[08-02-2021]

- Level of configuration:

  PCCSA → PCNSA (EDU-110/210) → PCNSE 114/214

➢ Security Operating Platform and Architecture

Reconnaissance
Weaponization (which method to use to deliver malicious payload)
Delivery
Exploitation
Installation (maintaining access or privilege escalation)
Command and Control
Act on the objective

➢ Security Operating Platform and Architecture

Cortex: cloud-based, no infrastructure (Data Lake + XDR)
XDR significa rilevamento e risposta multi-livello. XDR raccoglie e correla automaticamente i dati tra più livelli di sicurezza (email, endpoint, server, workload in cloud e rete), in modo che le minacce possano essere rilevate più rapidamente e gli analisti di sicurezza possano migliorare i tempi di indagine e risposta

- Network security
- Advanced endpoint protection
- Cloud Security

➢ Additional products Palo Alto

- Panorama
- Prisma SaaS (protects cloud-based application such as Box, Drop Box, Salesforce and so on)
- Global Protect (safeguards mobile workforce by inspecting all traffic using next generation firewall that are deployed as internet gateways, SSL VPN)
- Autofocus (gathers information about vulnerability and threats and analyze it with the help of Unit 42 for example)
- Mine Meld

➢ Next-generation firewall Architecture

- Control plane vs Data plane
- Physical platforms next generation firewalls
  - PA-5200 Series (5280 with PAN-OS/8.1 with double data-plane memory)
  - PA-3200 Series
  - PA-800 Series
  - PA-220/R
  - PA-7000

➢ Initial Configuration

- Default MGT IP:
  - 192.168.1.1
  - VM series firewall: obtain IP through DHCP
- Initial configuration must be performed using either:
  - Dedicated out-of-band management Ethernet interface MGT port
  - Serial Console

- Default access: <admin: admin> stored locally but encrypted
- Administrative access:
  - WEB
  - SSH
  - Panorama (manage multiple firewalls, aggregate data from firewalls)
  - REST XML API (Palo alto offers → https://<ip_firewall>/api)

❖ Reset to factory configuration
- **request system private-data-reset**
  - erase all logs, reset all settings, restore default configuration after changed MGT IP
- without username and password

maint -> Restore to default settings

❖ Web Interface
- Device -> Setup -> Interface -> Management

❖ Configure general settings
- Hostname: max 31 chars alphanumeric, hyphen, underscore (default: model name)
- Domain: max 31 chars alphanumeric, hyphen, dot (default: empty)
- DHCP options if enabled on MGT interface resolves and configure hostname and domain with DHCP
- SSL/TLS firewall requires a digital certificate that is trusted by clients
- DNS & NTP (if there is a DHCP get automatically)
- It's possible to configure an additional port in band (labeled PORT)
- 

❖ Configuration management
- Running configuration (running-config.xml)
- Candidate configuration (modifications are made on candidate-configuration.xml)
- Candidate -> Commit -> Running

❖ PAN-OS supports RADIUS, Active Directory, LDAP, RADIUS and TACACS+

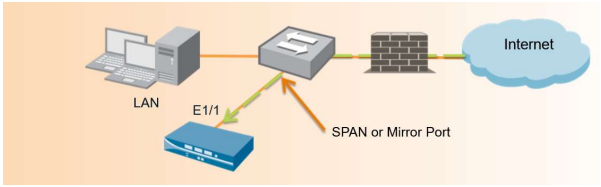
➢ Security Zones & Security Policy

❖ Traffic between zones denied by default

❖ Tunnel zones aren't defined in this course

➢ Interface configuration

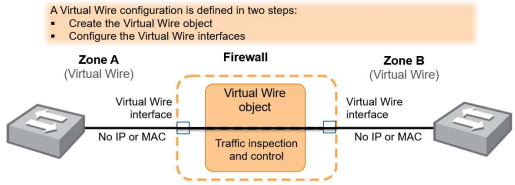
❖ TAP INTERFACE:



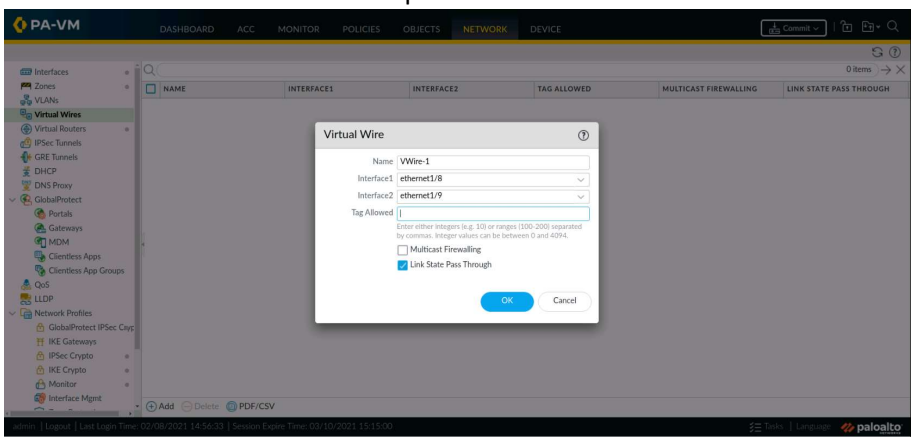
- Used to connect to a switch's SPAN or mirror port, passively collect and logs monitor traffic

- Information are recorder in the Traffic log
- Cannot be used to block traffic or perform traffic shaping
- Pro: doesn't require any network address changes
- Cons: only support SSL INBOUND DECRYPTION

❖ VIRTUAL WIRE INTERFACE (Bump in the wire/Transparent inline deployment)

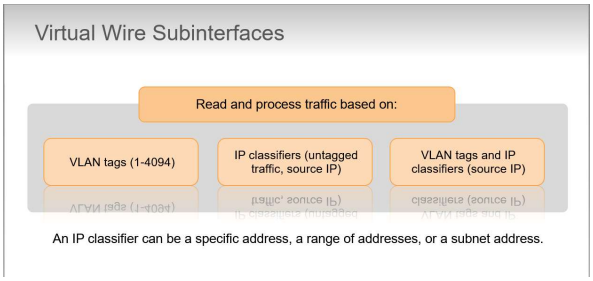


- No MAC/IP is assigned to either Virtual Wire interface
- Used typically when no switching or routing is required
- A virtual wire requires no changes to adjacent network devices.20 gen 2021
- All firewall has by default Ethernet ports 1 and 2 preconfigured as a virtual wire interfaces and these interfaces allow all untagged traffic
- Network traffic flows through a firewall in virtual wire → examine, traffic shape & block
- Virtual wire doesn't support switching or routing because doesn't have IP
- Cannot function as a termination point for IPSec VPN tunnel

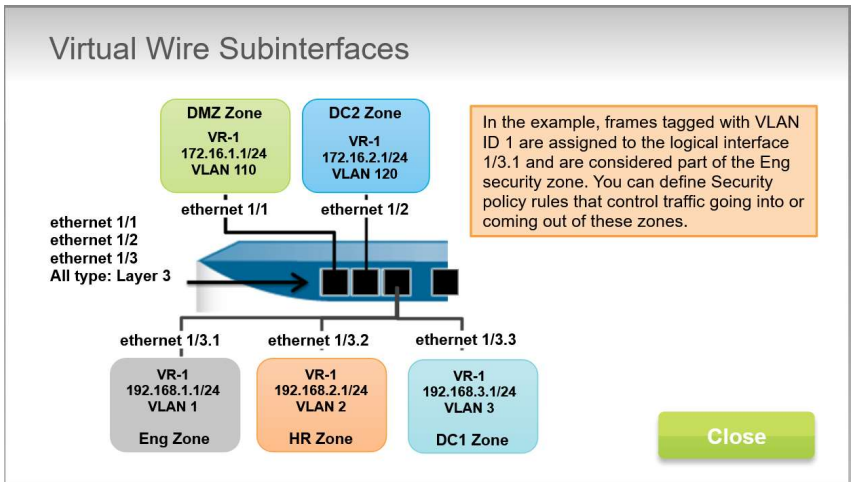


> If we specify **Tag Allowed** only vlan with these tags will be allowed on this virtual wire

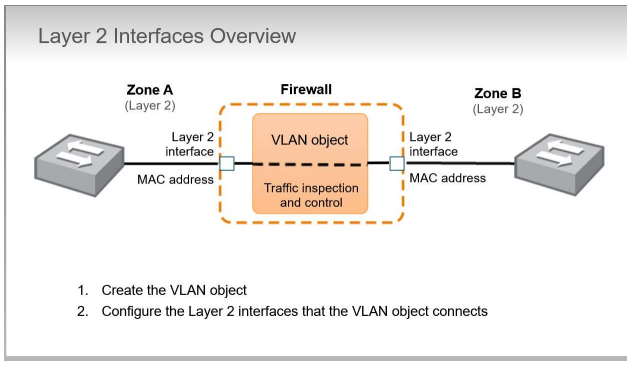
> Link state pass through: checked by default simply pass those messages to one interface from another devices that is on the other side of virtual wire



> We can create multiple Virtual Wire sub interfaces that will read and classify traffic according to an administrator-defined VLAN tag, IP classifier or both

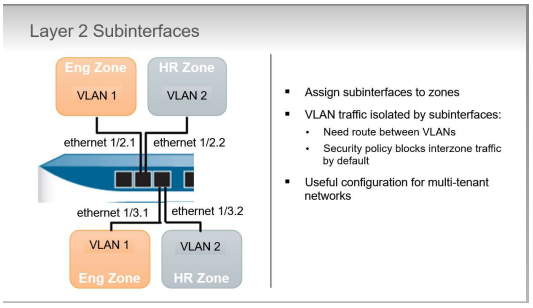


- ❖ LAYER 2 INTERFACES



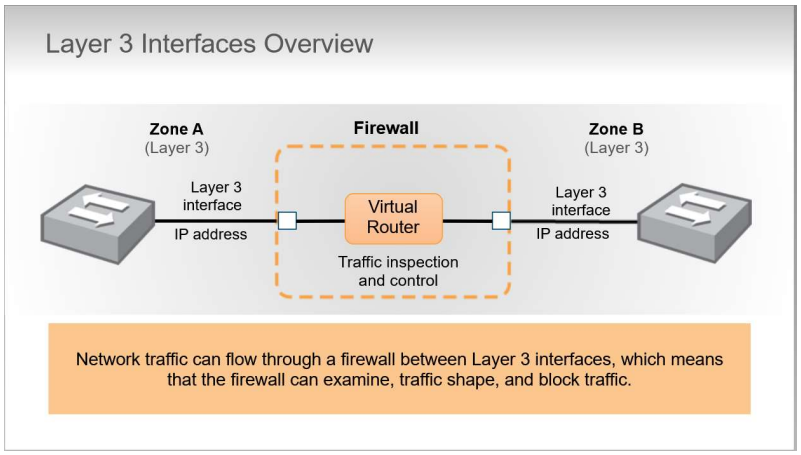
- VLAN Object connects the interfaces into a single Ethernet broadcast domain
- Firewall not participate in STP however from external switches STP packets are forwarded to other external switches
- Network traffic flows through a firewall between Layer 2 interfaces, which means that the firewall can examine, traffic shape and block

- ❖ LAYER 2 SUBINTERFACES

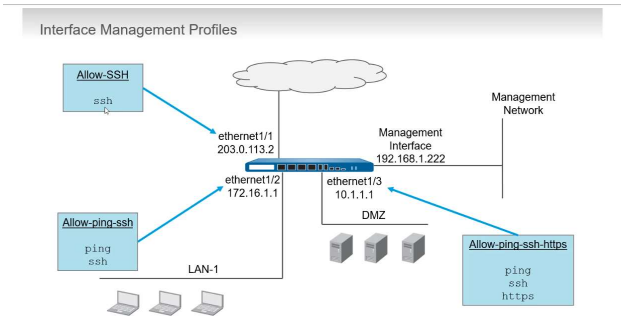


- Traffic in different VLANs can share a common physical firewall port but traffic between separate them is blocked by default
- BEST PRACTICE: use Layer 3 sub interfaces with each Layer 3 sub interface assigned to a VLAN rather than to use VLAN objects and Layer 2 sub interfaces. Layer 3 sub interfaces provides isolation at Layer 2 yet provides a routing path between networks at the IP layer.

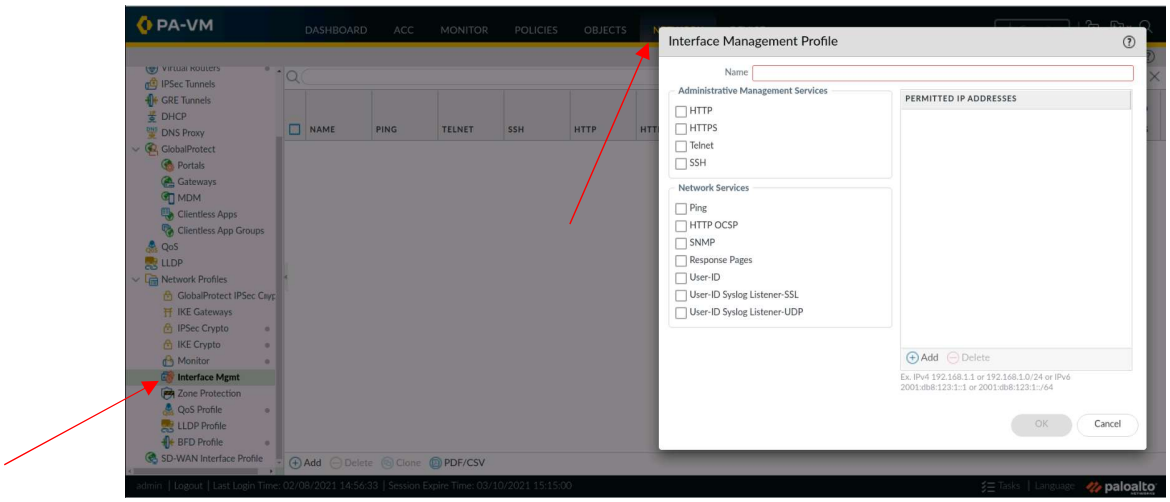
❖ LAYER 3 INTERFACES:



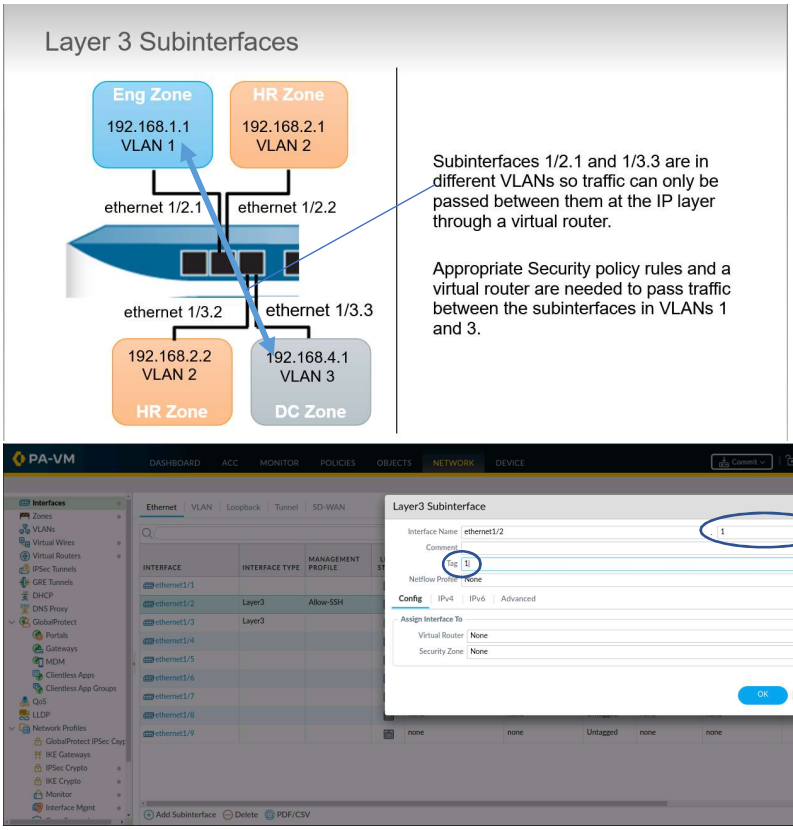
- Layer 3 deployment enables routing traffic between multiple Layer 3 interfaces
- We've to assign an IP address to each interface (we can have network reconfiguration in enterprise)
- Routing between Layer 3 interfaces requires a router. In the figure we've an internal Virtual Router
- A Layer 3 interface can support firewall management traffic because have an assigned IP address
- Support both IPV4 and IPV6 (can be deployed separately or in dual-stack)
- **Interface Management Profile: determines which firewall services are accessible from external devices**



