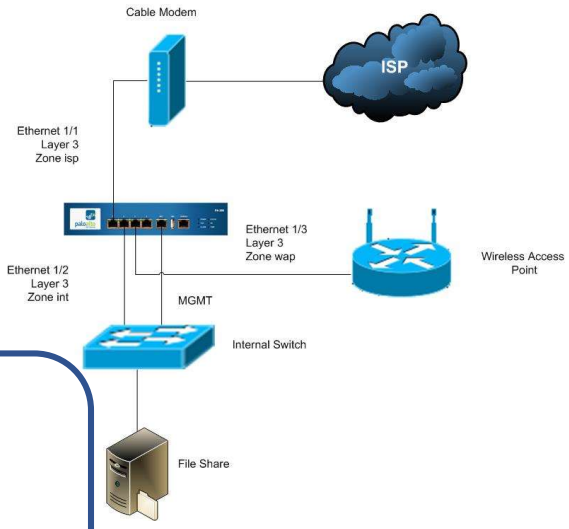


1. **Tap Zone**
   - **Monitors traffic only**, no control
   - Used with **SPAN/RSPAN** for packet inspection
   - Good for **passive monitoring** of network traffic
2. **Virtual Wire (VWire)**
   - Also called **transparent firewall**
   - Firewall sits in the path but **doesn't do any routing or switching**
   - Ideal when you don't want to change your existing network setup
3. **Layer 2 Zone**
   - Works like a **switch**
   - Interfaces can communicate within the same network (like VLANs)
4. **Layer 3 Zone**
   - Used when you need to **route traffic between networks**
   - Each interface must have an **IP address**
   - This is the most common zone type in enterprise networks

What is a Virtual Router in Palo Alto?

A **Virtual Router (VR)** is like a **built-in router** inside the firewall.
It helps the firewall **know how to reach other networks** by using:

- ☑ **Static routes** (manually added)
- ☑ **Dynamic routes** (like OSPF, BGP)



Where is it used?

Every **Layer 3 interface**, **loopback interface**, and **VLAN interface** on the firewall **must be linked to a virtual router**.

- ✓ A **virtual router** makes routing decisions for those interfaces.
- ✓ **One interface can belong to only one virtual router** at a time.

Why Use Multiple Virtual Routers?

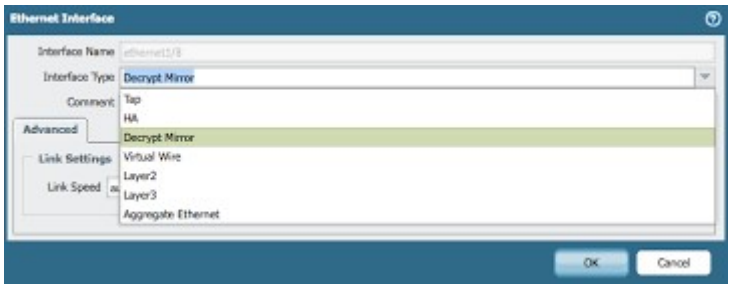
- The firewall can **act like multiple routers** at the same time.

- This helps when you want to **separate departments or customers**, like:
    - HR traffic uses **VR-HR**
    - Finance traffic uses **VR-Finance**
- You can even **reuse the same IPs** in different VRs without conflict. (Perfect for **multi-tenant** environments!)

Palo Alto Interface Types & Deployment Modes –

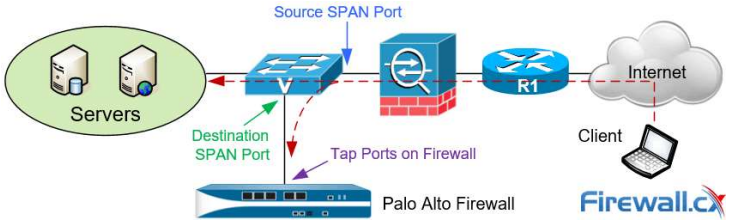
Why it's powerful?

Palo Alto firewalls are **very flexible**.
You can mix and match different interface types and deployment modes to fit your network.
That makes **network segmentation**, **monitoring**, and **security enforcement** super easy!



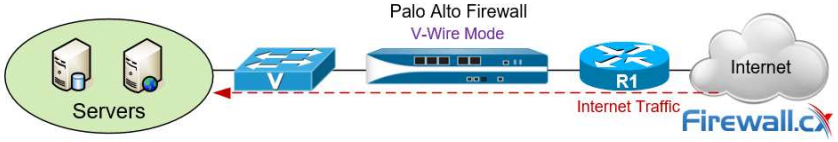
Physical Interface Modes (How to connect it)

1. **Tap Mode**



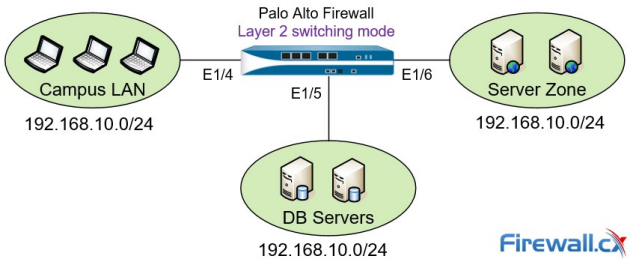
- ✓ Like a **CCTV camera** for your network.
- ✓ It **monitors** traffic using **SPAN ports** on a switch.
- ✓ 🔶 Good for: seeing what's happening, without changing anything.
- ✓ ❗ Can't **block** or **control** traffic, just **watch**.

2. **Virtual Wire (V-Wire)**



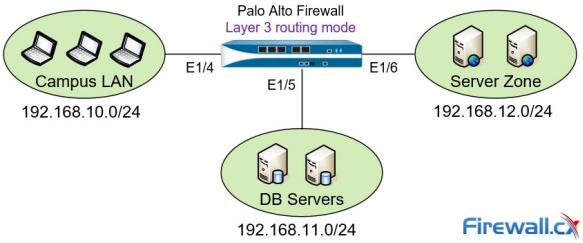
- ✓ Think of it like a **transparent firewall**.
- ✓ Sits between two devices **without needing an IP address**.
- ✓ 🔶 Good for: dropping in the firewall **without redesigning** your network.
- ✓ ✅ Can **monitor** and **control** traffic with full features.

3. Layer 2 Mode



- ✓ Works like a **switch**.
- ✓ Traffic flows between segments (like VLANs) within the firewall.
- ✓ 🔶 Good for: securing traffic inside your network.
- ✓ Can use **access or trunk ports** (802.1Q), but **no routing**.

4. Layer 3 Mode



- ✓ Works like a **router**.
- ✓ Interfaces have IP addresses and route between networks.
- ✓ 🔶 Good for: controlling traffic between **different subnets or VLANs**.
- ✓ Fully supports **routing, NAT, DHCP, VPNs**, etc.

5. Aggregate Interfaces

- ✓ Combines multiple physical ports into one logical link for **higher bandwidth** and **redundancy**.

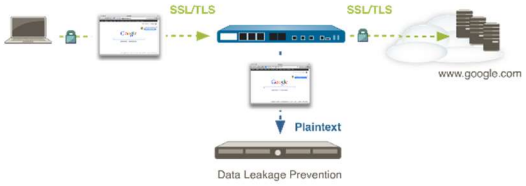
6. HA (High Availability)

- ✓ Use special interfaces to link **two firewalls** for redundancy.
- ✓ If one fails, the other takes over.

Logical Interface Types (Used inside config)

1. **VLAN Interface**
   - Used in Layer 2 mode to route between VLANs using a Layer 3 gateway.
2. **Loopback Interface**
   - A virtual interface (doesn't connect to a cable).
   - Useful for testing, management, or VPN termination.
3. **Tunnel Interface**

- ✓ Used for **VPNs** (IPSec/SSL).



4. **Decrypt Mirror**

- ✓ Copies decrypted traffic to a monitoring tool for inspection (great for SOC/security teams).

(Quick View)

Mode	Controls Traffic	Needs IP	Used For
Tap	✗ No	✗ No	Monitoring only
Virtual Wire	✓ Yes	✗ No	Inline control, no IP needed
Layer 2	✓ Yes	✗ (L2)	Segmenting VLANs (switching)
Layer 3	✓ Yes	✓ Yes	Routing between networks/subnets

Palo Alto Packet Flow –

Think of the packet flow like a **security checkpoint** at the airport, where every packet (data) goes through checks before it's allowed through. Here's how it works:

---

1. Ingress (Packet Enters)

- ✓ The packet **enters the firewall** through a physical interface (like Ethernet).
- ✓ The firewall checks if the interface and zone are valid.
- ✓ If the interface isn't in a security zone, the packet is **dropped**.

