

PCNSE Bootcamp v10.1

Exam Domain #1
Planning & Core
Concepts



PCNSE Overview

How the Program Works

- Weekly Seminar Provides Overview of Testing Domain
- Self Study Between Sessions
- Questions Supported via Slack Channel
 - Get into the Slack Channel - all the information is there
- Sessions Recorded and Published on YouTube
- Lab Resources Available via FUEL Virtual Test Lab Program

Email sent 9/14 8am from rschotsal@paloaltonetworks.com

With all the required links and instructions.



Slack Channel

PCNSE

1-core-concepts

Roger Schotsal 9:36 AM [YouTube](https://www.youtube.com/channel/UCmLLIVYaHYie29AT-hb48IA)

PCNSE
Channel dedicated to Palo Alto Networks PCNSE Certification.

9:36 <https://www.fuelusergroup.org/page/fuel-virtual-lab>

fuelusergroup.org
Fuel (26 kB)

fuel
PALO ALTO NETWORKS
USER GROUP

<https://www.paloaltonetworks.com/services/education/palo-alto-networks-certified-network-security-engineer>

Palo Alto Networks
Palo Alto Networks Certified Network Security Engineer (PCNSE)
The PCNSE certification covers how to design, deploy, operate, manage, and troubleshoot Palo Alto Networks Next-Generation Firewalls.

PDF

pcnse-study-guide.pdf

PCNSE Program Overview

- Exam Length = 80 Minutes
- Number of Questions = 75 Multiple Choice

PCNSE Scoring Matrix	
Domain	Weight
Core Concepts	12%
Deploy & Configure Core Concepts	20%
Deploy & Configure Features & Subscriptions	17%
Deploy & Configure Firewalls Using Panorama	17%
Manage & Operate	16%
Troubleshooting	18%
Total	100%

Exam Domain #1

Planning & Core Concepts

1.1 Identify how Palo Alto Networks products work together to improve PAN-OS services

1.1.1 Security Components

The Palo Alto Networks cybersecurity portfolio is organized into three offerings: **Strata** for enterprise security, **Prisma** for cloud security, and **Cortex** for security operations. The following sections describe how they work together to address some of the world's greatest security challenges.