Configuration of **Network profiles**:

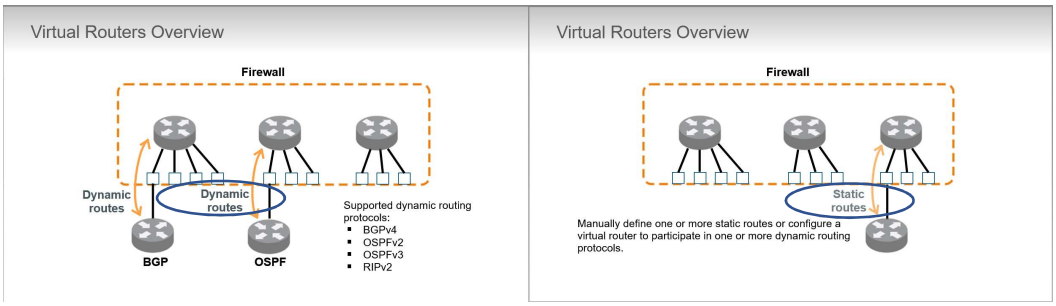


❖ LAYER 3 SUBINTERFACES:

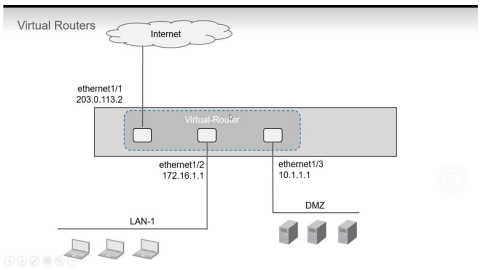


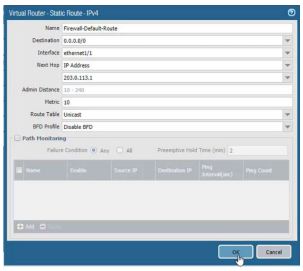
> id of sub interface and tag may not match, IS THE NUMBER INSERTED IN THE TAG THAT DETERMINES WHICH VLAN WE ARE ASSIGNING TO THE SUBINTERFACE

❖ VIRTUAL ROUTERS:

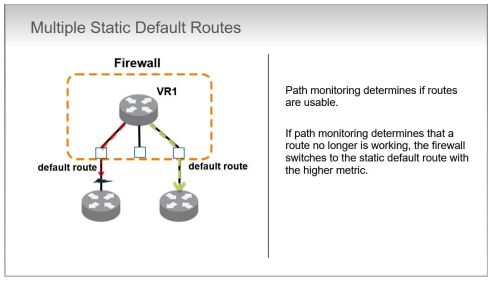


- Supported multicast routing protocols:
  - PIM-SM
  - PIM-SSM
  - IGMPv1, v2, v3 also supported on host-facing interfaces
- Virtual router is needed when we configure LAYER 3 INTERFACES:



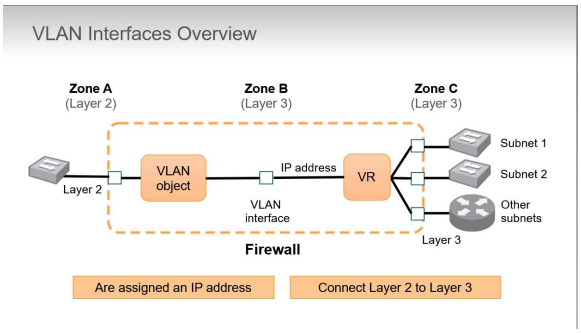


- We can also configure multiple static default routes



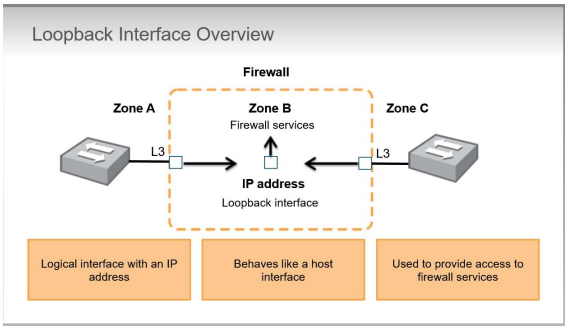
> **path monitoring** continues to monitor all paths, even after a failure. Path monitoring that detects that the static default route with the lower metric is available again will cause the firewall to switch back to that route path.

❖ VLAN INTERFACES:



Networks attached to Layer 2 interfaces and a VLAN object can be attached to a virtual router through configuration of a VLAN interface. You assign a VLAN interface,an IPv4/6 address and attach it to a virtual router which provides a routable path from the firewall's Layer 2 interfaces to the firewall's Layer 3 interfaces

❖ LOOPBACK INTERFACES:

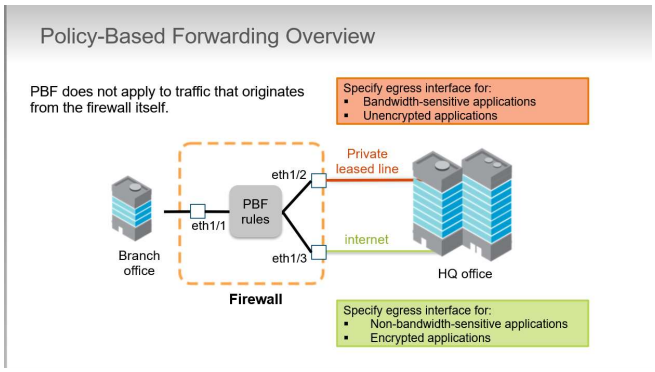


Logical interface reachable through a physical/subinterface.

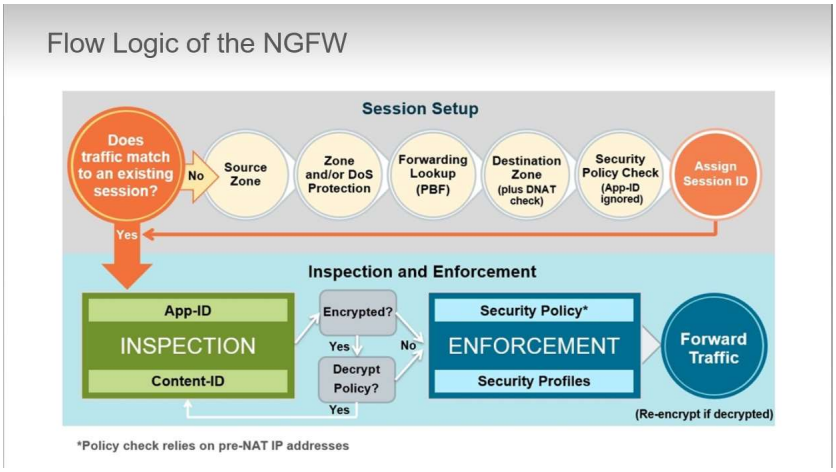
Loopback interface is the access point to the web interface usign HTTPS, GlobalProtect Portal or Gateway services

❖ POLICY BASED FORWARDING:

- PBF rules allow traffic to take an alternative path from the next hop specified in the route table and are used to specify an egress interface for security or performance reasons

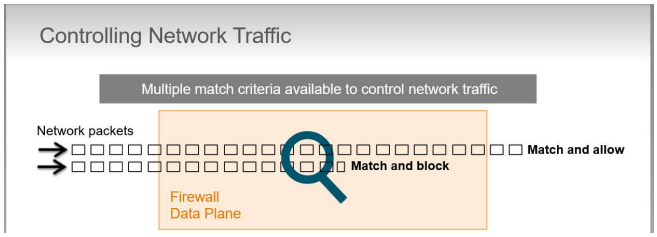


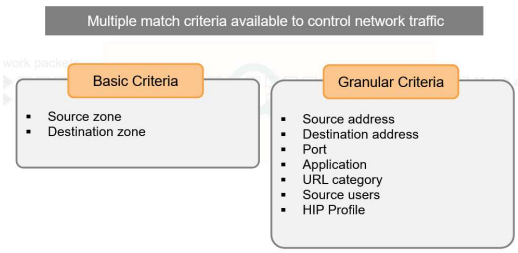
➢ Security and NAT policies



> show a simplified version of the flow logic of a packet traveling through a Palo Alto firewall.

❖ Security policy fundamental concepts:

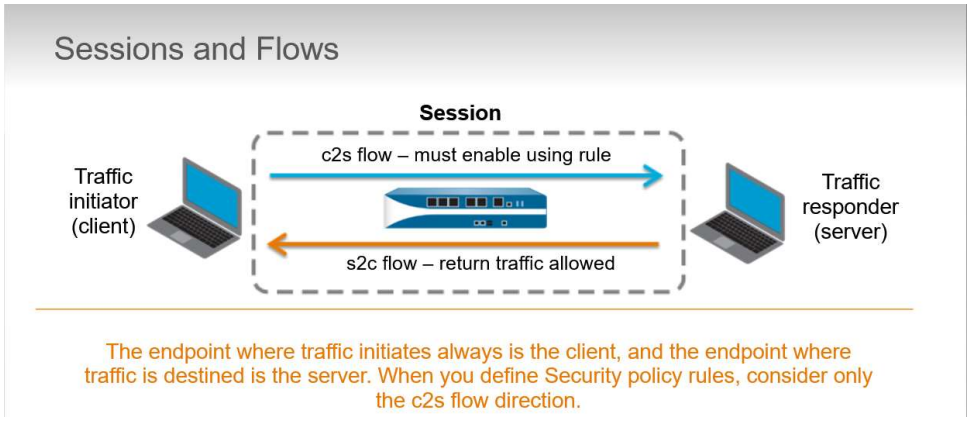




- All traffic traversing firewall is matched against a Security Policy, this traffic matching doesn't include traffic originating from the management interface of the firewall because by default this traffic isn't passed through data plane
- Security policy rules can be defined using:
  - Zones
  - Applications
  - IP addresses
  - Ports
  - Users
  - Host information profile (HIP profile)
- Stateful firewall: all traffic passing through the firewall is matched against a session and each session is then matched against a Security Policy rule.
- Session (**have a unique id number → UUID)** is a six-tuple consisting of:

- Source and destination IP address
- Source and destination Port number (for non UDP/TCP traffic different protocol fields are used)
- Protocol
- Source security zone

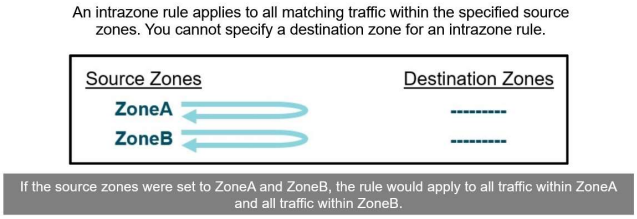
- Each session can consist of 2 type of flows:



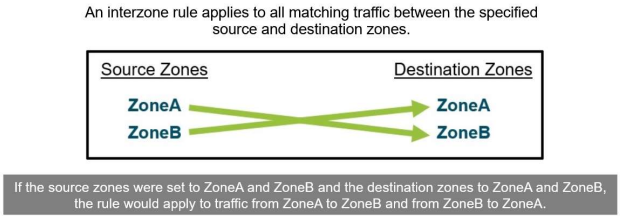
> client-to-server flow (c2s)
> server-to-client flow (s2c)

defines policy rules that allow or deny traffic from the source zone to the destination zone, that is in the c2s direction. The return s2c flow does not require a separate rule because the return traffic automatically is allowed

- Security policy Rule Types:
  - Intrazone



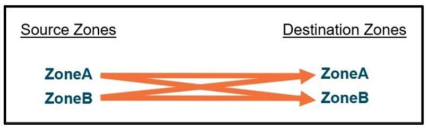
  - Interzone



    The rule wouldn't apply to traffic within ZoneA or ZoneB

  - Universal

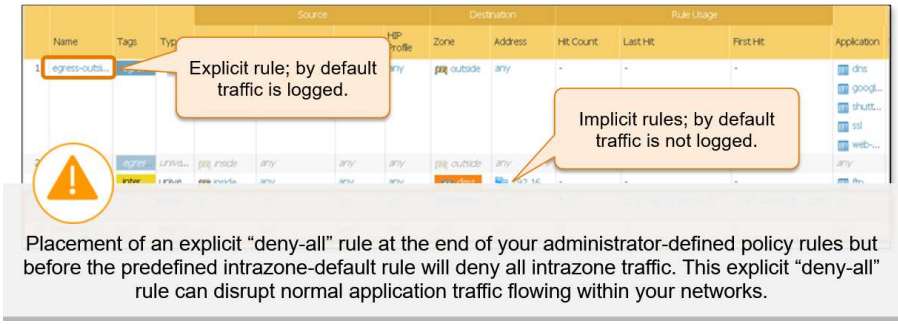
A universal rule applies to all matching interzone and intrazone traffic in the specified source and destination zones.



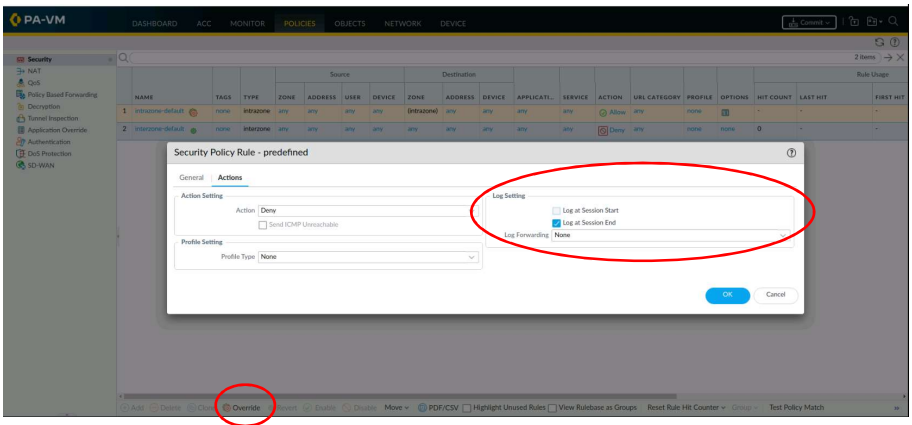
For a universal role with source zones ZoneA and ZoneB and destination zones ZoneA and ZoneB, the rule would apply to all traffic within ZoneA, all traffic within ZoneB, all traffic from ZoneA to ZoneB, and all traffic from ZoneB to ZoneA.

- Implicit and Explicit rules:
  - By default firewall implictly allow intrazone traffic and implictly denies interzone traffic
  - These implicit rules are processed after all the explicit administrator-defined rules on the firewall and match traffic that has not matched any other Security policy rule.

Palo Alto Networks recommends that you log all traffic and change the default behavior.



Placement of an explicit “deny-all” rule at the end of your administrator-defined policy rules but before the predefined intrazone-default rule will deny all intrazone traffic. This explicit “deny-all” rule can disrupt normal application traffic flowing within your networks.