---

2. Flow/Session Lookup

- ✓ The firewall checks if this traffic already has an **existing session**.
  - If yes → it uses the **fast path** (skips deep checks).
  - If no → it goes to **slow path** (full inspection).

---

3. Slow Path (First Time Traffic)

- Full inspection of traffic begins:

  - ✓ **Zone checks**
  - ✓ **Policy lookup** (matches rules you've configured)
  - ✓ **Routing decisions**
  - ✓ **NAT policies**

If it passes all checks, a new **session** is created in the firewall.

---

4. Fast Path (Subsequent Packets)

- ✓ Once a session is set up, next packets in the same session go through **fast path** for **quicker performance**.
- ✓ Still gets checked for threats, but skips the full slow path steps.

---

5. App-ID (Application Identification)

- ✓ The firewall inspects the packet's content to **detect what application** is being used (e.g., Facebook, YouTube, BitTorrent).
- ✓ Doesn't just rely on port numbers.

6. Content-ID (Deep Security Check)

- Checks for:
  - ✓ **Viruses**
  - ✓ **Spyware**
  - ✓ **Malware**
  - ✓ **URL filtering**
  - ✓ **Data loss (DLP)**

Basically, this is the **deep security brain** of the firewall.

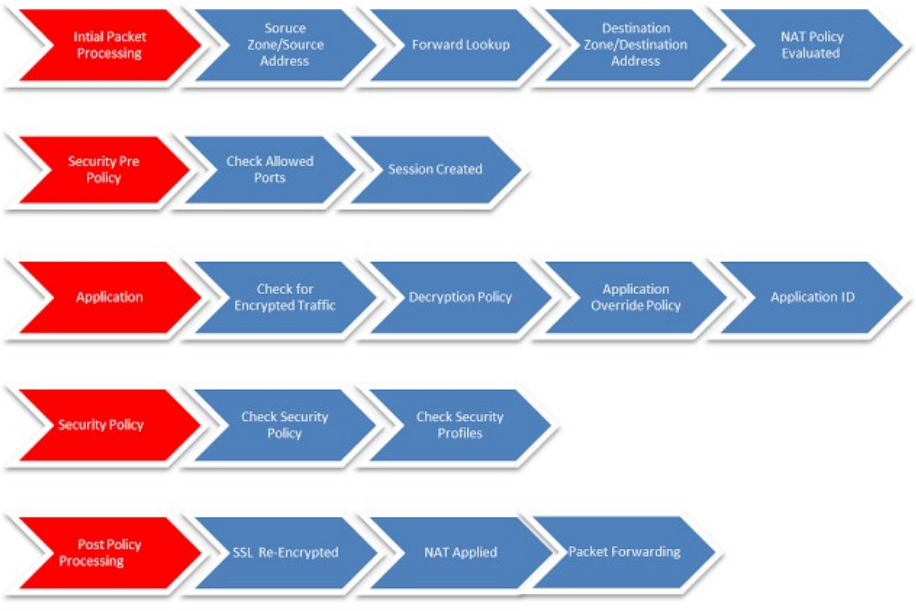
---

7. Forwarding / Egress

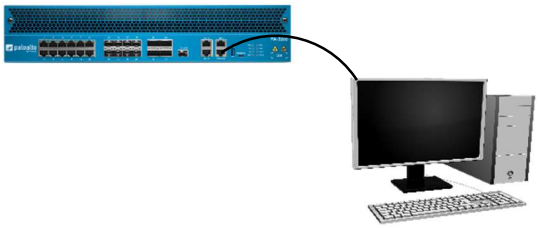
- ✓ After passing all inspections, the packet is **forwarded** to its destination.
- ✓ Routing and NAT rules are applied again if needed.

In Short:

1. **Ingress** – Packet enters
2. **Session Lookup** – Fast path or slow path?
3. **Slow Path** – Deep check if new
4. **Session Setup** – Save session details
5. **App-ID** – What app is this?
6. **Content-ID** – Is it safe?
7. **Forwarding** – Send it out



How to Manage a Palo Alto Firewall



All Palo Alto firewalls come with a **dedicated management port (MGT)** — this is used just for **managing the device**, not for passing user traffic.

Ways to Access the Firewall

You can manage the firewall using:

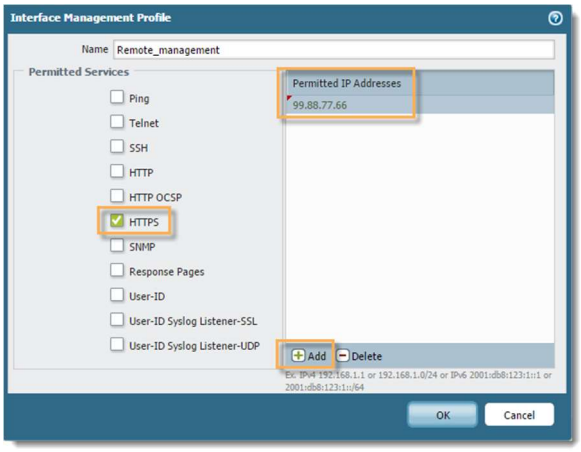
- ✓ **Web Interface** – Easy-to-use browser-based GUI
- ✓ **CLI (Command Line Interface)** – For advanced users
- ✓ **Panorama** – Centralized management for many firewalls

You can give the **MGT port** an **IP address manually (static)** or **get it from a DHCP server**.

⚠ What If the MGT Port Goes Down?

No problem! You can still manage the firewall through any **data interface** (the ones that carry user traffic), but you must **explicitly allow** this.

Services You Can Enable on Data Interfaces



(Using a **Management Profile**)

You can **choose which services** are allowed on each interface. Examples:

- ✅ **HTTPS** – For secure web access (enabled by default)
- ✅ **SSH** – For remote command-line access (enabled by default)
- ✅ **Ping** – For testing connectivity (enabled by default)
- 🔄 **Telnet** – Older remote access (not secure)
- 🌐 **HTTP** – Unsecure web access
- 📡 **SNMP** – For monitoring
- 📄 **Response Pages** – Shown when access is blocked
- 👤 **User-ID** – For identifying users

To make this work, you **create and assign a Management Profile** to that interface.

By Default:

If you **don't assign a Management Profile**, the firewall will **block all management access** on that interface — even ping or web access.

Example Use Case:

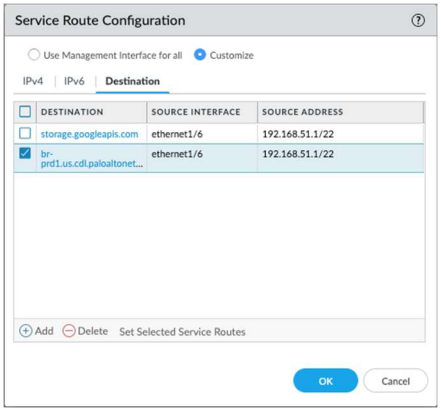
You want to **manage the firewall using a LAN port** if the MGT port fails:
→ Assign a Management Profile that allows **HTTPS and Ping**
→ Apply it to the LAN interface
→ Now you can still log in if MGT goes down!

What are Service Routes?

By **default**, Palo Alto firewalls use the **Management (MGT) interface** to reach out to external services like:

- ✓ **DNS** (Domain Name System)
- ✓ **Email servers** (for alerts, etc.)
- ✓ **Palo Alto update servers** (for threat updates, firmware, etc.)
- ✓ **External Dynamic Lists (EDLs)**
- ✓ **Panorama** (for centralized management)
- ✓ **LDAP** (for user authentication)

Why Use Custom Service Routes?



Sometimes, you may want these services to go **through a different interface** instead of the MGT port — maybe due to:

- ✓ MGT not having internet access
- ✓ Using a different ISP
- ✓ Better routing or performance
- ✓ Security policies

That's where **Service Route Configuration** comes in.

Example Use Case

You want **DNS and updates** to go through your **Ethernet1/1** interface instead of MGT:

- ✓ You go to **Device > Setup > Services > Service Route Configuration**
- ✓ Choose services like DNS, LDAP, Updates, etc.
- ✓ Set the **"Source Interface"** to ethernet1/1
- ✓ Set the **"Source Address"** (e.g., 203.0.112.20)

Now the firewall will send DNS and updates **through Ethernet1/1** instead of the MGT port.

What Are Dynamic Updates?

Palo Alto Networks regularly releases ***updates to protect your network*** from new and emerging threats. These updates include:

- ***Application Updates*** – New apps or changes in how apps behave (App-ID).
- ***Threat Updates*** – New viruses, malware, spyware signatures, and attack patterns (Threat Prevention).
- ***GlobalProtect Updates*** – For VPN and remote access improvements.
- ***WildFire*** – New threat intelligence from cloud-based analysis.
- ***URL Filtering & EDLs*** – Updates for web filtering and external block lists.