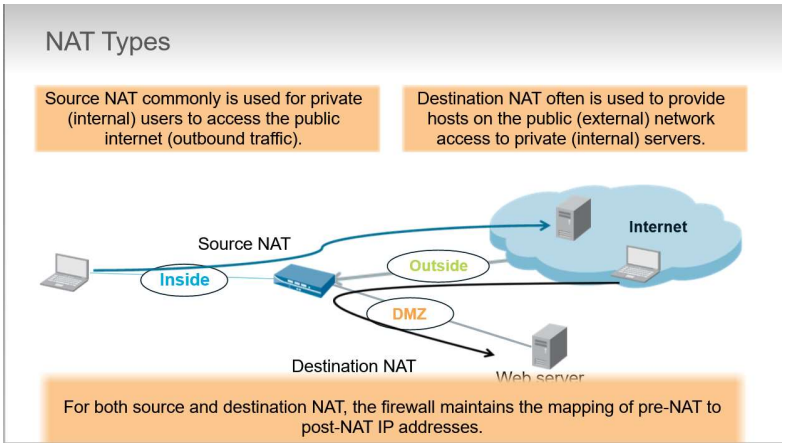


To override default behaviour of this predefined rules to, for example, log traffic intrazione click on Override -> Actions

- Security policy match:
  - Evaluated for a match from top to bottom
  - Are unidirectional, only in the direction specified with source and destination zone
    - Source zone → Destination zone
    - Replies are always allowed
    - If traffici s intended to be initiated in both directions, 2 policy rules are recommended

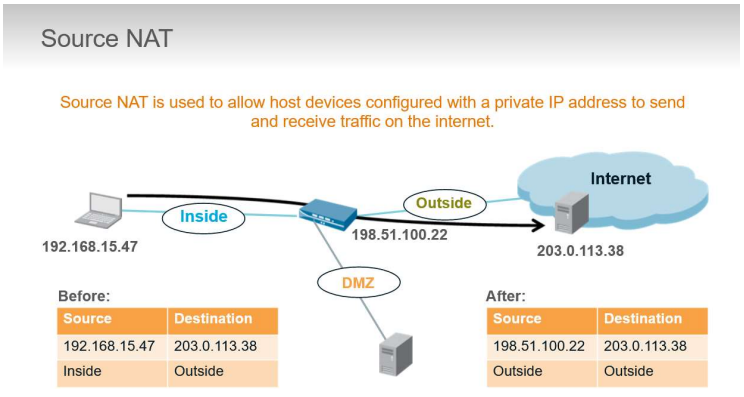
- Minimize *any* in the columns

❖ Security policy fundamental concepts:



- NAT configuration can take 2 forms, that are directional and described from the perspective of the NAT device, firewall:
  - Source NAT: translate address of outbound traffic
    PRIVATE NETWORK → INTERNET
  - Destination NAT: translate address of inbound traffic
    INTERNET → PRIVATE NETWORK

❖ Source NAT configuration:



Source NAT changes source address of packets that match NAT policy

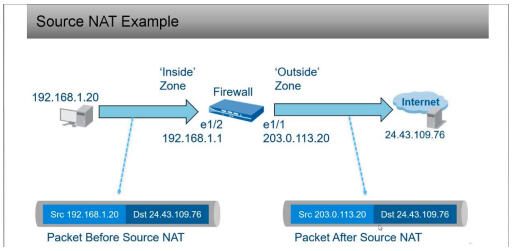
Can also change source port number

Is commonly used to allow host devices configured with private IP address to send and receive traffic on the internet

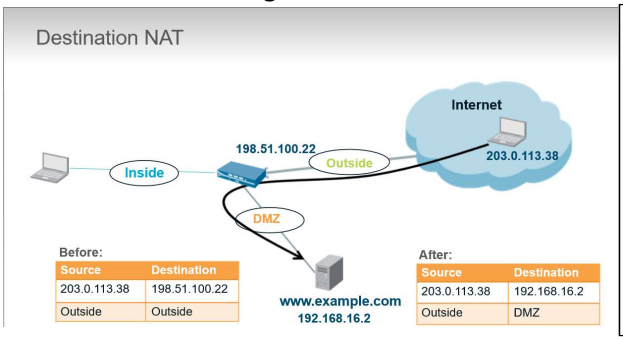
Without this translation, ISP carrier would be discard traffic from private network because see a private address

- Source NAT types provide administrator different options for setting the size and nature of the translated source address pool. Firewall supports 3 ways of provisioning a translated source address pool:
  - STATIC IP: is used to change the source ip address by leaving source port unchanged. **Use of bidirectional option in static source NAT rules implictly creates a destination NAT rule for traffic to the same resources in reverse direction**

- DYNAMIC IP: private source address are translated to next available address in the range specified. If the pool of available IP to NAT is exhausted we can switch to DIPP
- DYNAMIC IP AND PORT (DIPP): allows multiple client use same public ip address with different source port number



❖ Destination NAT configuration:

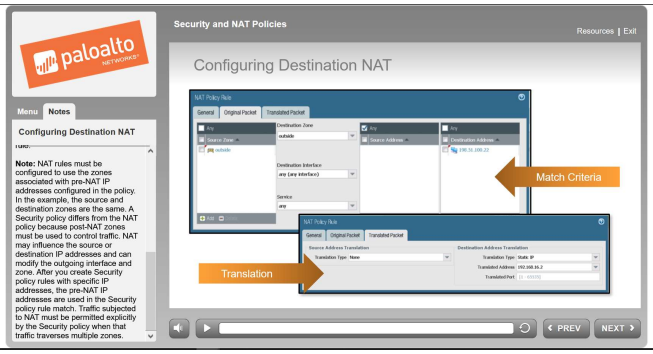


Destination NAT change destination address in IP header of packets that match NAT policy and is commonly used to make a server within a private network reachable from the public internet.

User from external system with IP address 203.0.113.38 queries DNS server for IP address of web server www.example.com. DNS server return an address of 198.51.100.22 which is the external address of the firewall interface in the Outside zone.

For the packet to reach the web server, the destination IP address , must be translated to the private IP address 192.168.16.2

Esempio:

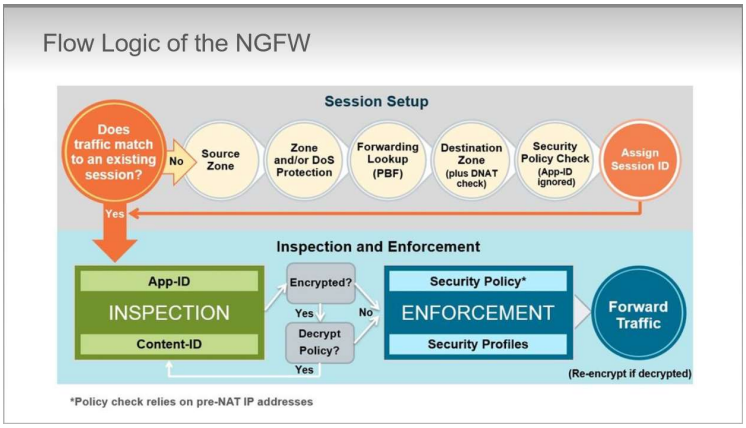


source == destination zone perché per come funziona il firewall ha bisogno di fare un secondo lookup, quindi quando la prima volta riceve il pacchetto con l'IP pubblico, se non mettessimo che la Destination Zone è la outside, non potrebbe fare questo 2° lookup e compiere il dynamic nat sull'IP pubblico <-> IP privato.

>show running nat-policy # per mostrare da CLI tutte le policy

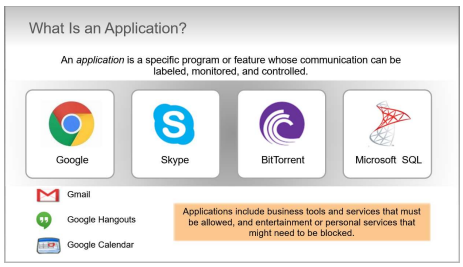
➢ App-ID

❖ Application Identification (App-ID):



- After initial processing is complete, Palo Alto examines traffic to accurately apply the Security policy rules.
- Firewall can classify traffic by port as does traditional firewall, next-generation firewall is designed to examine application associated with the traffic to provide more granular control over data on your network

❖ Overview:



- App-ID use multiple identification mechanism to determine the exact identity of application traversing the firewall

- Today's applications can easily bypass a port-based firewall by hopping ports, using SSL/SSH encrypted traffic, sneaking across port 80 or using non-standard ports.

Port-based security rule

Allows any traffic from the private zone to the public zone as long as it is going to ports 20 and 21

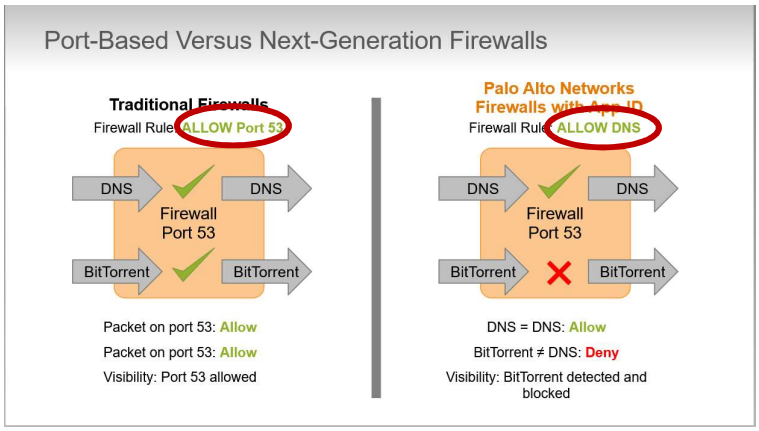
	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Application	Service	Action
1	FTP	egress	universal	inside	any	any	any	outside	any	any	service-ftp	Allow

Application-based security rule

Allows only FTP traffic from the private zone to the public zone that is going to ports 20 and 21

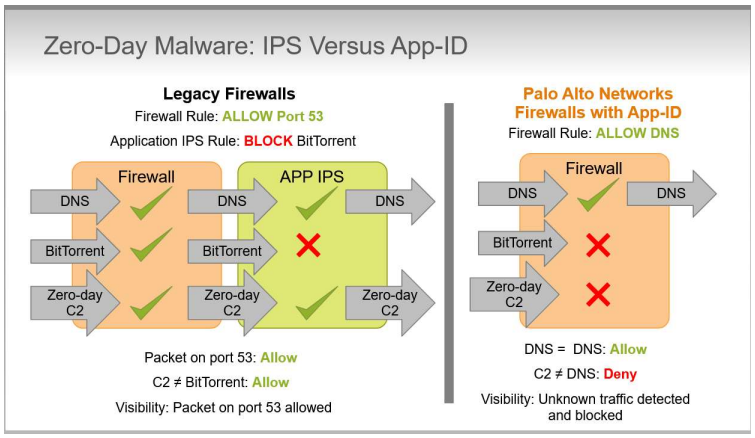
	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Application	Service	Action
1	FTP	egress	universal	inside	any	any	any	outside	any	ftp	application-default	Allow

- **Port-based** security policy rule allows *any* traffic from the private zone to the public zone as long as it's going to ports 20 and 21 (as defined in the service service-ftp). The actual traffic might or might not be TFP traffic. **Application-based** security policy rule allows *only* FTP traffic from the inside zone to outside zone that is going to ports 20 and 21



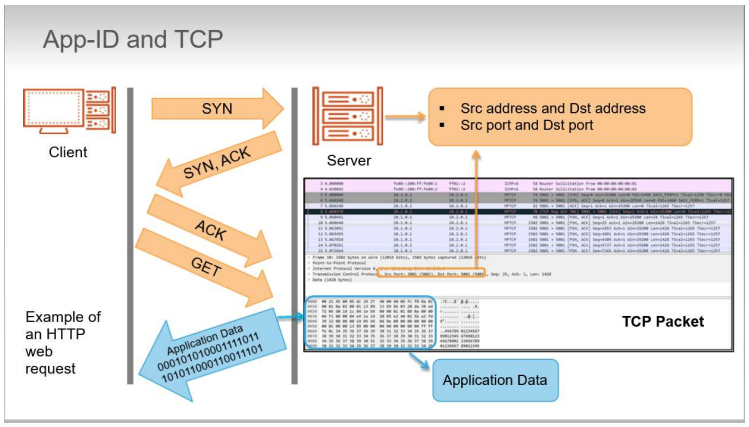
If we configure the firewall Security Policy rule to use the application-default port, then the firewall allows only DNS traffic on port 53 and denies all other non-DNS traffic on this port.

In this way PAN protects network from evasive applications that switch ports or use non-standard ports.



The Zero-Day virus using port 53 is allowed through the firewall because it's using an allowed port and is not BitTorrent. Because is a Zero-Day, virus is also allowed by IPS because is not specifically blacklisted yet by the IPS. No logs are generated to identify this occurrence.

The Palo Alto firewall is configured to allow only DNS application traffic. Even if the zero-day malware is unknown to PAN-OS software, it still is not allowed to pass because it has not been specifically identified as the DNS application. Also, the blocked traffic is logged.

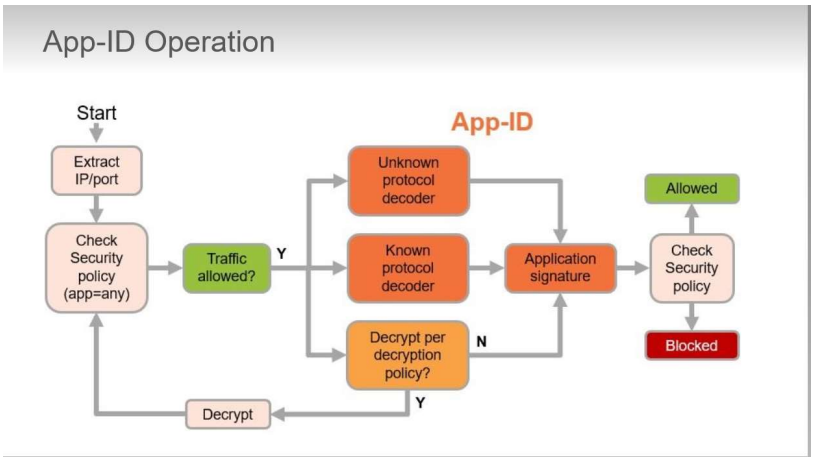


Applications that use TCP requires multiple packet transfers to identify an application. The first packet in this example doesn't contain application data. Firewall might have to examine the fifth packet before App-ID can detect either the application or the presence of encrypted traffic. If traffic is encrypted firewall must evaluate the administrator-defined Decryption policy to determine what to do next.

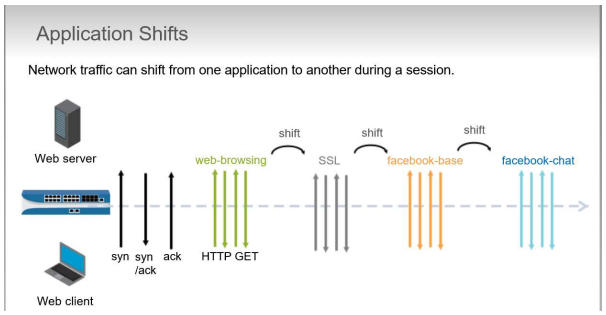
Depending on the configured policy traffic could be allowed or blocked in either encrypted or decrypted form.

- Palo Alto App-ID uses 4 major techs to help identify applications:
  - **Application Signature**: database of application signatures updated as part of the firewall content updates
  - **Unknown Protocol Decoder**: heuristics engine used to look at patterns of communication. It attempts to identify the application based on its network behavior. Is required for example for application that use proprietary e2e encryption.
  - **Known Protocol Decoder**: set of application decoders that understand the syntax and commands of common applications
  - **Protocol Decryption**: SSH and SSH decryption capabilities

- Operation:
  - Network traffic is classified based on IP and port. Consults Security Policy to determine if it should allow or block the traffic based on IP and port. During this initial Security Policy Check application is set to any
  - If traffic is allowed, session is created and App-ID search for an application signature. Use known/unknown protocol decoders to identify application
  - If traffic is encrypted and there is a Decryption policy traffic could be applied to the decrypted traffic to detect application signature. If application signature cannot be identified, traffic can be labeled as unknown-tcp or unknown-udp.
  - Finally firewall checks Security Policy to determine whether to block, allow or allow and scan for threats.