Why Schedule These Updates?

To **stay protected**, you should **automatically download and install** these updates regularly (like every hour or daily), so your firewall is always ready to block the **latest threats** — even ones that were just discovered.

How It Works:

1. **Go to**:
   Device > Dynamic Updates
2. **Set a schedule** for each update type:
   - Download Frequency (e.g., every 1 hour)
   - Install Immediately after download
3. The firewall will **check Palo Alto's cloud**, download the updates, and **install them automatically**.

✅ *Benefits:*

- Always up to date
- Better protection against new threats
- No need to manually update

Firewall Configuration Management :

1. *Candidate Configuration*

When you make changes to a Palo Alto firewall (like editing policies, interfaces, or routes), the changes are first stored in a **candidate configuration**.

- ✓ This config is temporary and **resides in the memory** of the **management (control) plane**.
- ✓ It does **not affect live traffic** until committed.

---

2. *Commit Process*

To make the changes active, you must **commit** them.

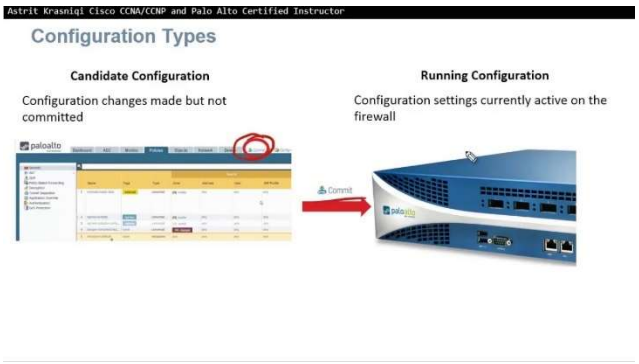
- ✓ **Commit** applies the candidate config to the actual firewall operation.
- ✓ During commit, the configuration is pushed to the **data plane**, which handles real traffic.

---

3. *Running Configuration*

Once committed:

- ✓ The active config becomes the **running configuration**.
- ✓ It is saved in a file named **running-config.xml**.
- ✓ This is the version of the config the firewall uses to process live traffic.



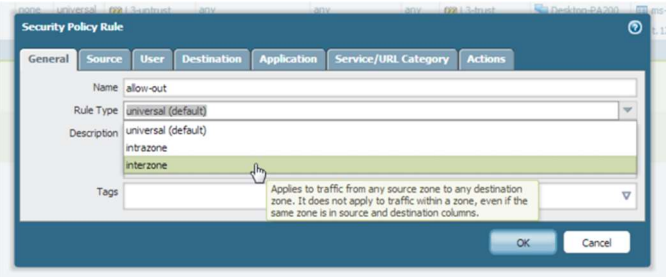
---

4. *Why This Method is Useful*

- You can review and verify changes **before they go live**.
- Mistakes can be caught and corrected before affecting production traffic.
- It supports **safe and controlled configuration management**.

What Are Security Rules?

Security policies (rules) control **what traffic is allowed or denied** through the firewall. You can make them **specific** (like allowing one app from one IP) or **general** (like blocking all traffic from a zone).



Types of Security Rules

1. Intrazone Rule

- ✓ **Traffic Source & Destination:** From **same zone**
- ✓ **Default Behavior: Allow**
- ✓ Example: Traffic between devices in the LAN zone (e.g., PC to Printer).
- ✓ **You can still customize it.**

2. Interzone Rule

- ✓ **Traffic Source & Destination:** From **different zones**
- ✓ **Default Behavior: Deny**
- ✓ Example: Traffic from the LAN zone trying to reach the internet (Trust → Untrust).
- ✓ You need to **explicitly allow** this traffic by creating a rule.

3. Universal Rule

- ✓ **Traffic:** Can apply to **both same and different zones**
- ✓ Useful when you want a single rule to cover **multiple situations.**

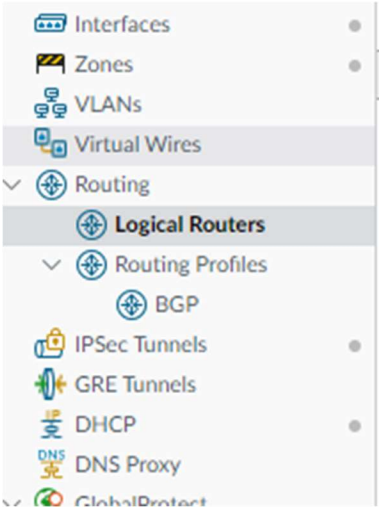
Actions in Security Policies

Action	*Description*
Allow	Permits the traffic.
Deny	Blocks the traffic without a response.
Drop	Silently discards packets (no feedback to sender).
Reset Client	Sends a TCP RST to the client only.
Reset Server	Sends a TCP RST to the server only.
Reset Both	Sends a TCP RST to both client and server (clean termination).

What is the Advanced Routing Engine?

The **Advanced Routing Engine** in Palo Alto's PAN-OS helps the firewall do **advanced routing** like a full-featured router. It supports both **basic and dynamic routing protocols**, which makes it suitable for use in:

- ✓ **Enterprises**
- ✓ **Data centers**
- ✓ **ISPs**
- ✓ **Cloud environments**



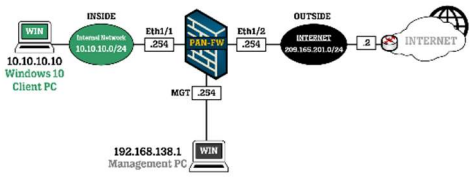
What Routing Features Are Supported?

Feature	Description
Static Routes	Manually set paths for traffic to follow.
BGP	Border Gateway Protocol, used between large networks like ISPs.
OSPFv2 / OSPFv3	Open Shortest Path First – for IPv4 (v2) and IPv6 (v3).
RIPv2	An older dynamic routing protocol.
Route Redistribution	Shares routes between different routing protocols.
Route Maps & Filters	Control which routes go in or out.
Prefix/Access Lists	Define what networks or IPs to allow or block in routing.

Virtual Routers = Logical Routers

- ✓ On Palo Alto firewalls, **"Virtual Routers"** are like **independent routers** inside the same device.
- ✓ You can use multiple virtual routers to **separate traffic** or clients (e.g., departments or customers).
- ✓ Each VR can run different routing protocols.

Administrative Distance (AD)



When **multiple routing options** exist to the same destination, the firewall uses **Administrative Distance (AD)** to choose the **best route**.

- **Lower AD = More Trusted**

Route Type	AD Value
Static Route	10
Static IPv6	10
OSPF Internal	30
OSPF External	110
OSPFv3 Internal	30
OSPFv3 External	110
RIP	120 (not shown but standard)
BGP	20 (assumed standard unless changed)

What is NAT?

NAT changes private IP addresses (like 192.168.x.x) into public IP addresses (like 203.x.x.x) so your internal devices can talk to the internet.

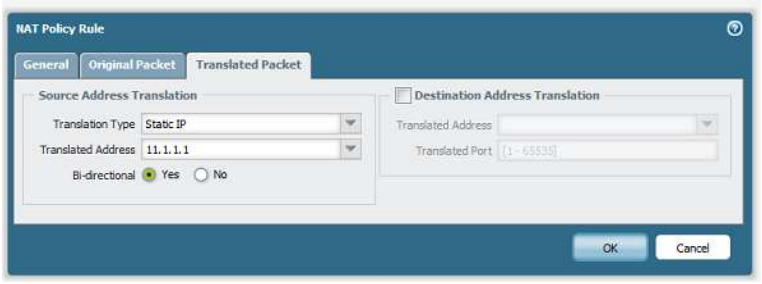
Palo Alto firewalls support NAT on:

- ✓ **Layer 3 interfaces**
- ✓ **Virtual Wire interfaces**

🔒 It also hides internal IPs for **security**
📉 It helps save **public IP addresses**

1.*Source NAT (SNAT)*

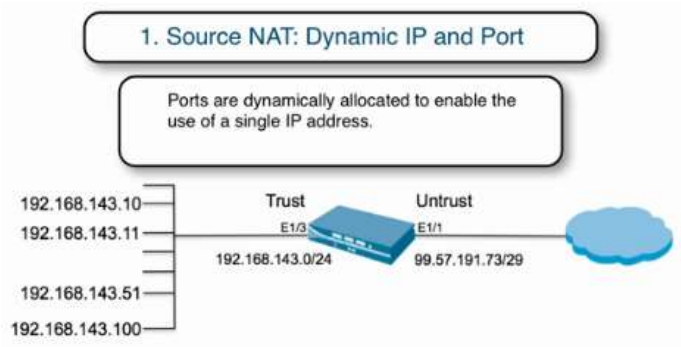
Used when **internal users** want to **access the internet**.