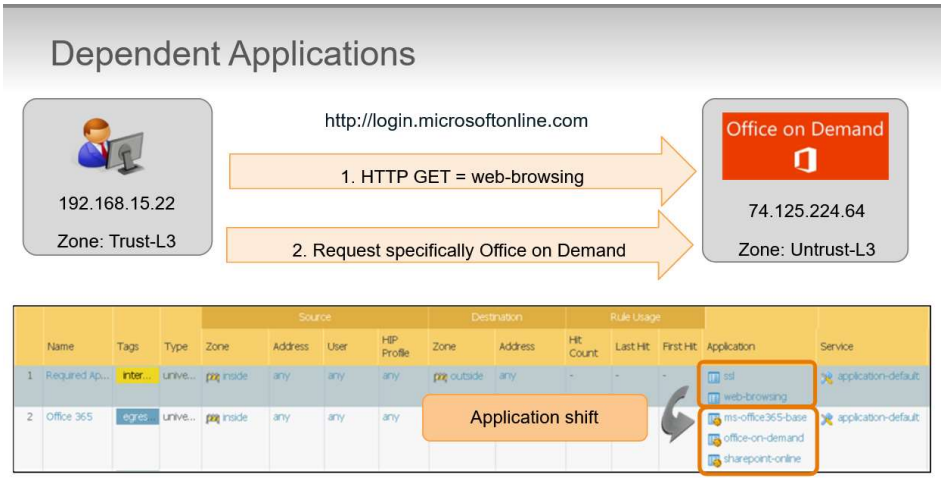


- Using App-ID in a Security Policy:
  - Application Shifts:
    - Network traffic can shift from one application to another during lifetime of a session.
    - App-ID cannot identify traffic from only TCP 3-way handshake
    - When HTTP-GET is reported, App-ID can report application as web
    - More packets receive and more App-ID is able to further classify traffic.



  - Dependent Applications:
    - Some applications can depends on ore or more other applications. Network traffic can shift from one dependent application to another during lifetime of a session.
    - When you create policy to allow dependent application, you also ensure that firewall allows other dependencies apps.
    - Joe want to access *Office on Demand* in another zone.

- App-ID find initially an HTTP GET which matches web-browsing application.
- First rule is matched →HTTP is allowed and rule about Office 365 isn't checked at this time because a matching rule has already been found
- **When Joe tries to access *Office on Demand* application shift in current session is initiated. App-ID engine detects shift and finds application signature for office-on-demand.**
- Firewall moves on the next rule. Order of 2 rules doesn't matter in this example because traffic that matches one rule cannot match other rule, so neither rule prevents other from being evaluated

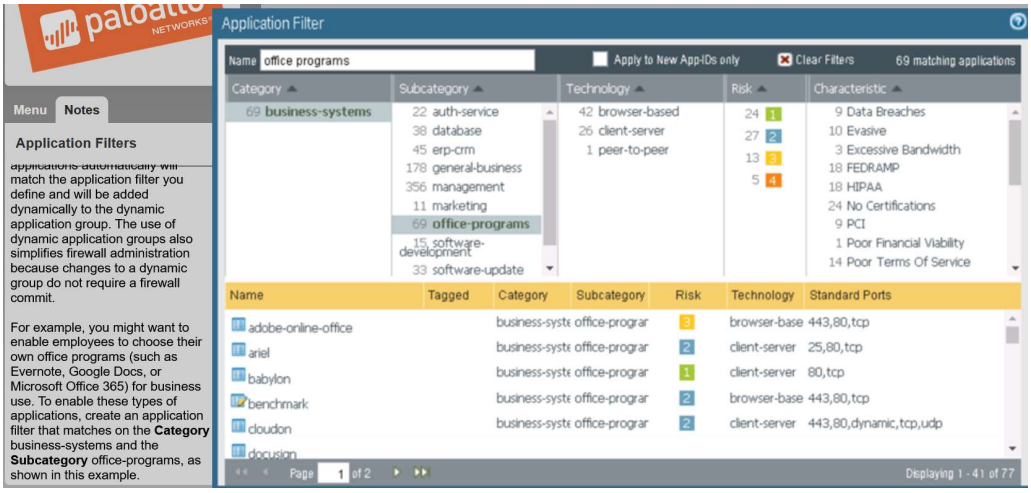


- Implicit Applications:
  - For many dependent applications, App-ID db implicitly allows required parent applications without need to explicitly add parent application to Security policy

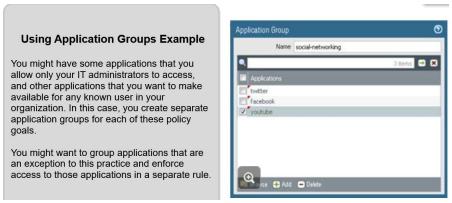
  - facebook-base application implicitly allows the required web-browsing applications without need for you to explicitly add web-browsing rule to Security Policy
  - facebook-chat and email depends on facebook-base so facebook-base explicitly must be added to the rules to enable users to chat or email using Facebook

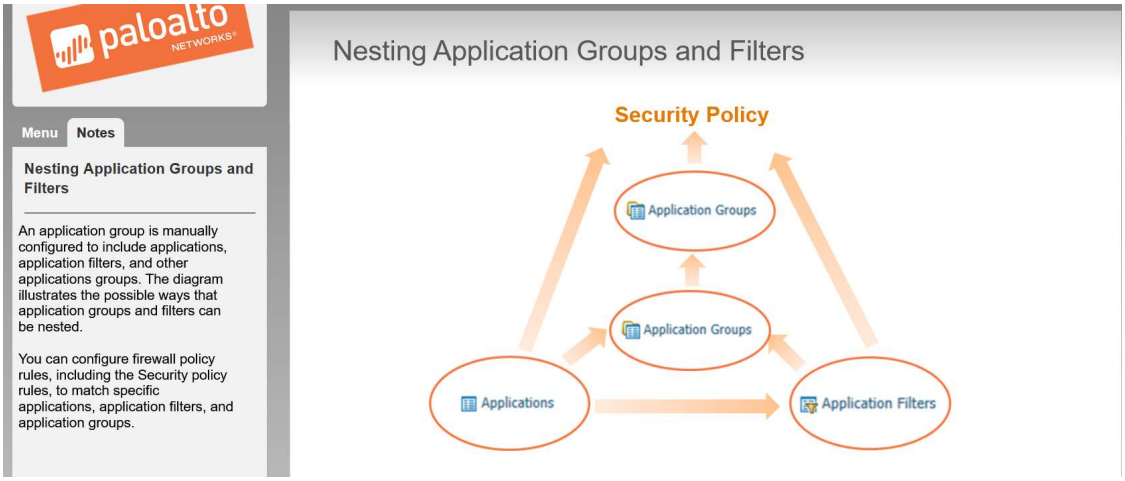
- Application Filters:
  - Object that dynamically groups applications based on application attributes that you select from App-ID db. Possible attributes are:
    - Category
    - Subcategory
    - Technology
    - Risk
    - Characteristic

- Useful when we want to enable access to applications that match filter criteria rather than match specific application names

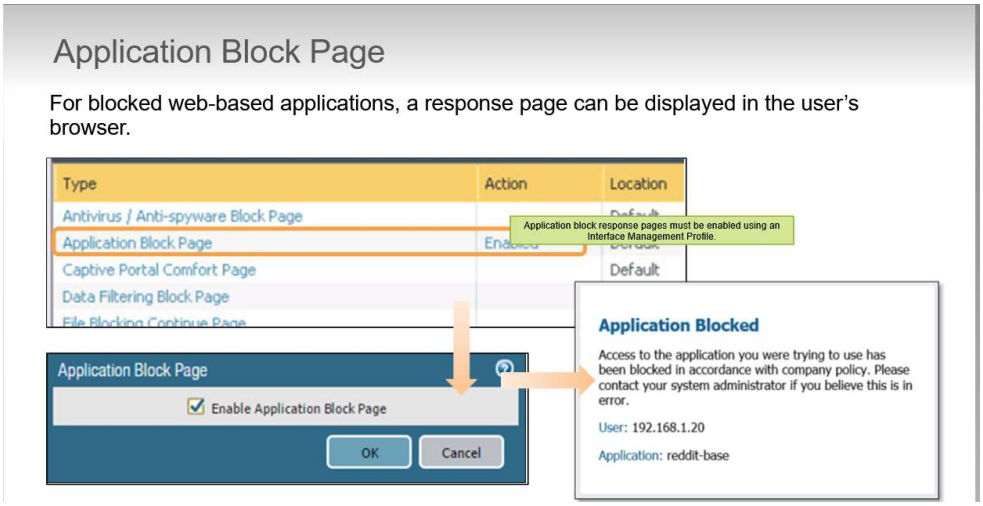


- Application Groups:
  - Is a static, administrator-defined set of applications.
  - Enable you to create logical grouping of applications that can be applied to Security, QoS and PBF policy rules.
  - Is used when we want to treat set of applications similarly in a policy.



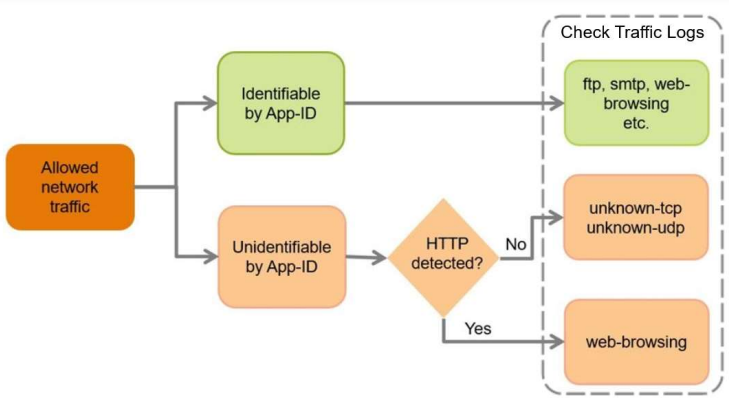


- Application Block Page:



❖ Identifying Unknown Application Traffic:

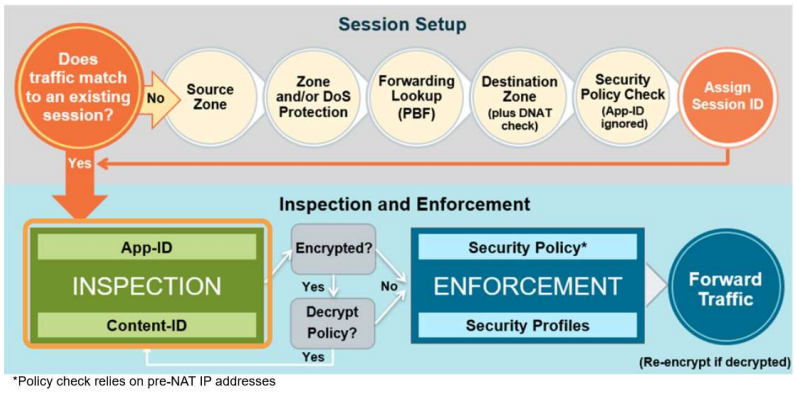
- Unknown Network Traffic:
  - First task after add firewall to network is identify network traffic.
  - Palo Alto is not a port-based firewall, identification of traffic → identification of applications traversing your firewall
  - Applications can be:
    - Known to App-ID: named in Traffic Log
    - Unknown to App-ID: unknown traffic



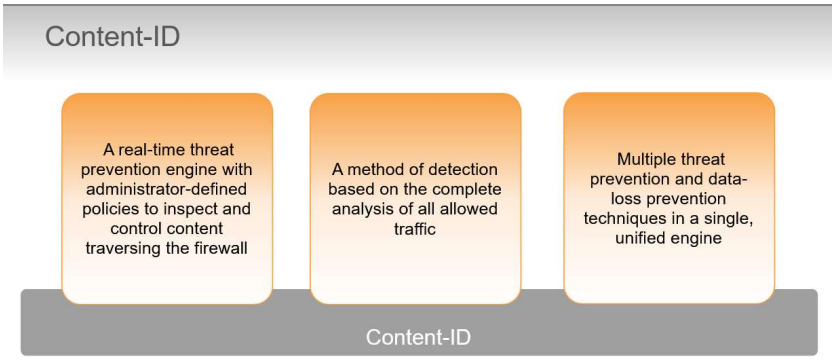
➢ Content-ID

❖ Content Identification (Content-ID):

- Firewall allow/denies traffic based only on source, destination, application, user and port information.
- Can also examines traffic for specific threats (viruses, spyware, and software designed to exploit application vulnerabilities

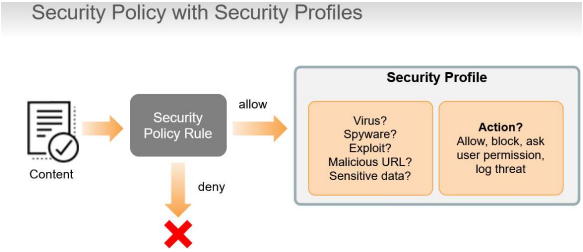


- Overview:
  - Applications are identified immediately by firewall and all allowed traffic is analyzed for exploits, viruses, spyware and malicious URLs



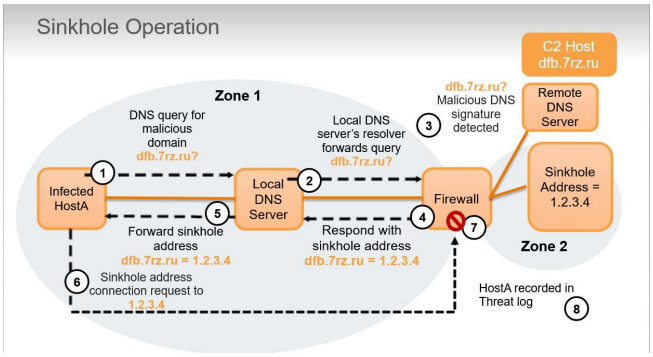
Palo Alto Networks controls the threat vectors themselves through the granular management of all types of applications.

  - **Security Profiles** are objects added to Security Policy rules that are configured with an action of “allow”. Are not necessary for configured Security Policy rules configured with “deny” action because no further processing is needed if the network traffic will be blocked.



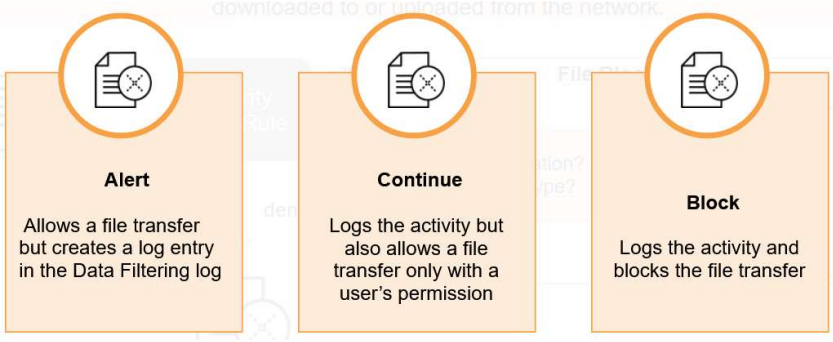
- Represents additional security checks to be performed on allowed network traffic. For example, web browsing may be allowed but user want to download a virus from website. Antivirus Security Profile can be attached to Security Policy rule to detect, block and log virus.
- There are different Security Profile Types:
    - Vulnerability Protection: detects attempts to exploit known software vulnerabilities
    - URL Filtering: classifies and controls web browsing based on content
    - Anti-Spyware: detects spyware downloads and traffic from already installed spyware
    - Antivirus: detects infected files being transferred with the application
    - File-Blocking: tracks and blocks file uploads and downloads based on file type and application
    - Data Filtering: Identifies and blocks transfer of specific data patterns found in network traffic (credit numbers, security number, passwords …)
    - WildFire: forwards unknown files to the WildFire service for malware analysis

- AntiSpyware configuration:
    - DNS signature: available through real tile on demand cloud database providing you with access to the complete Palo Alto DNS signature set (36 million)
    - Built-in domain detection logic that can identify potentially malicious domains by analyzing lookups to suspiciously named domains and unusual DNS query patterns
    - Exceptions are meant to handle false positives (to add exception we use DNS signature Threat ID number found in Threat Log)
    - **Sinkhole:** enable to quickly identify infected hosts on the network (default action for DNS signature is “sinkhole”)

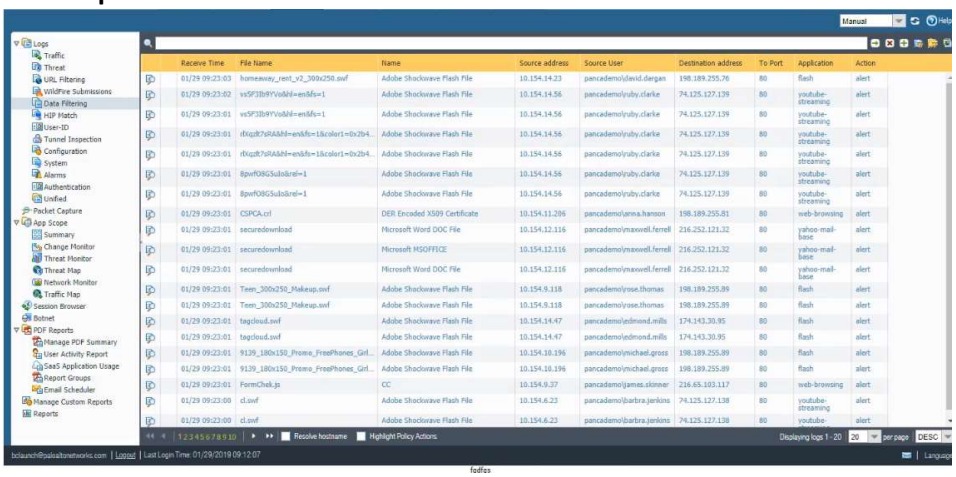


Sinkhole IP address is a Palo Alto server. We can configure another IP address as the sinkhole address. Sinkhole IP address doesn’t have to be assigned to a real host. The only recommendation is that the sinkhole address be in a different zone that the DNS client because by default only network traffic that travels between firewall zones is logged. DNS sinkhole involves forging responses to select DNS queries so that clients on the network attempt to connect to the specified sinkhole IP address rather than to a known malicious domain name.

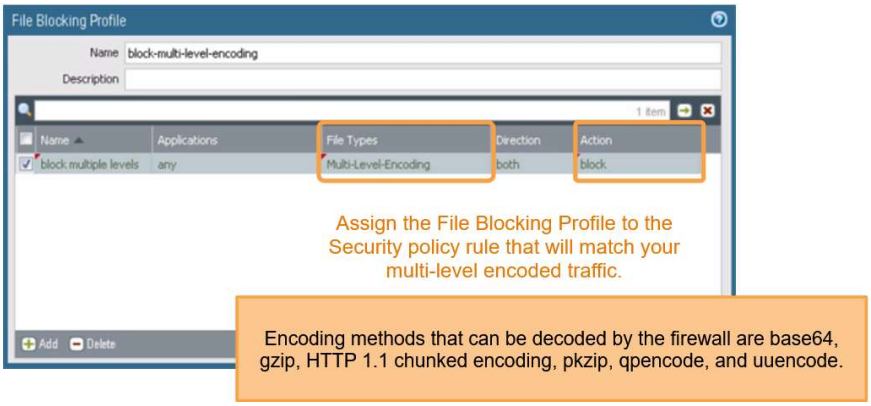
- FileBlocking configuration:
    - Activity is logged to Data Filtering Log
    - Implement by type on a per-application basis (FileBlocking Profile to block executable file attachments in Gmail while allowing executable file transfers in FTP)



- In Data Filtering Log **source address** is the system that **sent the file** and **destination address** is the system that receive the file. Is different!!!
  In *Traffic Log* **source address** is the system that **initiate session** and **destination** who **responds to session**.



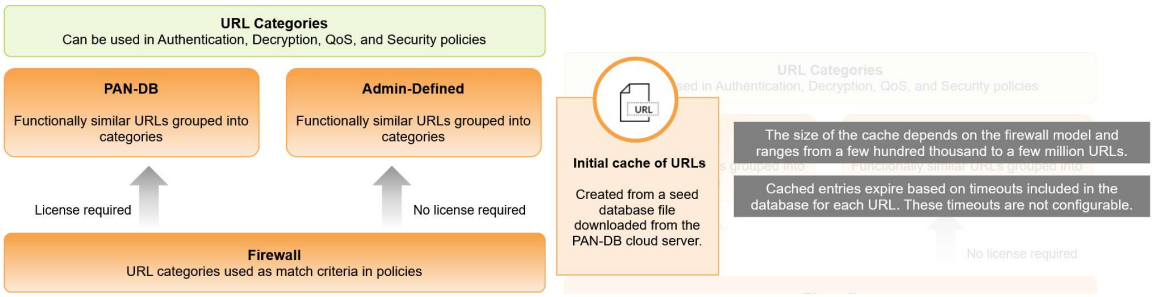
- Files can be encoded by multiple layers of protocols and applications. Word document with file extension .docx is an encoded file containing XML and binaries. If the file is zipped then there are 3 levels of encoding. If the zipped file is sent using HTTP chunk encoding, then there are 4 levels of encoding. In PAN-0S7.0 began decoding up to 4 layers. Earlier versions of PAN-OS support only 2 layers. File encoded more than 4 layers cannot be completely decoded but can be blocked by a File Blocking Profile

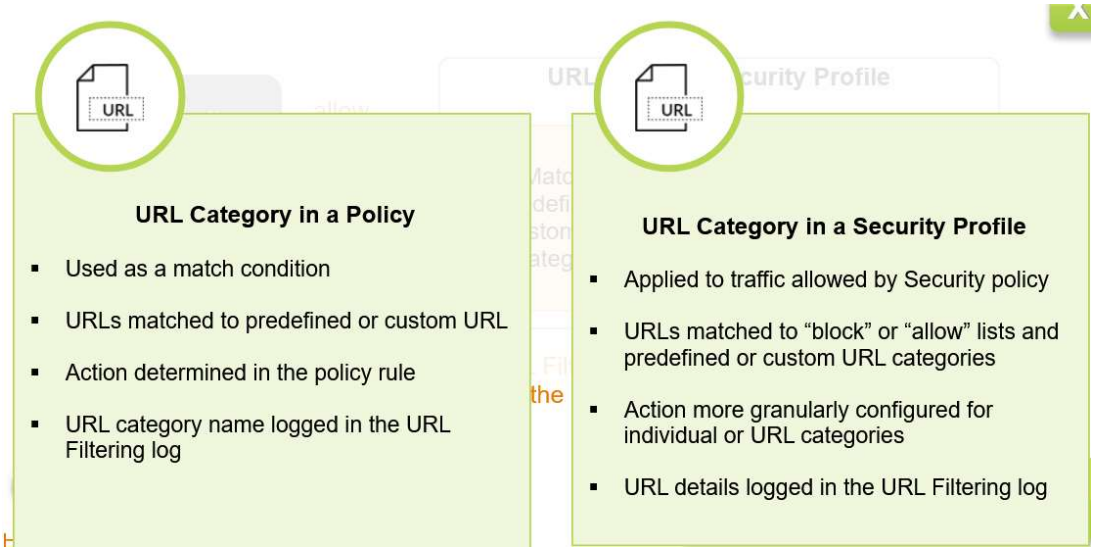


➢ URL Filtering

❖ URL Filtering Security Profile

- URL Filtering Feature:

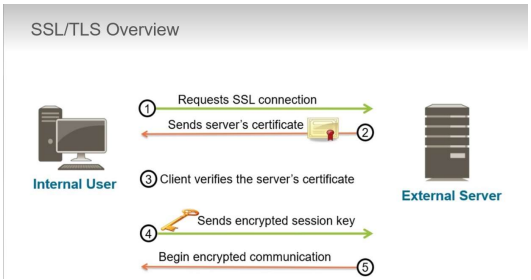




➢ Decryption

❖ Decryption Concepts:

- SSL/TLS Overview:

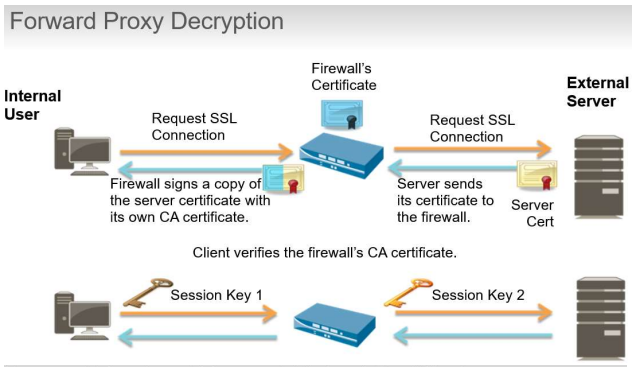


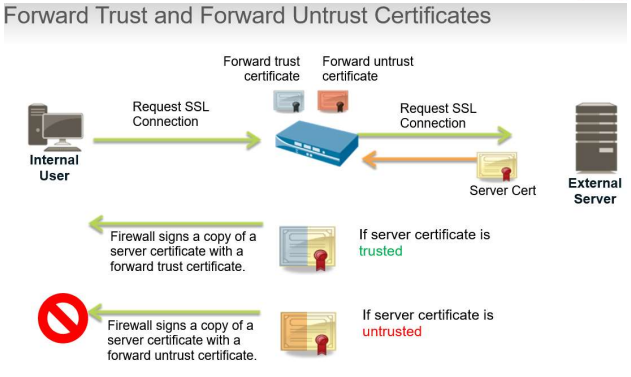
- 2) Certificate sent by server to client contains its identity and public key
- 3) Client use PKI to validate the server's certificate and server's public key
- 4) If the certificate is valid client uses the server's public key to encrypt symmetric session key and send it to server
- 5) Server uses its private key to decrypt the session key. Both sides use the session key to encrypt communications
- Communication partners periodically might need to establish a new session and rekey the communication. This is known as PERFECT FORWARD SECRECY or PFS provides assurance that if a key is compromised any recorded former sessions cannot be decrypted.
- There are 3 firewall decryption types:
  - **SSL FORWARD PROXY:**

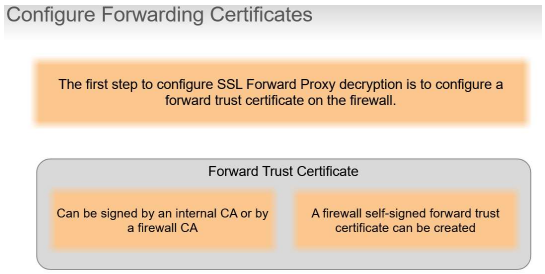
- Configure an SSL Forward Proxy decryption on the firewall to decrypt SSL traffic between an internal host and an external web server.
- The firewall acts as an SSL proxy.
- A connection is formed between an internal user and the firewall, while a separate but related SSL connection is formed between the firewall and the external web server.

Usefulness: internal user will connect via an encrypted connection to Facebook. The company policy is to allow employees to read Facebook but to prevent facebook-chat and facebook-posting. If SSL decryption is enabled for the Facebook application, company policy can be implemented easily with the firewall. If SSL decryption is not enabled, then the firewall cannot identify which application is inside the SSL connection nor can it recognize that application shifts are occurring within the connection.

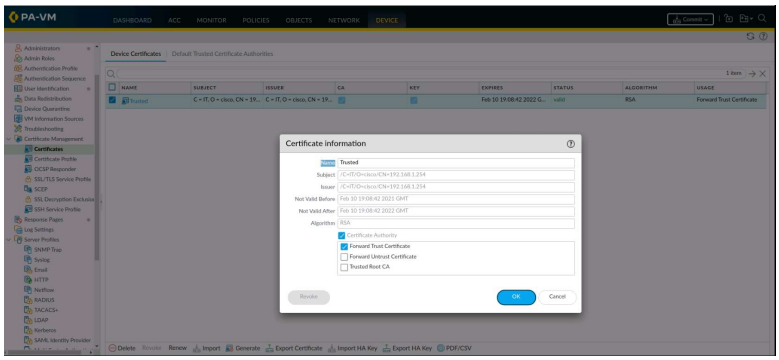
Prevents malware concealed as SSL encrypted traffic from being introduced to an organization's network. ALTRIMENTI NON POTREMMO DECRIPTARE IL TRAFFICO E FARE INSPECTION







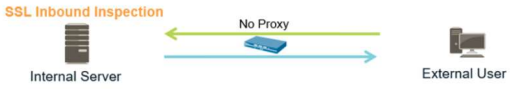
If we create a forward trust certificate self-signed by firewall every SSL client will have to have this certificate installed in their certificate store. Otherwise they will get certificate warning errors.



Enables firewall to use the certificate as its forward trust certificate during SSL Forward Proxy decryption

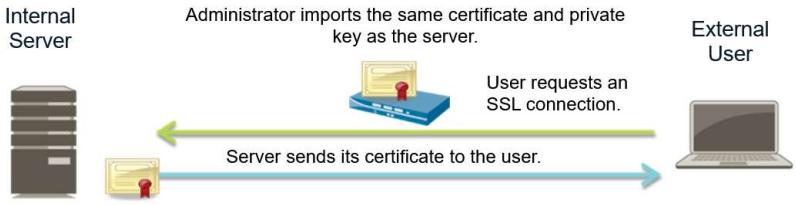
PALO ALTO RECOMMENDS ALSO CONFIGURING A FORWARD UNTRUST CERTIFICATE WHICH ENSURES THAT AN SSL CLIENT WILL RECEIVE A BROWSER BLOCK PAGE WHEN THE FIREWALL DOES NOT TRUST THE CA OF THE SERVER TO WHICH THE CLIENT IS ATTEMPTING TO CONNECT. THIS CERTIFICATE SHOULD NOT BE TRUSTED BY SSL CLIENTS OR THEY WILL NOT GET A BROWSER CERTIFICATE WARNING WHEN THEY TRY TO CONNECT TO AN UNTRUSTED SERVER. TO ENSURE THIS CERTIFICATE SHOULD NOT BE ISSUED BY A TRUSTED CA OR NOR SHOULD IT BE COPIED TO AN SSL CLIENT'S CERTIFICATE STORE.

- **SSL INBOUND INSPECTION:**



- Configure SSL Inbound Inspection to decrypt SSL traffic coming from external users to internal servers.
- The administrator must have access to the server's private key and certificate.
- The firewall decrypts and inspects only the traffic flowing through it.

A direct connection SSL is formed directly between the external user and the internal server. Firewall can inspect inbound SSL traffic for potential threats from external hosts to internal SSL servers. After inbound traffic has been decrypted and the underlying application and data are exposed, the session can be controlled by Security policy rules and Security profiles.

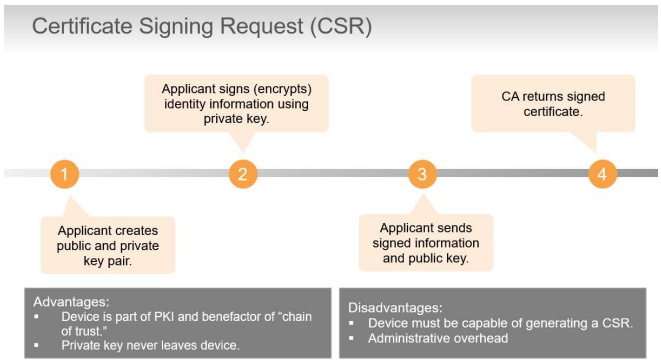


Before firewall can inspect SSL traffic going to an internal server, it needs a copy of the server's certificate and private key. An SSL Decryption policy rule also must be configured on the firewall to inspect the inbound traffic. After this configuration is complete, the firewall can decrypt and read the traffic before it forwards the traffic to the server. The secure SSL connection remains between the SSL client system and internal SSL server. *Non fa man-in-the-middle perché il client vede direttamente il certificato del server.*

- **SSH DECRYPTION:**

- Configure SSH Decryption to decrypt outbound and inbound SSH traffic.
- If an SSH tunnel (port forwarding) is discovered, the SSH connection is blocked to ensure that SSH is not being used to tunnel disallowed applications and content.
- Apply a Decryption Profile to Security policy rules to control normal, non-port-forwarded SSH traffic.