☑ *1. Dynamic IP and Port (DIPP)*

- ✓ **Many private IPs** share **one public IP**, but with **different ports**.
- ✓ Example:
  - 192.168.1.10 → 203.0.113.5:5001
  - 192.168.1.11 → 203.0.113.5:5002

➢ **Great for saving public IPs**



Translation Options:

- ✓ **Address Pool**: You define a range (e.g., 203.0.113.5–203.0.113.10)
- ✓ **Interface Address**: The public IP of the firewall interface is used for translation

➢ If the interface gets a new IP (DHCP, PPPoE), the NAT rule will automatically update.

☑ *2. Dynamic IP*

- ✓ ***One-to-one*** mapping (but dynamically assigned)
- ✓ Only IP address is changed — ***ports are not used***
- ✓ Each internal IP gets its own pu*b*lic IP from a pool

If the **NAT pool is small**, and all IPs are in use, **new connections get dropped**.

Optional Fix: Use "***Dynamic IP and Port Fallback***" so it uses ports if IPs run out.

Summary Table

TYPE	DESCRIPTION	USE CASE
DYNAMIC IP & PORT	Many-to-one	Internet browsing for many users
DYNAMIC IP ONLY	One-to-one	More control per user/device

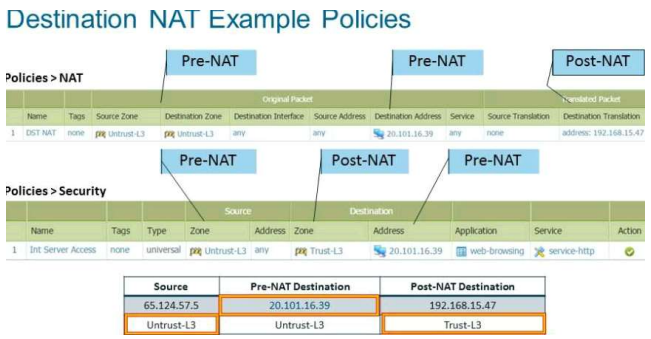
Static IP NAT

☑ *Source NAT – Static IP*

- ✓ **One-to-one** translation of an internal IP to a fixed public IP
- ✓ **Always the same IP** is used
- ✓ 🔁 Best for when an **internal device/server** needs to go out using a **specific public IP**

***Example**:*
Your internal server (192.168.1.100) always uses public IP **203.0.113.5** for outgoing traffic.

2.*Destination NAT (DNAT)*



Used when **someone from the internet** needs to **access your internal server** (like a website or mail server).

☑ *Static IP*

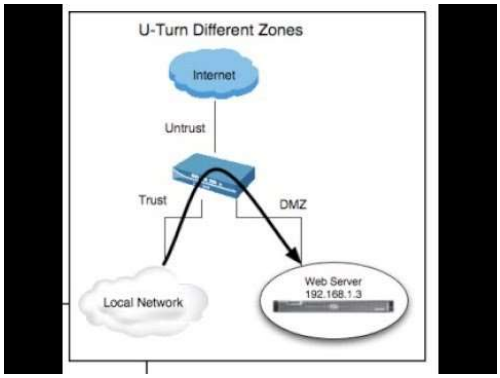
- ✓ Public IP maps **permanently** to one internal server
- ✓ Used for **hosting internal services to the public**

***Example**:*
Public IP **203.0.113.10** always forwards to **192.168.1.10 (Web Server)**

☑ *Dynamic IP (with Session Distribution)*

- ✓ Used with **FQDN-based address objects** (like server.example.com)
- ✓ DNS might return multiple IPs for the FQDN
- ✓ Firewall **balances** traffic among those IPs
- ✓ Useful in **cloud setups** where public IPs change dynamically

3.*U-Turn NAT*



Used when:

- ✓ An **internal user** accesses an **internal server** using its **external/public IP**

Why?

- ✓ Sometimes, DNS gives external IPs even to internal users

U-Turn NAT ensures the traffic ***goes out and comes back in properly***, so internal users can still access internal servers using public URLs.

Example:

- ✓ Internal client: 192.168.1.5
- ✓ Tries to access: www.yourcompany.com → (Public IP: 203.0.113.10)
- ✓ U-Turn NAT will route that request back to internal web server: 192.168.1.10

Summary Table

Type	*Use Case*
Static Source NAT	Fixed public IP for internal device
Destination Static NAT	Public can access internal service
Dynamic DNAT (FQDN)	For cloud/dynamic IP environments
U-Turn NAT	Internal clients access internal servers via public IP

What is the Data Plane?

The **data plane** is the part of the firewall that handles **actual network traffic**—it's where **packets are inspected, forwarded, blocked, or allowed**.

Key Components of the Data Plane

To process traffic fast and efficiently, Palo Alto firewalls use different **specialized chips and CPUs** in the data plane. Here's a breakdown:

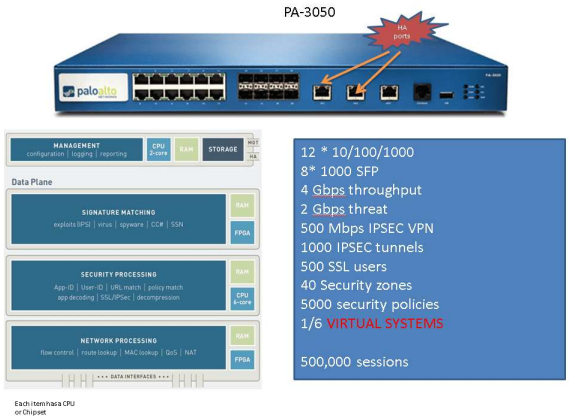
---

1. *Network Processor (Session Offloader CPU)*

- ✓ Handles **network layer tasks** like:
  - **Routing**
  - **NAT (Network Address Translation)**
  - **QoS (Quality of Service)**
- ✓ Think of it as the **fast lane** for routing packets.

---

2. *Security Processor (Data Plane CPU)*

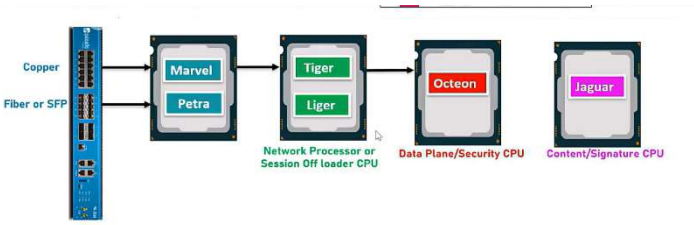


- ✓ Performs **security-related tasks** such as:
  - Policy checks
  - SSL decryption
  - Session setup
- ✓ Helps **enforce firewall rules** for each session.

3. *Content Processor (Signature/Content CPU)*

- Deep inspection of traffic:
  - Looks for **viruses**, **malware**, **intrusions**
  - Runs **App-ID**, **Content-ID**, and **Threat-ID**
- It checks the **actual content** inside the packets (payload scanning).

⚙ *Custom Hardware Components*

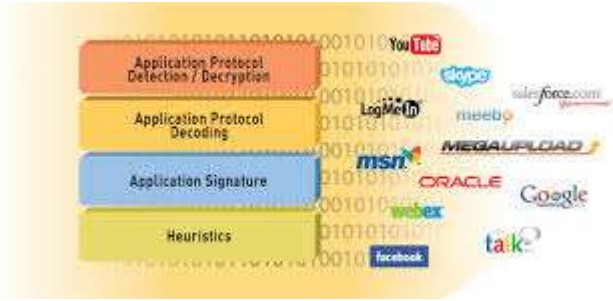


Some chip names you mentioned refer to **specific hardware units** (ASICs or FPGAs) used in Palo Alto firewalls. Here's a simple mapping:

Chip/Name	*Function*
Octeon	General-purpose CPU used for data processing
Marvel	Handles physical interfaces like copper and fiber
Petra, Tiger, Liger, Jaguar	Specialized ASICs/FPGAs for high-speed packet processing
Copper/Fiber/SFP	Types of physical ports used for network connectivity

---

What is App-ID?



App-ID is Palo Alto Networks' ***unique, patented technology*** that identifies *applications* passing through the firewall — regardless of **port number, protocol, or even encryption** (like SSL or SSH).

It lets you create **security rules** based on actual applications, not just IP addresses or ports. This makes the firewall **more accurate and secure**, especially at **Layer 7 (application layer)**.

How Does App-ID Work?

App-ID identifies applications using a **four-step process**:

1. ***Protocol and Port Analysis***
   - First, it looks at the port and basic protocol to make an initial guess about the traffic.
2. ***Decryption (if needed)***
   - If traffic is encrypted (SSL or SSH), App-ID **decrypts it temporarily** (if allowed) to see what application is inside.
3. ***Application Protocol Decoding***
   - It checks how the protocol behaves (how the data is structured or communicated) to better recognize the app.
4. ***Application Signatures & Heuristics***
   - It uses **signatures** (predefined patterns) and **heuristics** (behavioral analysis) to accurately identify the application.
   - For example, it can tell whether the traffic is **Skype**, **Facebook**, **Webex**, etc., even if they're all using port 443.

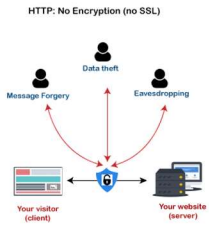
Application Signatures and Updates

- ✓ *2,000 App-ID signatures*
- ✓ *Grouped into 5 main categories Further split into 40 sub-categories (e.g., File sharing, Collaboration, etc.)*
- ✓ *New App-IDs are added weekly (3–5 per week) to keep up with evolving applications.*

Why is App-ID Important?

- **Better Security: Blocks risky apps like file-sharing tools or remote access software.**
- **Granular Control: Allows specific actions like:**
  - **"Allow Facebook, but block Facebook Chat"**
  - **"Block unknown applications after hours"**
- **Improved Visibility: You get full insight into what apps are being used on your network — no more relying only on IPs and ports.**

SSL (Secure Sockets Layer)



Feature	*SSL*	*TLS*
Full Form	Secure Sockets Layer	Transport Layer Security
Developed By	Netscape	IETF
Versions	SSL 1.0–3.0 (Deprecated)	TLS 1.0–1.3 (Latest: TLS 1.3)
Security	Less secure	More secure
Performance	Slower, outdated cryptography	Faster, improved encryption
Current Use	Deprecated, not recommended	Actively used, industry standard
Compatibility	Old systems	Modern systems

Why SSL/TLS Is Important

✅ 1. ***Protects Data in Transit***

- ☑ SSL (Secure Sockets Layer) and TLS (Transport Layer Security) **encrypt data** when it's sent between a user's browser and a website or service.
- ☑ This **prevents hackers** from reading sensitive information like:
  - Passwords
  - Credit card numbers
  - Personal details

✅ 2. ***Builds Trust***

- ☑ When a website uses SSL/TLS (shows 🔒 or "HTTPS"), users feel **safe** and **trust** the site.
- ☑ Without it, modern browsers show **"Not Secure"** warnings.

Real Stats:

- ✓ **85–95% of internet traffic** is now encrypted.
- ✓ **70% of malware** campaigns use encryption to **hide from security tools** (Gartner).
- ✓ **Modern protocols (TLS 1.2, TLS 1.3)** and **HTTP/2** are the new standards.
- ✓ **Free SSL certs** (e.g., via Let's Encrypt) have made it **easy for anyone—even attackers—to use encryption.**

✅ 3. Required for Compliance

- Industries like **banking, healthcare, and e-commerce** require encryption for legal and compliance reasons (e.g., GDPR, HIPAA, PCI-DSS).

The Hidden Danger: Encrypted Traffic Can Carry Malware

Even though SSL/TLS is good for security, attackers use it **against you** by **hiding threats inside encrypted traffic**.

How It Works:

1. A hacker **uploads a malicious file** to a website over HTTPS.

The Solution: Decryption + Inspection

- ✓ Firewalls like **Palo Alto Networks NGFW** can **decrypt SSL/TLS traffic**, **scan it for threats**, and then **re-encrypt it** before sending it to the user.
- ✓ This process:
  - Blocks **malicious downloads**
  - Detects **hidden malware**
  - Protects users even if traffic is encrypted

2. A user **downloads it** thinking it's safe because it's from a "secure" site.
3. The malware **bypasses inspection** because the firewall **can't see inside** the encrypted content.
4. The malware **infects the user's device** and starts stealing data or damaging the network.

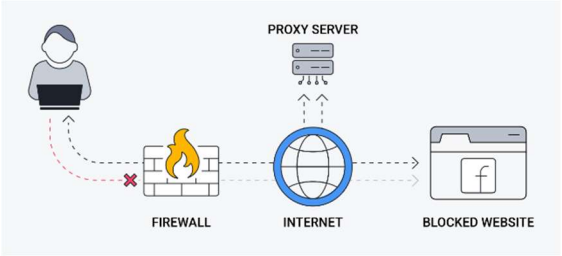
Why Decrypt Traffic at All?

When data (like emails, web browsing, apps) travels on your network, it's often encrypted using HTTPS or other secure methods. That's great for privacy, but **if you can't see inside the encrypted traffic, you can't inspect it for threats** like malware or data leaks.

To solve this, companies use tools that **decrypt, check, then re-encrypt** the traffic.

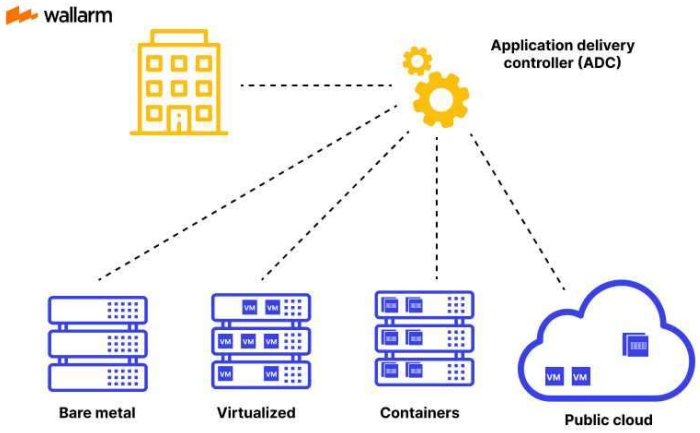
1.*Web Proxies*

- ✓ Think of a **web proxy** like a **traffic inspector standing between your browser and the internet**.
- ✓ It can **decrypt** your traffic, look inside for anything bad, then **re-encrypt** and send it out.
- ✓ Works **only for web traffic** (like sites using HTTP/HTTPS).
- ✓ **Can't inspect** traffic from other apps like Microsoft Office 365, which use more than just web ports.
- ✓ Requires setting it up in the browser or using a config file.
- ✓ Adds extra steps in troubleshooting if users face issues.



---

2. *Application Delivery Controllers (ADCs)*



- ✓ ADCs are used to **handle and optimize app traffic**.
- ✓ Usually, two devices are used:
  - One to **decrypt**
  - One to **re-encrypt**
- ✓ **Risk:** Once traffic is decrypted, it travels **unencrypted** between the devices.
- ✓ If someone is snooping on the internal network (like a hacker), they could **steal or change** the data.

---

3. *Next-Gen Firewalls (NGFWs) & SSL Appliances*

- ✓ These are advanced firewalls that can:
  - **Decrypt, inspect, and re-encrypt** traffic
  - Work with **more than just web traffic**
- ✓ NGFWs are **more versatile** than web proxies.
- ✓ SSL appliances do a similar job but are focused mainly on handling encrypted (SSL/TLS) traffic.

☑ **Palo Alto NGFW decrypts and inspects all kinds of traffic (web + non-web) securely inside the firewall, giving full visibility and protection — without compromising on encryption standard**

Visual Summary:

Tool	*What it Does*	*Traffic Type*	*Risk*	*Setup*
Web Proxy	Decrypts only web traffic	HTTP/HTTPS	Limited visibility	Browser setup needed
ADC	Handles app delivery + decrypts	App-specific	Data unencrypted between devices	Complex setup
NGFW / SSL Appliance	Full inspection of all types of traffic	All (not just web)	More secure	More integrated

---

1. *Without SSL Decryption*

- ✓ When SSL is used, the **firewall sees only the outside of the packet** (just the destination, not the content).
- ✓ It's like **looking at a sealed envelope** — you know where it's going, but not what's inside.

- ✓ ❗**Problem:** Hackers and malware can hide inside encrypted traffic, and the firewall won't catch them.