- Certificate Signing Request (CSR):

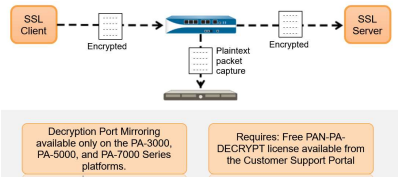


- Unsupported Applications: some applications are not implemented to standards or use capabilities in the standards that are not compatible with Palo Alto. SSL decryption also cannot be used when servers require client-side certificates
  - Application that fail are added to an exclude cache:
    - Decryption not attempted again for 12 hours after first occurrence
    - After 12 hours firewall attempts to decrypt the traffic from that website again
    - If decryption fails again, website is re-added to the cache and the process start over
    - To avoid this failure every 12 hours for a site that is known, you can add the site to the decryption exclusion list
      #show system setting ssl-decrypt exclude-cache

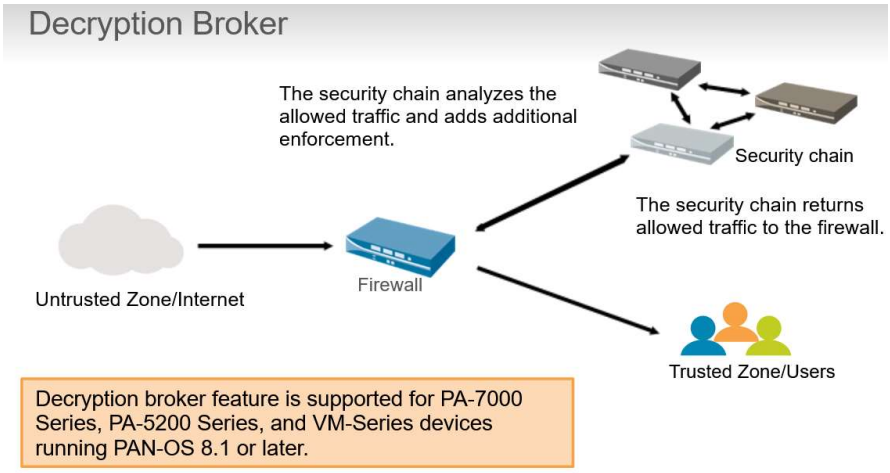
```
> APP_UNSUPPORTED: The application, such as an SSL VPN, is not RFC-compliant.
> SSL_CLIENT_CERT: The application uses a client certificate.
> SSL_EXCLUSION_LIST_MATCH: The SNI or CN matched a username in the exclusion list.
> SSL_UNSUPPORTED: The firewall does not support the SSL version required.
```

```
> SSL_UNSUPPORTED_CIPHER: The server does not support a compatible cipher suite.
> SSH_ERROR: An SSH application error occurs.
> SSH_UNSUPPORTED_VERSION: The firewall does not support the SSH version required.
> SSH_UNSUPPORTED_ALG: Application-level gateway support is not supported.
```

- Decryption Port Mirroring: enables firewall to forward packet captures of decrypted traffic to traffic collection tool for archiving and analysis.



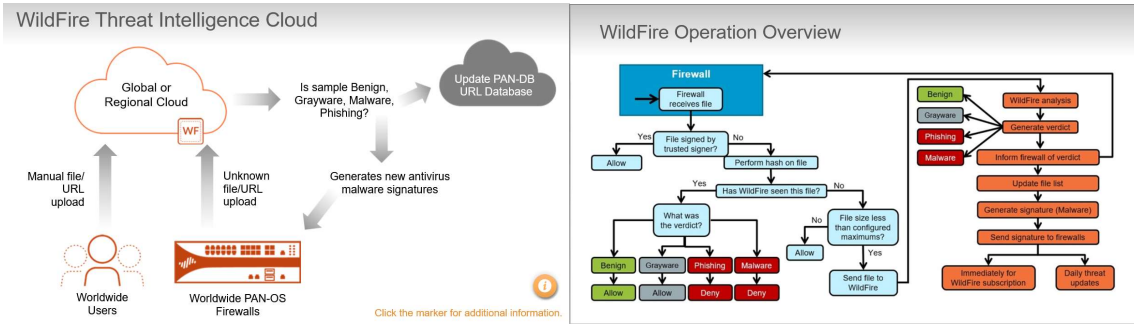
- **Decryption Broker**: can provide a single central point for decrypting all of your network traffic.
  - The decryption broker enables firewall to forward plain, cleartext traffic to a security chain for additional enforcement, which provides complete visibility into network traffic.
  - Security chain is a set of inline, third party appliances dedicated to perform specific security functions such as an Intrusion Prevention System.
  - Single firewall can distribute decrypted sessions to a maximum of 64 security chains and can monitor it to ensure that they are effectively processing traffic



➢ WildFire

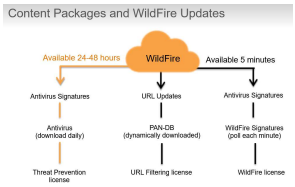
❖ WildFire Concepts:

the maximum number of WildFire appliances that can be grouped into a WildFire appliance cluster is 20.



- WildFire Verdict Descriptions:
  - **Grayware**: introduces in PAN-OS7.0 to identify executables that behave similarly to malware but are not malicious in nature or intent.
  - **Malware**: WildFire has determined that the file or the URL is malicious in nature and intent and can pose a security threat to your organization. If a current signature does not exist, WildFire will create one and make it available to firewalls around the world

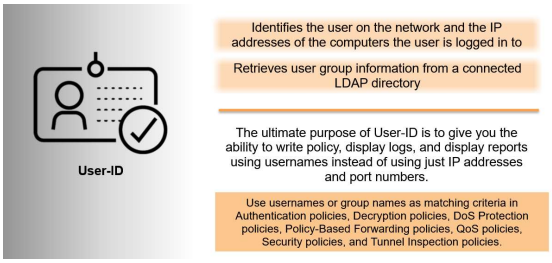
- **Phishing**: introduced to classify phishing links found in emails separately from emailed links found to be exploits or malware. Palo Alto security researchers also manually review certain links to check for phishing activity. Phishing links are added to PAN-DB database



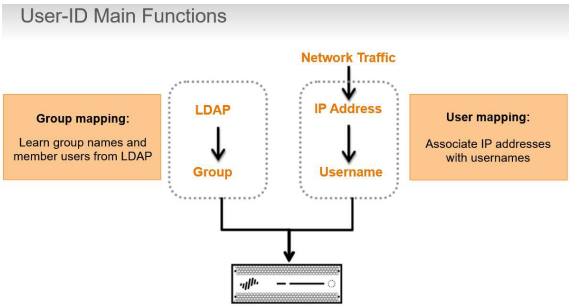
➢ User-ID

❖ User-ID overview

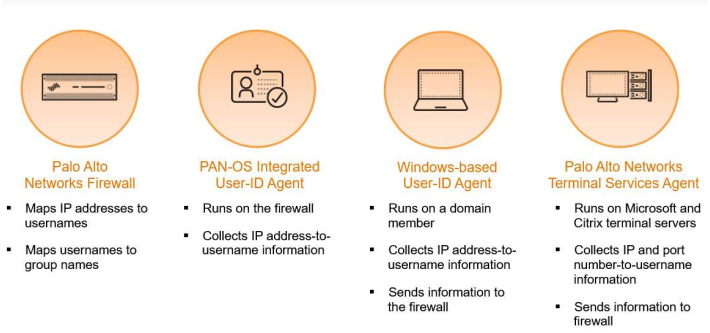
- Increasingly dynamic nature of users and applications means that IP addresses alone have become less effective as a mechanism for monitoring and controlling user activity



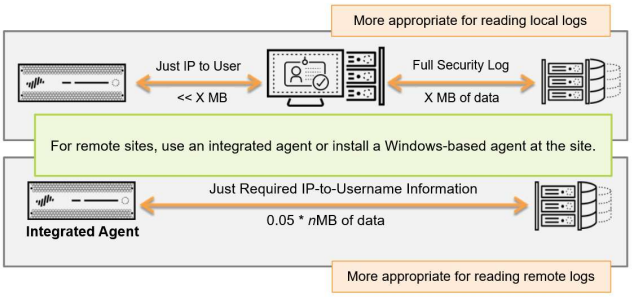
- Firewall requires a list of all available users and their corresponding group mappings. Firewall uses group mapping and user mapping to collect this information.



- Components of User-ID tech:



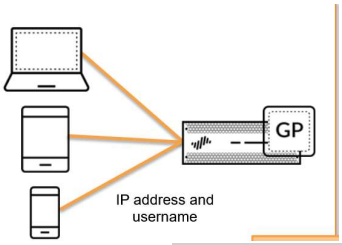
- Integrated Agent vs Windows-Based Agent:



Windows base agent uses MS-RPC, which requires the full Windows Security logs to be sent to the agent, where they are filtered for the relevant User-ID information.

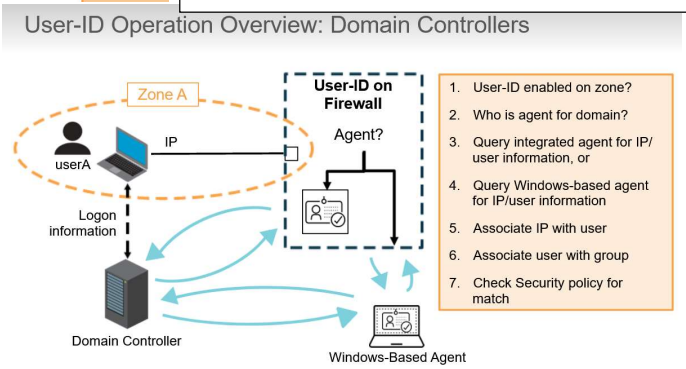
PAN-OS integrated agent uses either the Windows Management Instrumentation or WMI or the Windows Remote Management Protocol or WinRM, which enables the agent to retrieve only the relevant User-ID information from the Windows Security logs.

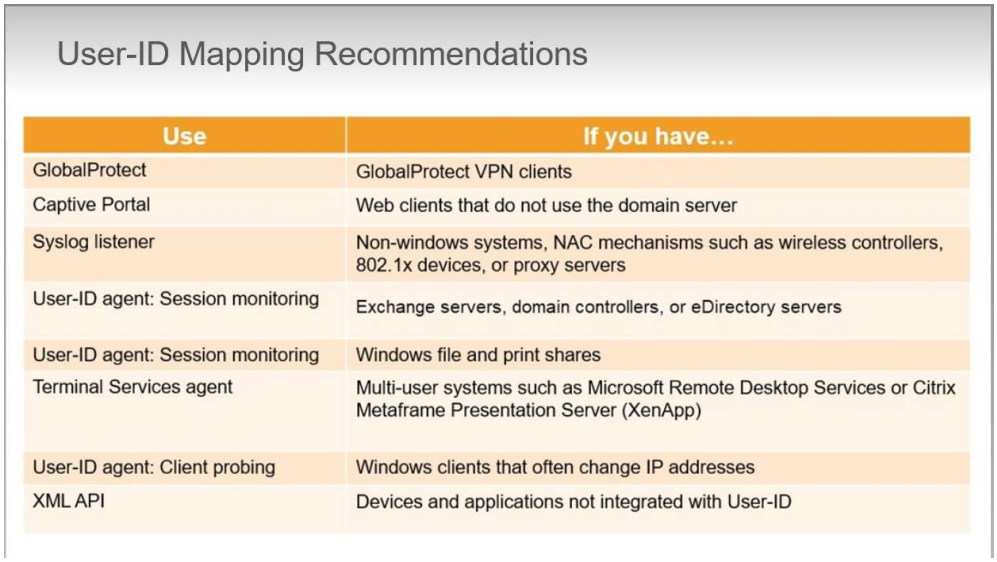
- User Mapping using GlobalProtect:



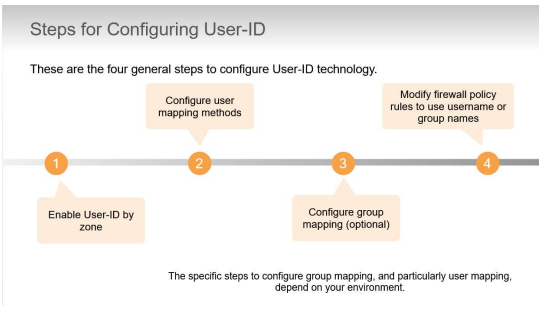
For remote romaing users, GlobalProtect client provides the user mapping information to the firewall directly. In this case, every client require user to enter login credentials for VPN access to firewall.

User-ID information also can be provided from clients that are connected to an internal network via an internal Global Protect gateway without establishing a VPN tunnel to firewall.

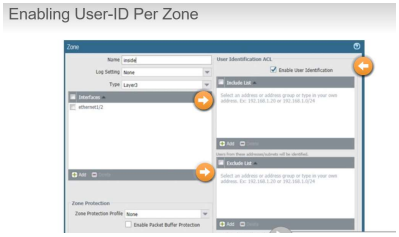




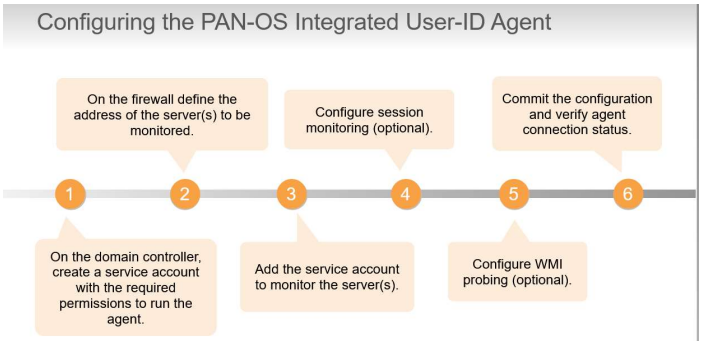
❖ Configuration of User-ID:



Never enable User-ID on the zone that contains the Internet because firewall will attempt to identify every user from outside you network. By default User-ID will try to map users from all subnetworks found within a User-ID-enabled zone.
Use the **Include List** to limit the subnet or specific addresses that firewall will attempt to map to users.
Use the **Exclude List** only to exclude user mapping information for a subset of the subnets you added to Include List

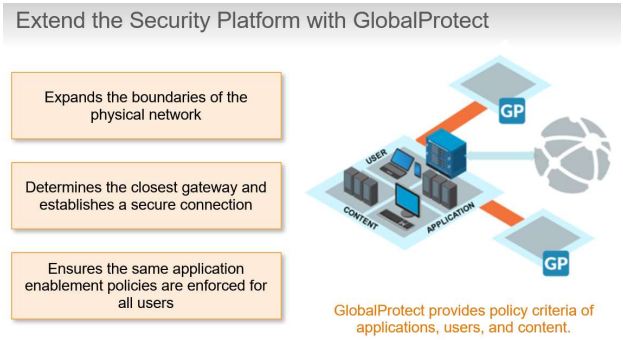


❖ Configuration of PAN-OS integrated User-ID agent:



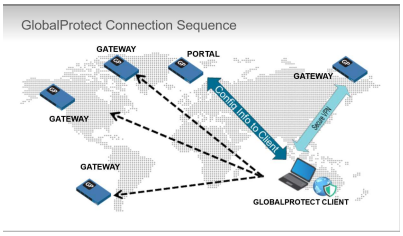
➢ GlobalProtect

❖ GlobalProtect overview:

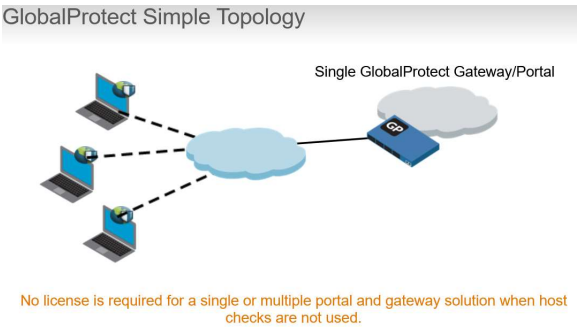


- Firewall requires a list of all available users and their corresponding group mappings. Firewall uses group mapping and user mapping to collect this information.
- GlobalProtect components:

- **GlobalProtect Portal**: provides the management functions for the GlobalProtect infrastructure. Every client connecting to the GlobalProtect network receives configuration informations from the portal.
- **GlobalProtect Gateway(s)**: provides security enforcement for traffic from GlobalProtect agents and apps:
    - External Gateway provide security enforcement and VPN access for remote users
    - Internal Gateways apply Security policy for access to internal resources
- **GlobalProtect Client Software**: Runs on end-user systems and enables access to network resources via the deployed GlobalProtect portals and gateways.