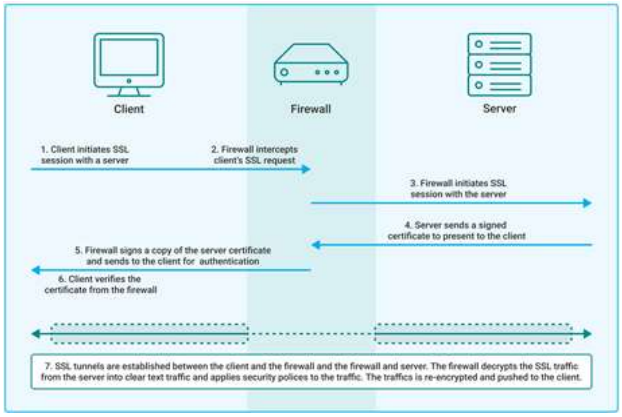
2.With SSL Decryption (on Palo Alto)

- ✓ Palo Alto firewall can **temporarily decrypt** the SSL traffic:
  - Opens the packet securely
  - **Inspects the content** for bad stuff (malware, data leaks, unknown apps)
  - Then **re-encrypts** it before sending it out
- ✓ Now the firewall acts like a **secure checkpoint**:
  - It sees the **real content**
  - It can stop **hidden threats**
  - It gives full **visibility into apps, websites, and user behavior**

What You Can See With SSL Decryption

Without SSL Decryption	*With SSL Decryption*
Just destination IP/domain	Full website URL, file downloads, keywords
No visibility into hidden apps	Detect apps like Psiphon, Tor, or tunnels
Missed threats inside HTTPS	Malware & data theft detection inside SSL

Step-by-Step: How SSL Decryption Works on a Firewall



When a client (like a user's browser) connects to a secure website (`https://`), here's how the **firewall decrypts and inspects the traffic** without the client or server knowing anything changed.

1.Client Sends Client Hello

- This is the first step in any SSL/TLS handshake.
- The **client (browser)** sends a **Client Hello** message to start the secure connection.
- This message includes:
  - Supported **SSL/TLS versions**
  - Supported **encryption algorithms (ciphers)**

2.*Firewall Intercepts the Connection*

- ✓ The firewall **intercepts** this Client Hello — it doesn't let it reach the real server yet.
- ✓ Now, the firewall **pretends to be the client**, and sends its own **Client Hello** to the **real server**, using the settings from the firewall's **SSL Decryption Policy**.

3.*Server Responds with Server Hello*

- ✓ The real **server** replies to the firewall with a **Server Hello**, which includes:
  - The selected TLS version
  - The encryption method to use
  - The server's **digital certificate**

4.*Firewall Validates the Server Certificate*

- The firewall checks the server's certificate to see if it's **valid and trusted**.
- If the certificate is invalid (expired, untrusted, etc.), the firewall **blocks the connection**.

5.*Firewall Creates a Dynamic Certificate*

- If the server certificate is valid, the firewall creates a **fake certificate** called a **dynamic certificate**.
- This dynamic certificate:
  - Is made to **look exactly like the real server's certificate** (same domain, etc.)
  - Is **signed by the firewall's root certificate**

> This is why the **client must trust the firewall's root certificate** — it's like saying: "I trust this firewall to sign secure certificates on my behalf."

6.*Firewall Sends Server Hello to the Client*

- The firewall sends this dynamic certificate to the client.
- To the client, it **looks like it's talking to the real server** — but it's actually talking to the firewall!

7.*Connection is Established*

- The **client trusts the certificate** (because the firewall's root cert is installed on the client).
- The secure TLS connection is established.
- The firewall can now:
  - **Decrypt** the traffic
  - **Inspect** it for threats
  - **Re-encrypt** it and send it to the real server

1.Outbound SSL Decryption (SSL Forward Proxy)

When users inside your network visit secure websites (like `https://google.com`), the firewall sits in the middle.
It **pretends to be the website**, so it can **see and check** what's inside the encrypted traffic.
To do this, the firewall quickly **creates a fake certificate** for that website, using the same validity period as the real one.

2.Inbound SSL Decryption

When someone from the internet is visiting your internal website (like `https://yourserver.com`),
you give the firewall **a copy of the website's certificate and private key**.
That way, the firewall can **decrypt the traffic**, check it, and then **forward it to your web server** safely.

Generating a Self-Signed Certificate

To *decrypt* HTTPS traffic, the firewall needs to act like a ***Certificate Authority (CA)***—just like trusted certificate companies do.
You can either:

- ✓ Create a **self-signed CA** directly on the firewall
- ✓ Or import one from your internal PKI system

Then you assign:

- ✓ A **Forward Trust Certificate** (for safe/trusted sites)
- ✓ A **Forward Untrust Certificate** (for risky/untrusted sites)

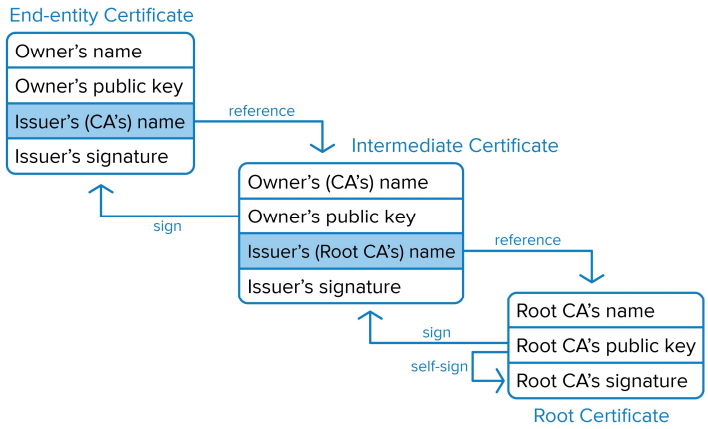
This helps the firewall **securely create fake certificates** for inspection while keeping your users safe.

Public Key Infrastructure (PKI)

PKI is a system that helps **prove who someone is** online using **digital certificates**.
It makes sure the public key you're using **actually belongs to the person or website** you think it does.

CA Hierarchy (Certificate Authority Hierarchy)

Think of it like a **family tree of trust**:



1. ***Root CA***
   - The top-level, most trusted certificate authority
   - Rarely used directly—**signs Intermediate CAs**
   - Stored safely, like a crown jewel
2. ***Intermediate CA***
   - Certified by the Root CA
   - Does the real work: **signs certificates for websites and devices**
   - Helps keep the Root CA safe
3. ***End-Entity Certificates (like websites, servers)***
   - Issued by the Intermediate CA
   - These are the certificates you see on websites like `https://example.com`

Certificate DB (Database)

- ✓ This is where the firewall or system **stores all certificates** it uses or trusts.
- ✓ The **Palo Alto firewall** uses this to **store and manage X.509 certificates**, which are standard digital certificates in PKI.

A Certificate = Public Key + Identity

It's like an ID card that says:

"*This public key belongs to* `www.google.com`*, and it was verified by a trusted CA*."

What is User-ID?

In modern networks, people use **multiple devices**—laptops, phones, tablets—and their **IP address keeps changing** (because of DHCP).
So, if you try to track users based on IP address, it becomes **very confusing and unreliable**.

User-ID Solves This Problem

User-ID is a feature (like in Palo Alto firewalls) that helps the firewall **connect a username to an IP address**.
This way, instead of saying:

"Block IP 192.168.1.25"
you can say:
"Block Vishu from using YouTube"

No matter **which device** Vishu is using or what his **IP address is today**, the firewall knows it's him.

How it works

- ✓ User logs in to a system (like Windows, AD, etc.)
- ✓ User-ID Agent or firewall sees that login and **maps the username to the IP address**
- ✓ Now, the firewall can track and **apply policies based on username**

Why it's helpful

- ✓ Easier tracking of user activity
- ✓ Better security policies
- ✓ Works across multiple devices and changing Ips

Why We Need User Mapping

To apply security policies **based on usernames**, the firewall needs to know **which user is using which IP address**.

1. *Server Monitoring*

- A special agent watches login events on **Windows servers** (like Domain Controllers or Exchange Servers).
- When a user logs in, it maps the **username to the IP address** using those logs.

- Can be done using a **User-ID agent on the firewall** or a **separate Windows-based agent**.

---

2. *XFF Headers (X-Forwarded-For)*

- If traffic goes through a **proxy**, the firewall might only see the **proxy's IP**, not the real user's IP.
- The proxy can add an **XFF header** that shows the real IP of the client.
- The firewall reads this header to **map the user correctly**.

---

3. *Port Mapping (Terminal Server Environments)*

- In environments like **Citrix or Terminal Servers**, many users **share one IP address**.
- The solution: track the **source port** each user is using.
- Requires installing the **Palo Alto Terminal Server Agent** to track **user-to-port mappings**.

---

4. *Syslog Parsing*

- Devices like **Wi-Fi controllers, proxies, NAC, 802.1x**, etc., log user activity.
- You configure them to send **syslog messages** to the firewall.
- The firewall reads the logs and **maps usernames to IPs** based on login/logout events.

---

5. *GlobalProtect*

- For **remote/mobile users**, GlobalProtect VPN can collect the **user login info**.
- This info is added to the **User-ID table** on the firewall.
- Keeps visibility and control even **when users aren't on-prem**.

---

6. *Authentication Policy & Captive Portal*

- If nothing else works (e.g., user is on **Linux**, or not logged into AD),
- The firewall can **ask the user to log in via a browser** (Captive Portal).
- Once the user logs in, the firewall maps the **username to the IP**.

Threat Prevention Technologies (Firewall Features)

These features are all about **protecting your network** from viruses, malware, hackers, and data leaks.

1. *Antivirus*

- **Stops viruses, worms, Trojans** (common malware).
- Works **in real-time**, scanning data as it flows through the firewall.
- Protects many protocols:
  `HTTP`, `SMTP`, `IMAP`, `POP3`, `FTP`, `SMB`
- Blocks infected files **before they reach the user**.

---

2. *Anti-Spyware*

- Stops spyware from **talking to hacker-controlled servers** (called C2 servers).
- Detects malware trying to **send data out** of your network.
- Blocks things like **keyloggers**, **browser hijacks**, and **remote control tools**.

---

3. *Vulnerability Protection*

- Blocks **attacks that try to exploit software bugs**, like:
  - Buffer overflows
  - Remote code execution
  - Denial of Service (DoS)
- Protects against attacks trying to **enter** the network.
- Complements Anti-Spyware, which protects what's already **inside**.

---

4. *URL Filtering*

- Every website belongs to a **category** (e.g., Social Media, Malware Sites, Adult, etc.).
- The firewall can:
  - **Allow** (whitelist)
  - **Block** (blacklist)
  - **Warn** or **log** based on category

- Helps stop users from visiting **malicious or phishing websites**.

5. *File and Data Filtering*

- Controls what types of files are allowed in or out (e.g., `.exe`, `.pdf`, `.zip`)
- Filters files **inside applications** (e.g., block file upload in WhatsApp Web but allow chat)
- Can detect and block **sensitive data** like:
  - Credit card numbers
  - Social Security numbers
  - Custom keywords or patterns
- Helps prevent **data leakage** or **unauthorized file transfers**.

☁ *WildFire Analysis –*

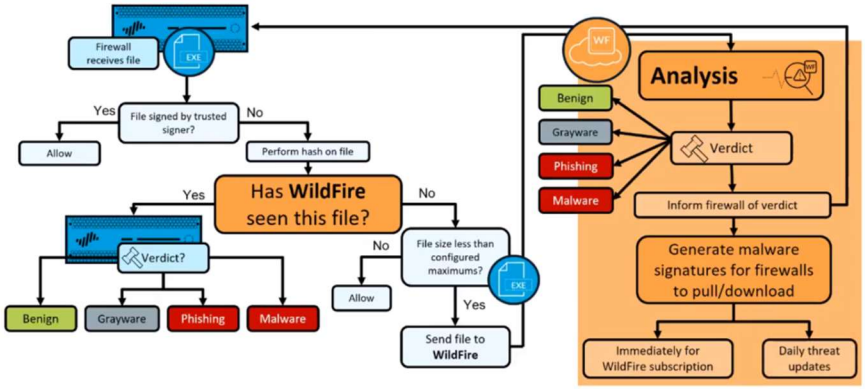
What is WildFire?

WildFire is a **cloud-based** system used by Palo Alto Networks firewalls to detect **unknown or new malware**.

Instead of only relying on **known virus signatures**, it **analyzes the behavior** of suspicious files in a **safe virtual environment** (sandbox).

How It Works

1. A user downloads or receives a file (email, web, etc.)
2. The firewall checks:
   - Is this file already known to be good or bad?
   - If it's **unknown**, it is sent to WildFire.
3. WildFire runs the file in a **virtual machine** and watches what it does.
   - Does it try to **encrypt files** (ransomware)?
   - Does it try to **steal data** or **connect to a hacker server**?
4. If it acts like malware, it's **classified as malicious** and shared with other firewalls worldwide.



What It Protects Against

- ✓ **Zero-Day Exploits** – brand-new attacks no one has seen before
- ✓ **Advanced Persistent Threats (APTs)** – stealthy, long-term attacks
- ✓ **Unknown Malware** – files not yet identified in antivirus databases

Why It's Powerful

- ✓ Doesn't just look at **file names or signatures**
- ✓ It looks at **what the file actually does**
- ✓ Updates the global threat intelligence **in minutes**

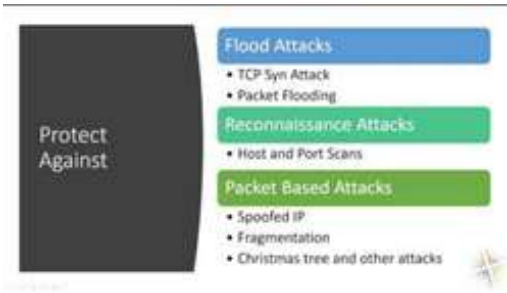
What is Zone Protection?

- **Zone Protection** is like a **security shield** at the **network edge** (your internet-facing zone).
- It protects against **Denial of Service (DoS)** attacks like:

1. **Flood attacks** (too many packets)
2. **Reconnaissance scans** (attackers scanning your network)
3. **Packet-based attacks** (malformed or spoofed packets)

---

1. *Flood Protection*



Flood attacks try to overwhelm a system with **too many requests**.
Palo Alto firewalls use two smart techniques to stop this:

1. *Random Early Drop (RED)*

- ✓ Used for **UDP, ICMP, and IP-based floods**.
- ✓ Once traffic crosses a certain threshold, the firewall **randomly drops** some packets to **reduce the load**.
- ✓ Think of it like a **traffic controller** that starts stopping a few cars early before a full traffic jam happens.

---

2. SYN Cookies

- ✓ Used for **TCP SYN flood attacks**.
- ✓ Works like a **traffic checkpoint**:

- When a device sends a **SYN** to start a connection, the firewall **doesn't forward it** right away.
- It replies with a **SYN-ACK** containing a hidden **cookie** (a kind of code).
- If the sender is **legit**, it replies with an **ACK + the cookie**.
- Then the firewall forwards the connection to the actual server.

✓ **Only valid traffic gets through**.

⚠ **Note**: Don't turn on SYN Cookies if your firewall's CPU is already heavily used—it may slow things down even more.

2.*Reconnaissance Protection*

Stop attackers from **scanning your network** to find open ports or active devices.

Types of Scans Blocked:

- **TCP Port Scan:** Scanning many TCP ports.
- **UDP Port Scan:** Scanning many UDP ports.
- **Host Sweep:** Scanning many IP addresses.

Actions Firewall Can Take:

- **Allow:** Let the scan happen (not recommended).
- **Alert:** Just **send an alert** if a scan happens (default setting).
- **Block: Drop packets** from the attacker for a short time.
- **Block IP: Block attacker's IP completely** for some time.

Key Settings:

- **Interval (sec):**
  Time window (like 60 seconds) to watch for scan activity.
- **Threshold (events):**
  Number of scan attempts (like 50 ports) before action is taken.
- **Source Address Exclusion:**
  IPs you **trust** (like IT admin systems) can be **excluded** from being blocked.
- Of course! Here's a **simple and short explanation** like before:
- Of course! Here's a **short and easy explanation** like before:
- ---

TCP and ICMP Drop Protection

Protect the network by **dropping weird or dangerous TCP and ICMP packets** that hackers might use.

TCP Drop Protection:

Check	*What It Means*	*What Firewall Does*
Mismatched TCP Segment	Overlapping bad TCP data	❌ Drops it
Split Handshake	Not using 3-way handshake properly	❌ Drops it
TCP SYN with Data	SYN packet wrongly contains data	❌ Drops it
TCP SYN-ACK with Data	SYN-ACK packet wrongly contains data	❌ Drops it
Reject Non-SYN TCP	First TCP packet is not SYN	❌ Drops it
Asymmetric Path	Out-of-order TCP packets	❌ Drops or Bypasses
TCP Timestamp	Remove extra timestamp info	🧹 Strips it out
TCP Fast Open	Remove fast open tricks from handshake	🧹 Strips it
MPTCP Options	Remove multi-path TCP options	🧹 Strips it

ICMP Drop Protection:

Check	*What It Means*	*What Firewall Does*
Ping ID 0	Ping with wrong ID (0)	❌ Drops it
ICMP Fragment	Broken up ICMP packet	❌ Drops it
Large ICMP (>1024B)	Oversized ICMP packet	❌ Drops it
Embedded Error	ICMP error inside another packet	❌ Drops it
Suppress TTL Expired	Stop sending "time expired" messages	🛑 Stops it
Suppress Frag Needed	Stop sending "need to fragment" messages	🛑 Stops it

3. *Packet-Based Attack Protection*

Protect the firewall and network from **bad or suspicious packets** that can cause harm.