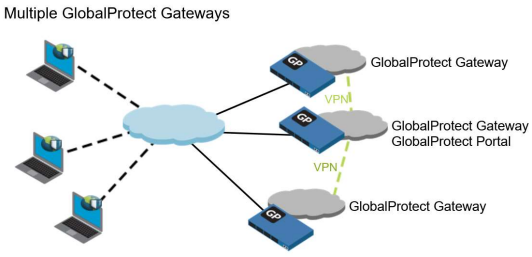
- **GlobalProtect Simple Topology**:



Require at least one portal and one gateway. Portal and Gateway can be configured on the same firewall, also with same IP address, which provides end users with VPN access to internal networks with a minimum of configuration.

If the gateway and portal share an IP address, only one certificate is needed for the firewall.

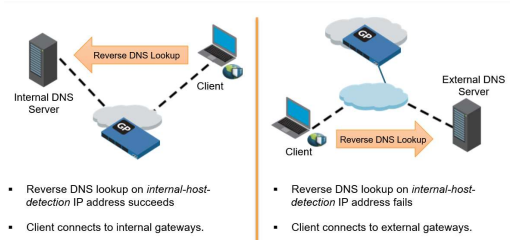
- **GlobalProtect Advanced Topology**:



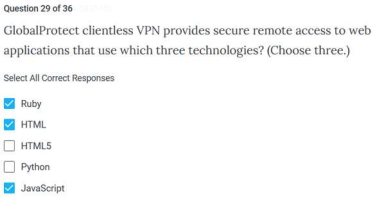
Additional gateways can be used to provide access to multiple protected networks. Also for redundancy and performance improvements for end users.

The chosen gateway is the one that responds fastest to the connection request. To ensure consistent access, multiple gateways often require the networks to be connected by VPN each other.

- Determining Internal of External Gateways
    - Portal may provide an IP address and DNS hostname as part of the information passed to the client to determine whether the host is inside or outside the corporate network.
    - DNS hostname and IP address must correspond to a device whose name can be resolved only by an internal name server.

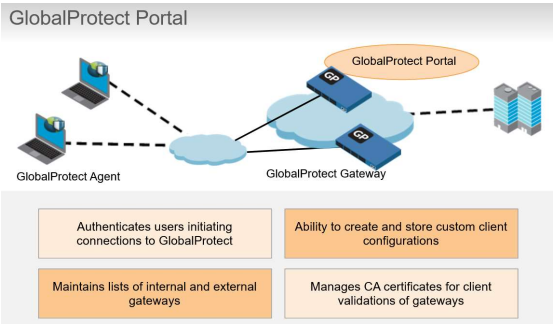


- **Clientless VPN**: provides secure remote access to common enterprise web application that use HTML, HTML5, Ruby and Javascript.



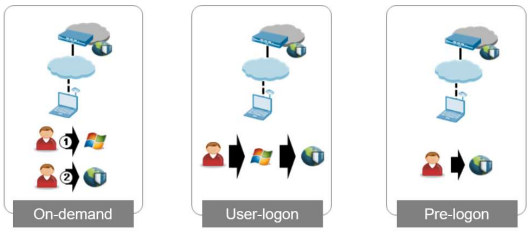
  - Users can have a secure access from SSL-enabled web browser without installing the GlobalProtect client software.
  - Remote users can login inside GlobalProtect Portal using a web browser and launch web applications you publish for the user.
  - We can allow to access additional corporate applications or a set of applications
  - Remote user who log in to the portal will see a published applications page with a list of web applications they can launch.
  - Security policies need to be configured to allow traffic from GlobalProtect clients to the security zone associated with the GlobalProtect portal that hosts published applications landing page.
  - Security policies will need to be configured to allow user-based traffic from GlobalProtect portal zone to the security zone where the published application servers are hosted

❖ GlobalProtect Portal:

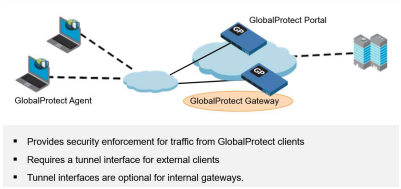


❖ Client Configuration:

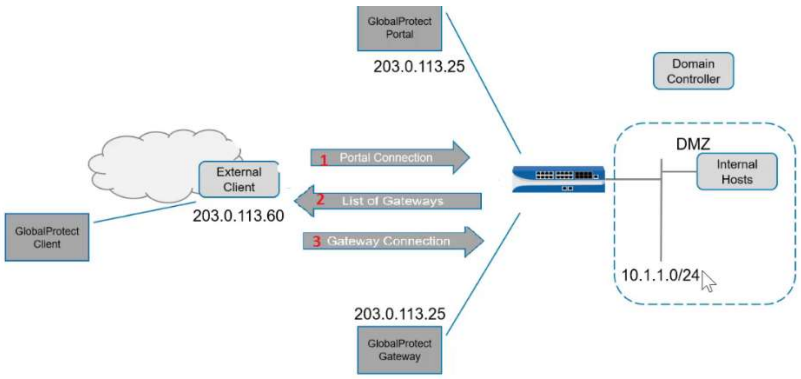
- App Connection Methods:
  - **On-demand:** allow users to establish a connection on demand. With this option, the user must explicitly initiate a connection.
  - **User-logon:** automatically establishes a GlobalProtect client connection **after** the user logs in to their computer. This methods requires the Authentication Profile to use the same verification service as login process (Active Directory or RADIUS)
  - **Pre-logon:** preserves pre-login and post-login services provided by a corporate infrastructure regardless of where the user machine is located. GP establish a connection even if the user is not logged in to their computer. This practice means that a company can create a “logical network” that maintains the security and management features normally achieved by a physical network.



- GlobalProtect Gateway:
  - Provides the endpoint for the agent's connection
  - Gateways support split tunneling. Though this feature is not recommended for extending the firewall policy with application control and visibility to all mobile users



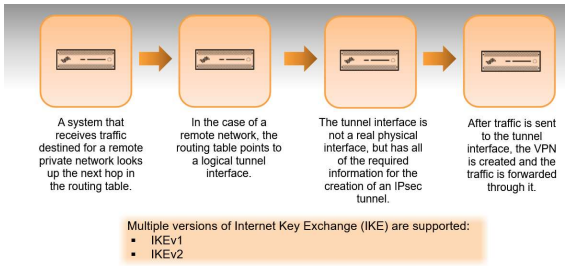
- GlobalProtect HOW IT WORK (example):
  - In this example we have also a Domain Controller that we can use to authenticate users that want to establish a Global Protect connection.
    1. Clients connect to the Portal
    2. Portal authenticates client and send back the list of gateways to GlobalProtect client software can connect to. In this case there is only one gateway.
    3. Client can pick a gateway in this case 203.0.113.25 to establish a secure tunnel. Gateway send back an IP address in 10.1.1.0/24 and now client can be considered inside the local network



➢ Site to Site VPN

❖ Site to Site VPN:

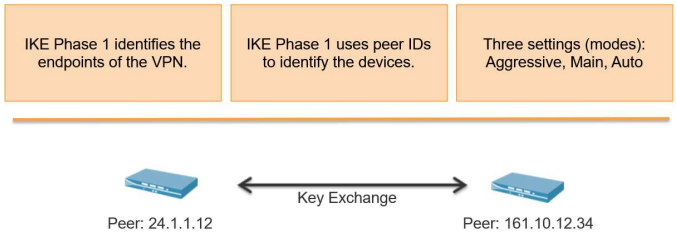
1. PAN-OS software implements IPsec VPN as route-based tunnels, as opposed to policy-based designs. In a route-based VPN the determining factor of which traffic will be tunneled is the final destination of that traffic.
2. Route-based VPN are easy to deploy and scale readily to large environments because they take advantage of dynamic routing protocols.



3. IKEv1 is the more commonly used version. IKEv2 primarily is used to meet the requirements of the NDPP (Network Device Protection Profile), Certification, Microsoft Azure compliance or/and Suite B support.
4. IKEv2 preferred mode provides the ability to fall back to IKEv1 after 5 retries (about 30 secs)

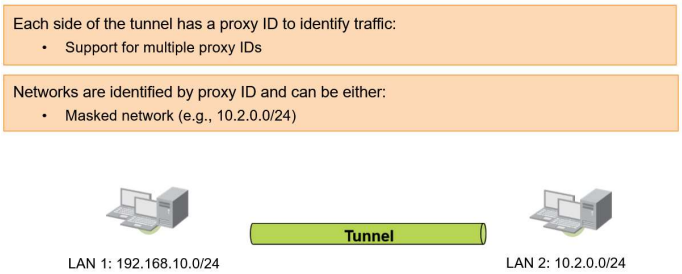
❖ IKE phases:

1. **PHASE 1: the IKE protocol authenticates the firewalls to each other and sets up a secure control channel. Use IKE-Crypto Profile for IKE negotiation**
    1. Each device is identified to the other by a per ID. In most cases this ID is just the public IP address of the device. In situations where the public ID is not static, this value can be replaced with a domain name or other text value
    2. Five pieces of information are passed during the IKE phase 1:
        1. Authentication method
        2. Diffie-Hellman key exchange
        3. Symmetric Key Algorithm
        4. Hashing algorithm
        5. Lifetime

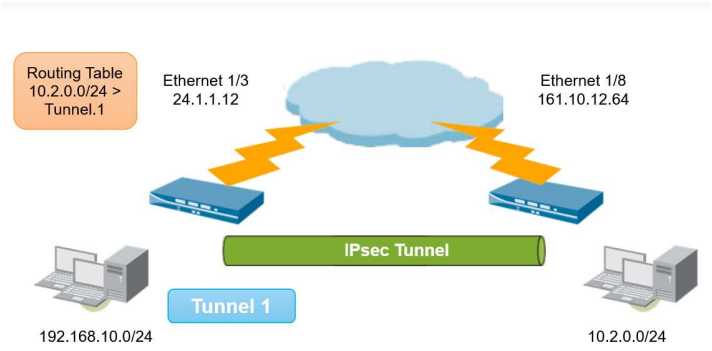


2. **PHASE 2: creates the tunnel that will encapsulate data traffic**
    1. Each side of the tunnel will have a proxy ID to identify the traffic it will be sending and what it expects to receive.

2. These IDs either can be a specific network range or a generic network of 0.0.0.0/0. In either case both sides need to know what the other side will be sending for the tunnel to work.
3. Five pieces of information are passed during the IKE phase 2:
    1. IPsec type/mode
    2. Diffie-Hellman PFS
    3. Symmetric Key Algorithm
    4. Hashing Algorithm
    5. Lifetime (before key renegotiation)



❖ Route-based Site-To-Site VPN:



We have to determine the required number of tunnels, for example a single VPN tunnel may be sufficient for connecting between a single central site and a remote site or connections between a central site and multiple remote sites require VPN tunnels for each central-remote site pair.

Each tunnel is bound to a tunnel interface. When moving VPN traffic across the tunnel interface to the same virtual router as the incoming (cleartext) traffic. In this way when a packet comes to the firewall, the route lookup function can determine the appropriate tunnel to use.

The tunnel interface appears to the system as a normal interface and the existing router infrastructure can be applied.

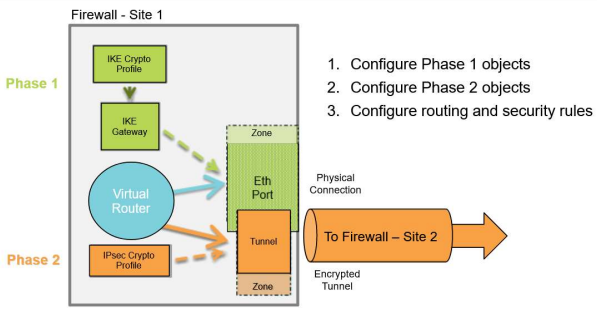
Each tunnel interface can have a maximum of 10 IPSec tunnels.

❖ VPN tunnel component interaction:

1. Diagrams show components that must be created to successfully configure IPsec VPN tunnel. The arrow indicate the dependencies among some components.
    1. Create tunnel interface (phase 1 object): Network -> Interfaces -> Tunnel. New logical interface must be added to a Layer 3 zone and to a virtual router, just as any other logical layer 3 interface would be handled
    2. Configure the IPSec tunnel (phase 2 object). Only values needed are the tunnel interface to use, the local peer ID, the remote peer ID and the pre-shared key or PSK. If the configuration is site-to-site with another Palo Alto Networks firewall, use

the default Crypto profiles. If the configuration is site-to-site with a different vendor's firewall, configure the advanced settings in the Crypto Profiles to match

3. Add a static route to the virtual router or enable an applicable routing protocol such as BGP, OSPF or RIP. Add a route table entry for the remote network that points to the tunnel interface used in Steps 1 and 2. Create a route for the remote network using the tunnel interface. No next-hop IP address is required when tunnel interfaces are used. Be sure to create a security rule to allow tunneled traffic.



❖ Configuration (main steps):

PHASE 1

1. IKE Gateway: Network > Network Profiles > IKE Gateways
2. IKE Crypto: Network > Network Profiles > IKE Crypto

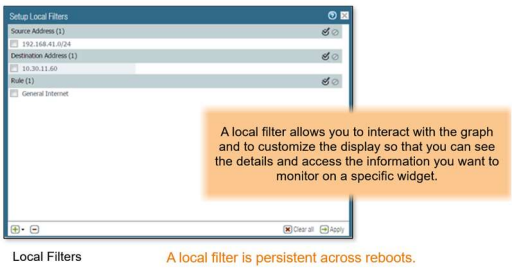
PHASE 2

1. IPsec Crypto: Network > Network Profiles > IPsec Crypto

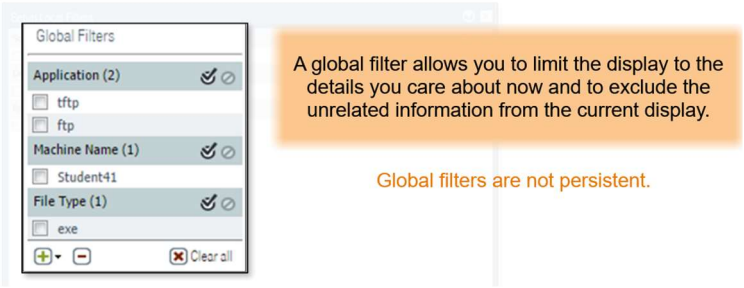
➢ Monitoring and Reporting

❖ Dashboard, ACC and Monitor:

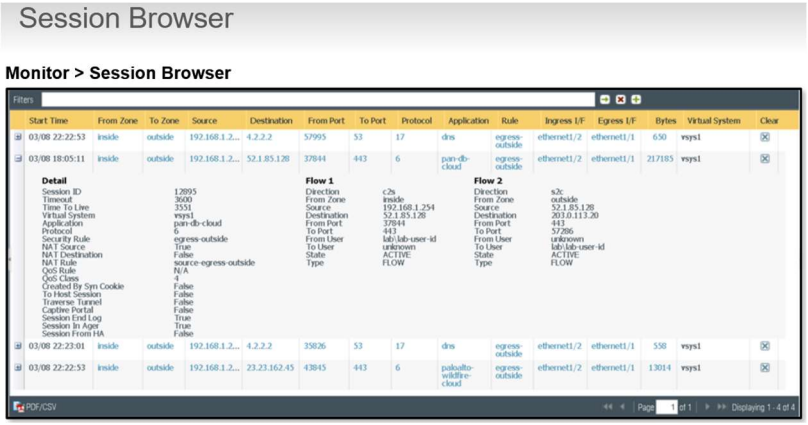
- Application Command Center allow to show network traffic, threat traffic, blocked activity etc…We can have custom tab by clicking on "+".
- Filters:
  1. Local filters are applied to a specific widget.



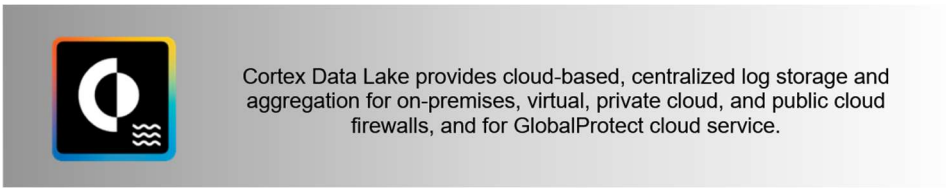
  2. Global filters are applied across all the tabs in the ACC. For example to display all events relating to a specific user and application, you can apply the user's IP address or username and the application as a global filter and display only the information pertaining to the user and the application through all the tabs and widgets on the ACC.