What the Firewall Checks:

Attack Type	*What It Means*	*What Firewall Does*
Spoofed IP Address	Packet comes from the wrong place	❌ Drops it
Strict IP Check	Source or destination IP is wrong/malformed	❌ Drops it

Fragmented Traffic	Packet is broken into parts	✗ Drops it
IP Option Drop	Special IP tricks used in attack packets	✗ Drops them

---

Specific IP Options Blocked:

IP Option	*What It Does*	*Action*
Strict Source Routing	Packet tries to define its path strictly	✗ Drop
Loose Source Routing	Packet suggests a flexible path	✗ Drop
Timestamp	Packet tries to record time at each router	✗ Drop
Record Route	Packet records each router it passes	✗ Drop
Security	Special security tags in the packet	✗ Drop
Stream ID	Special packet stream IDs used	✗ Drop
Unknown	Unknown or suspicious packet options	✗ Drop
Malformed	Packet is incorrectly made (bad format)	✗ Drop

☑ The firewall **checks every packet** for anything **weird, wrong, or dangerous** and **drops it** immediately to protect the network.

Protocol Protection and Ethernet SGT Protection (Palo Alto Firewall)

Protocol Protection:

- ✓ Normally, firewalls allow **non-IP protocols** (old networking protocols) between **Layer 2** zones (like switches or virtual wires).
- ✓ Examples of non-IP protocols:
  ➔ **AppleTalk**, **Novell**, **Banyan**, **NetBEUI**, etc.
- ✓ **Protocol Protection** lets you **control**:
  - **Include** (allow) certain non-IP protocols
  - **Exclude** (block) certain non-IP protocols
- ✓ This keeps your network **clean and safe** from old/unwanted protocols.

Ethernet SGT Protection:

- ✓ In **Cisco TrustSec** networks, devices get a **Security Group Tag (SGT)** — a small ID tag (16 bits) attached at Layer 2.
- ✓ Firewalls can **read SGT tags** inside the Ethernet frames (Ethertype `0x8909`).
- ✓ You can **configure** the firewall to **block** packets **with unwanted SGT values**.
- ✓ Helps in **controlling which groups/devices** can enter specific network zones.

- ☑ **Protocol Protection** = Control old, non-IP traffic.
- ☑ **Ethernet SGT Protection** = Control access based on Cisco security tags at Layer 2.

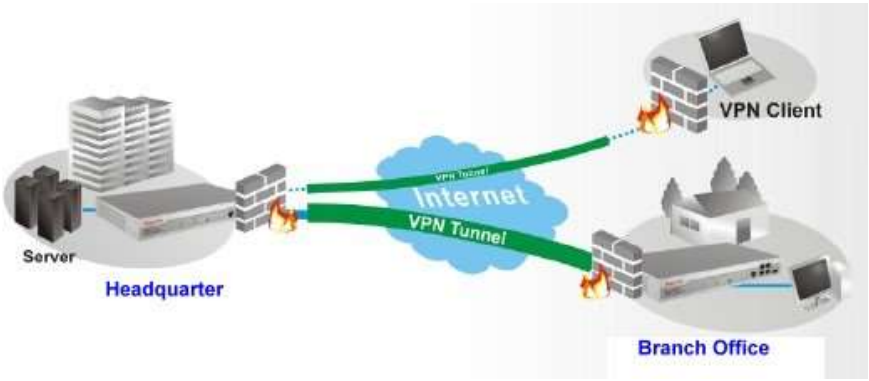
What is a VPN?

A **VPN** lets you **send private data** over the **public internet** in a **safe and secure way**.

Why We Need a VPN

Imagine you have two office branches in different cities.
They both use the **internet** to connect, but you don't want **anyone else** to see your company's internal traffic.

That's where **VPN** comes in.



How It Works

- A **VPN creates a secure tunnel** between two locations or users.
- All your data is **encrypted** (locked) before it leaves.
- Even if someone on the internet intercepts it, they **can't read it**.
- On the other end, the data is **decrypted** (unlocked) safely.

What VPN Provides

- **Data Confidentiality** → Keeps your information **private**
- **Data Integrity** → Makes sure your data is **not changed or tampered with**
- **Lower Cost** → Uses **public internet** instead of expensive leased lines
- **Secure Remote Access** → Allows employees to **connect securely** from anywhere

Example Use Cases

- ✓ Connecting office branches securely
- ✓ Allowing remote workers to access company files safely
- ✓ Protecting data when using public Wi-Fi (like in cafes or airports)

Types of VPN Connections

When using a VPN, there are mainly **two types** based on your description:

1. *Site-to-Site VPN*

- **Purpose:** Connects **whole office networks** together (for example, HQ to branch offices).
- **How:**
  - Each office (HQ and branches) has its own firewall/router.
  - A **VPN tunnel** is created between the devices over the **internet**.
- **Result:**
  - It feels like all offices are part of **one big private network**, even though they are in different cities.

Example from your case:

- **Headquarters** in Bangalore
- **Branch Office Pune**
- **Branch Office Delhi**
  All connected with **VPN tunnels** securely through the internet.

---

2. *Remote Access VPN*

- **Purpose:** Connects **individual users** (working from home, traveling, etc.) securely to the company's internal network.
- **How:**
  - The user's laptop or phone runs a **VPN client** software.
  - It creates a **VPN tunnel** directly to the **HQ (Data Center)**.
- **Result:**
  - The remote user gets **secure access** to company resources, just like sitting inside the office.

Example from your case:

- A remote employee connects to the **Data Center in Bangalore** over the **internet** using a **VPN tunnel**.

Summary Table

TYPE	WHO CONNECTS	PURPOSE
SITE-TO-SITE VPN	Office to Office (HQ ⇄ Branch)	Connect entire networks
REMOTE VPN	User to Office (Laptop ⇄ HQ)	Secure access for individuals

What is Cryptography?

Cryptography is the **science of securing information** so that only the **right people** can read or understand it.
It protects your data when you're sending it over the internet or storing it somewhere.

Key Terms in Cryptography

Term	*Simple Meaning*
Encryption	Turning normal data into **secret code** using a key.
Decryption	Turning the **secret code back to normal data** using a key.
Plaintext	The **original data** before encryption (readable).
Ciphertext	The **encrypted version** of the data (looks like random text).
Hash	A **unique digital fingerprint** of the data, created using a math formula. It can't be reversed back to the original data.

Two Types of Encryption

1. *Symmetric Encryption*

- Uses the **same key** to encrypt and decrypt data.
- Example: You lock and unlock a box with **one single key**.
- **Fast** and uses **less data**.

⚠ **Problem**: How do you **safely send the key** to someone else?

2. *Asymmetric Encryption*

- Uses **two keys**:
  - **Public key** to encrypt
  - **Private key** to decrypt
- Example: Anyone can **lock** the box using your public key, but only **you** can **unlock** it with your private key.
- **Very secure**, especially for sharing over the internet.

⚠ **Slower** and the encrypted message is **larger in size**.

What is Cryptography?

- Cryptography is a way to **secure communication**.
- It **hides** information from hackers and makes sure only the right people can see it.

Important Terms:

- ✓ **Encryption:** Turning normal data (**plaintext**) into **secret code** (**ciphertext**) using a **key**.
- ✓ **Decryption:** Turning the secret code (**ciphertext**) back into **original data**.
- ✓ **Plaintext:** Normal readable data.
- ✓ **Ciphertext:** Encrypted, unreadable data.
- ✓ **Hash:** A special unique number created from data. (Used for verifying data integrity.)

Types of Encryption:

Symmetric Encryption	***Asymmetric Encryption***
Same key for encrypt & decrypt	Key pair (Public Key + Private Key)
Fast	Slower
Small ciphertext	Bigger ciphertext
Problem: How to safely share the secret key?	No key sharing problem (public key can be shared freely)
Example: AES, DES, 3DES	Example: RSA, DSA, ECC, DH

Popular Encryption Algorithms:

Symmetric Algorithms:

- **DES:** Old, 56-bit key (weak today)
- **3DES:** Stronger, uses 3 keys
- **AES:** Modern, very strong (128/192/256-bit key)

Asymmetric Algorithms:

- **RSA:** Very popular for secure communication
- **DSA:** Used for digital signatures
- **ECC:** Newer, faster, smaller keys
- **DH (Diffie-Hellman):** Used for securely exchanging keys

In Short:

Symmetric = one key, Asymmetric = two keys (public/private).

AES is the best for fast encryption, **RSA/ECC** are best for secure key exchange.