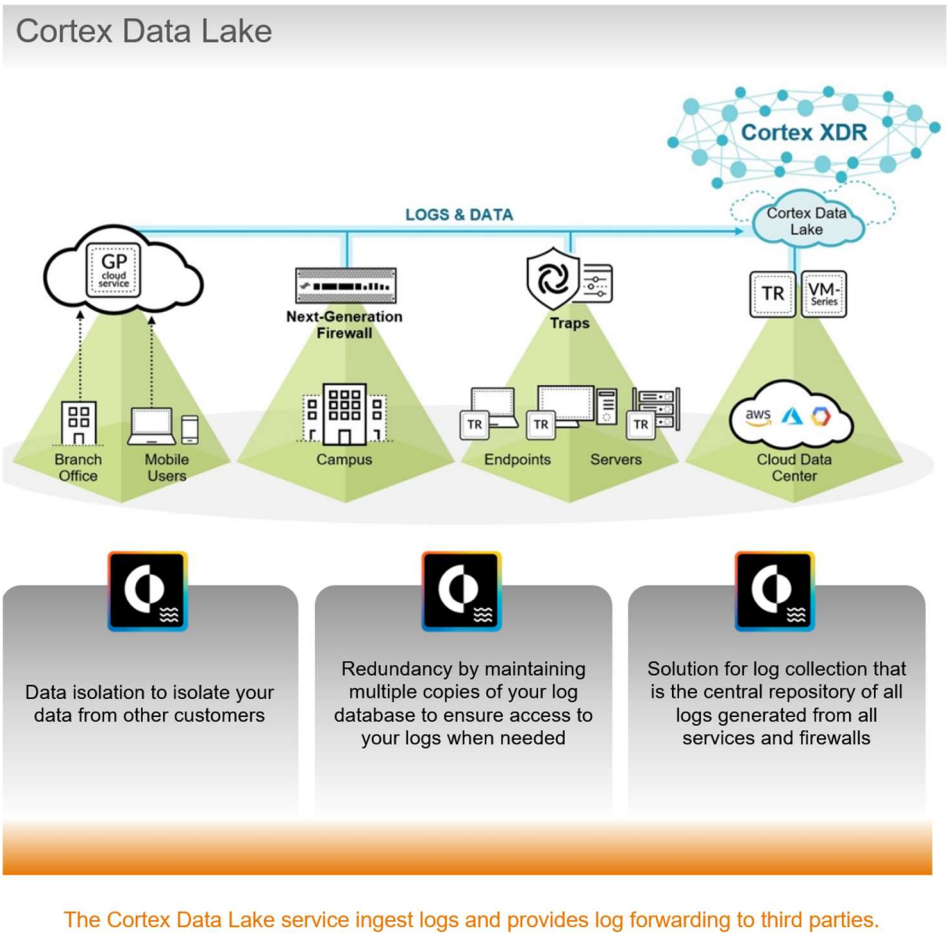


- Filters:
    1. Browse and filter sessions that are current on the firewall



- Cortex Data Lake:

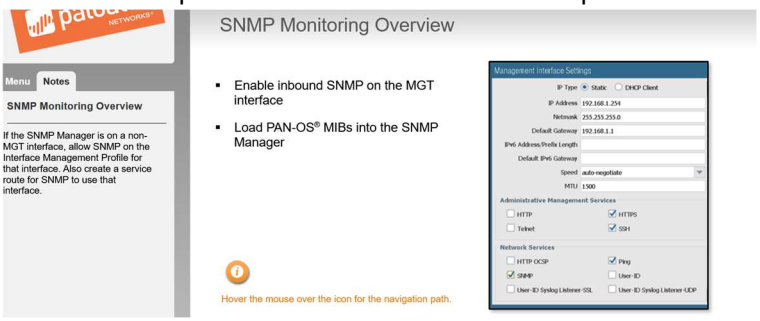




The Cortex Data Lake service ingest logs and provides log forwarding to third parties.

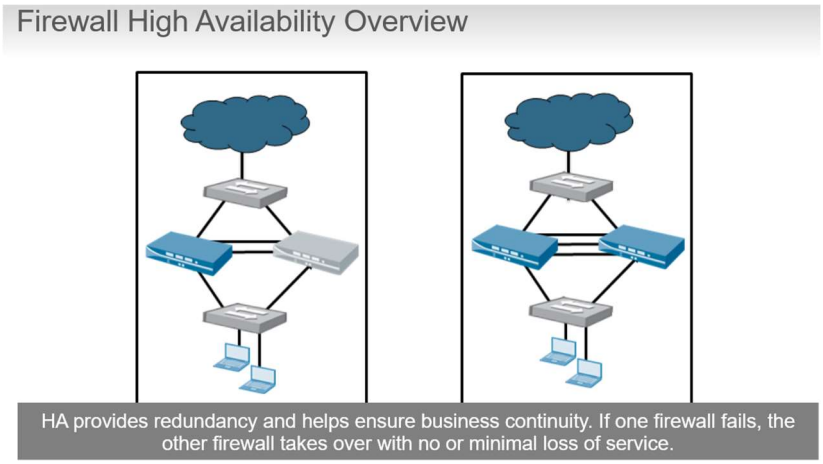
1. Cortex Data Lake unlocks the power of artificial intelligence for cybersecurity with services built to collect and store all your data combined with artifacts from a growing global community. The Cortex Data Lake service ingest logs and provides log forwarding to third parties. It offers flexible options to expand storage and log ingestion rates on demand without requiring you to purchase new hardware or to manually provision a new virtual machine.

- SNMP Monitoring:
    1. Device → Setup → Miscellaneous → SNMP Setup

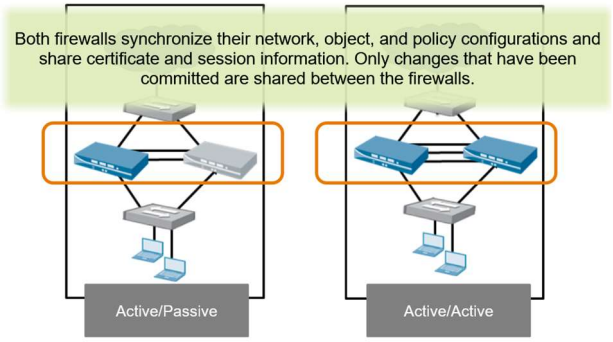


➢ Active/Passive High Availability

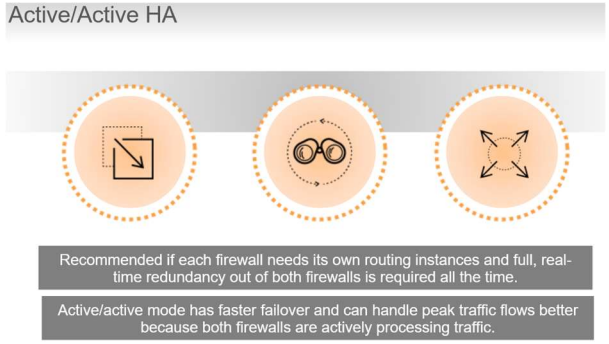
- Overview:



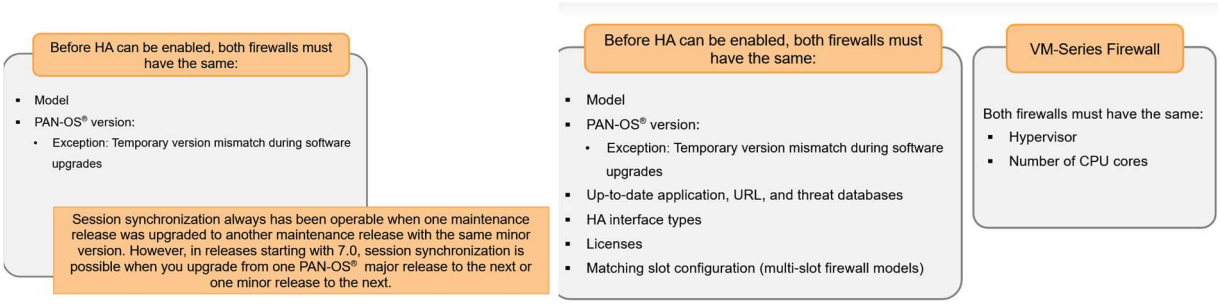
1. Firewall-specific configuration information such as management interface IP address, HA-specific configuration, log data, and the Application Command Center or ACC, is not shared between peers.
2. To get a consolidated view of applications and logs across the HA pair, you must use Panorama, the Palo Alto Networks centralized management system.



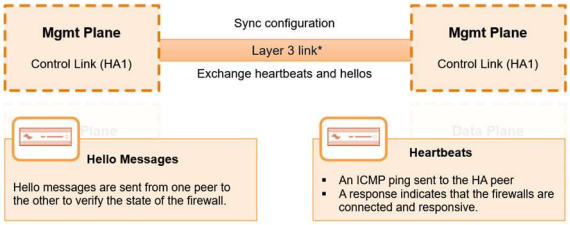
Active/Active can require advanced design concepts that can result in more complex networks (activation of dynamic routing, replication of NAT pools, and deployment of floating IP addresses to provide proper failover.)



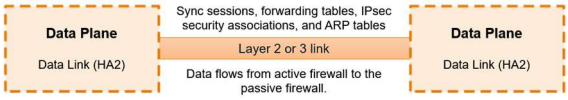
- HA Prerequisites:



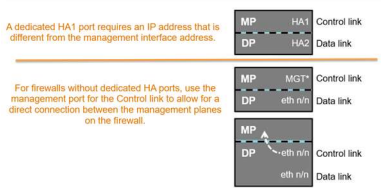
- Active/Passive HA Links:
    1. **Control Link** is a Layer 3 link and requires an IP address. Is used to exchange hellos, heartbeats and HA state infos to verify that peer firewall is responsive and operational. It's also used to synchronize routing and User-ID infos between management planes. Active firewall also use this link to synchronize configuration changes with its peer firewall.



    2. **Data Link** is a Layer 2 link but can be configured as a Layer 3 link that requires an IP address only if the Data Links are not on the same subnet. In Layer 2 mode, the Data Link uses Ethernet type 0x7261.



- Dedicated and Non-Dedicated HA Ports:
    1. Some firewall models have dedicated HA ports and others require you to use the management port or in-band ports as HA links. The Control Link provides synchronization for functions that reside on the management plane. Use of the management plane's dedicated HA1 port or management port as the Control Link is more efficient than use of the data plane's in-band ports because the need to pass the synchronization packets from the data plane over the management plane is eliminated. The ports MP and DP feature autosensing, so you can use a straight-trough or crossover cable.
    2. For firewall without dedicated HA ports, the best practice is to use the management port for the Control Link to allow for a direct connection between the management planes on the firewall. Use an in-band port for the Data Link. Any in-band port used as a Control or Data link must be configured as interface type HA.



- HA Backup Links: Provide redundancy for the Control and the Data Links

Purpose

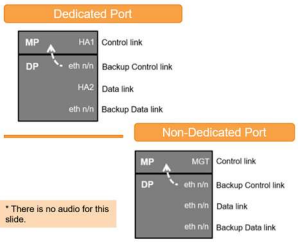
The purpose of configuring a backup Control link is to avoid a split-brain scenario.

What is a Split-brain Scenario?

- Occurs when a non-redundant Control link goes down
- The passive firewall concludes that the active firewall is down and attempts to start services that are already running on the active firewall.

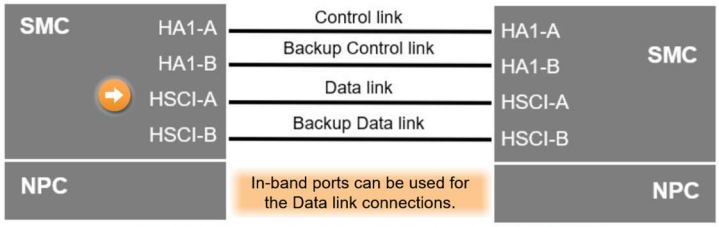
Consider the following guidelines when you configure backup HA links:

- The IP addresses of the primary and backup HA links must not overlap each other.
- HA backup links must be on a different subnet from the primary HA links.
- HA1 backup ports and HA2 backup ports must be configured on separate physical ports.



* There is no audio for this slide.

PA-7000 Series HA Links

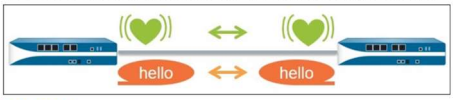


In software, the four HSCI-A are treated as a single HA interface; the same is true for the four HSCI-B ports.

- Failure Detection:
  1. **Heartbeats & Hellos**:

Used to verify that the peer firewall is responsive and operational

The **heartbeat** is an ICMP ping to the HA peer over the Control link, and the peer responds to establish that the firewalls are connected and responsive.

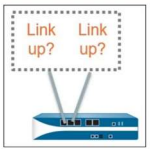


Hello messages are sent from one peer to the other to verify the state of the firewall.

  2. **Link Groups:**

You can configure the firewall to monitor the link states of its physical interfaces.

- Define and group the interfaces to monitor
- Configure a firewall to trigger a failure when either *any* or *all* of the monitored interfaces in the group fails.

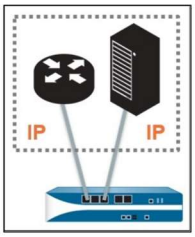


The default behavior is that failure of *any* one link in the link group causes a firewall failover.

  3. **Path Groups:** configure firewall to monitor path to mission-critical IP addresses using ICMP pings to test reachability.

Configuration Options

- Define and group the IP addresses to monitor.
- Configure a firewall to trigger a failure when *any* or *all* of the monitored IP addresses become unreachable.



Defaults

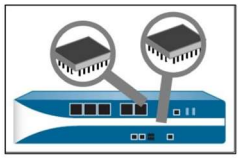
- Interval for pings is 200 milliseconds
- An IP address is considered unreachable when 10 consecutive pings fail.
- *Any* one of the IP addresses will cause a firewall failover if they become unreachable.

  4. **Internal Health Checks:**

On the PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls, a failover can occur when an internal health check fails.

- Health check is not configurable.
- Enabled to monitor the critical components, such as the Field Programmable Gate Arrays, or FPGAs, and CPUs.

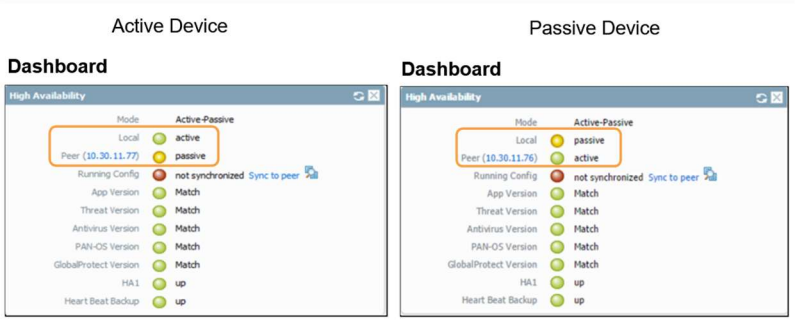
A failover also occurs when you suspend the firewall or when pre-emption occurs.



- Active/Passive Firewall States:

Firewall State	Description
INITIAL	Transient state of a firewall when it joins the HA pair. The firewall remains in this state after boot-up until it discovers a peer and negotiations begin.
ACTIVE	Normal traffic-handling state
PASSIVE	Normal traffic is discarded; might process LLDP and LACP traffic
SUSPENDED	Administratively disabled
NON-FUNCTIONAL	Error state

1. Monitor Firewall States: The High Availability widget on the Dashboard tab provides information about most of the major components of HA. This color-coded display show status as:
   I. Green (good)
   II. Yellow (passive)
   III. Red (critical)



Initiate synchronization manually the first time that a pair is connected

The manual initial synchronization prevent administrators from accidentally setting the wrong firewall as active and overwriting the configuration they want to push to the peer. **We should run "Sync to peer" from the active device or we may override the current configuration on the active device with the running configuration from the passive device, which may not be the most current configuration.**