SECURE THE ENTERPRISE



SECURE THE CLOUD



SECURE THE FUTURE

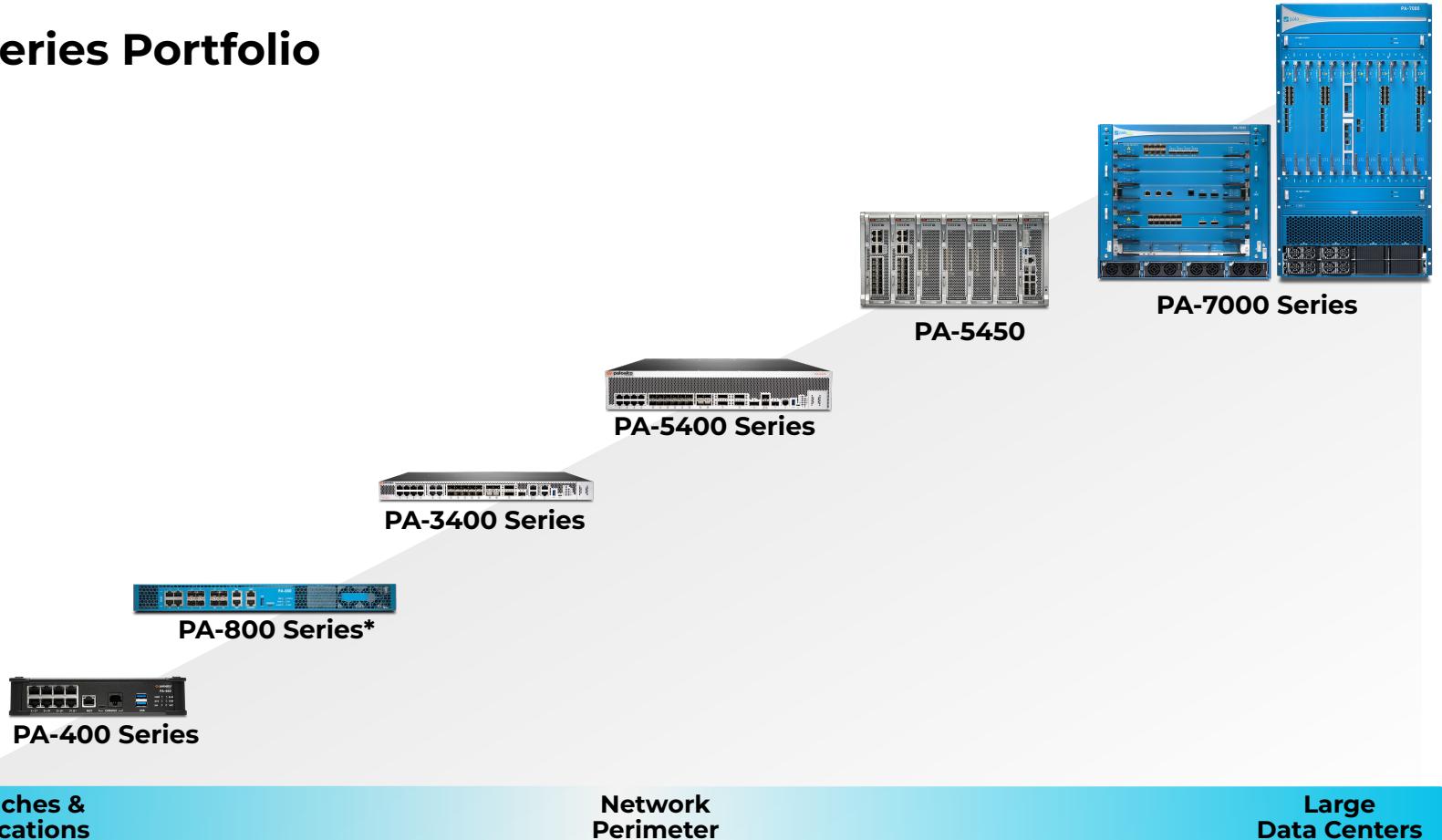


Palo Alto Networks Portfolio

Strata PA-Series	Prisma Access	Cortex XDR
ML-Powered Next-Generation Firewall	Secure Access Service Edge	Extended Detection and Response
App-ID User-ID Content-ID Device-ID	FWaaS Secure Web Gateway Zero Trust Network Access	Endpoint Threat Prevention Endpoint Detection & Response Behavioral Analytics Managed Detection & Response
VM-Series	Prisma Cloud	Cortex XSOAR
Virtual Next-Generation Firewall	Cloud Native Security Platform	Extended Security Orchestration, Automation and Response
App-ID User-ID Content-ID Device-ID	Cloud Security Posture Management Cloud Workload Protection Cloud Network Security Cloud Infrastructure Entitlement Management	Security Orchestration, Automation & Response Threat Intelligence Management
CN-Series	Prisma SD-WAN	Expanse
Containerized Next-Generation Firewall	Next-Generation SD-WAN	Attack Surface Management
App-ID User-ID Content-ID Device-ID	SD-WAN	Internet-Connected Asset Discovery & Mitigation
Panorama		Crypsis
Firewall Management		Cybersecurity Services
		Data Breach Response Cyber Risk & Resilience Management Incident Response Services

Cloud-Delivered Security Services (aka Content-ID)								
DNS Security	Threat Prevention	URL Filtering	WildFire	IoT Security	GlobalProtect	SD-WAN	Data Loss Prevention	Prisma SaaS
DNS Attack Prevention	Exploit, Malware, C2 Prevention	Malicious Site & Phishing Prevention	Malware Prevention	Enterprise IoT Security	Mobile User Security	Secure Branch Connectivity	Data Protection & Compliance	In-line & API SaaS Application Security

The PA-Series Portfolio



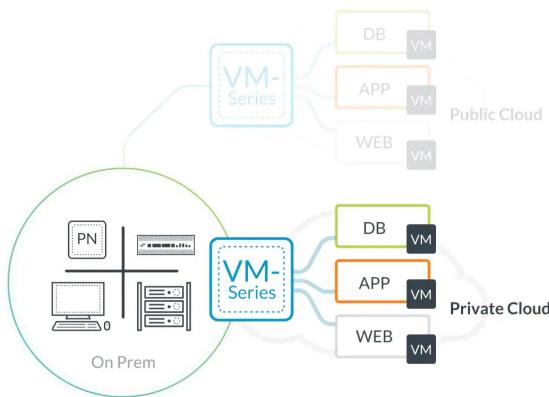
*For customers who need fiber ports

VM-Series NGFW

Security Where you need it When you Need it

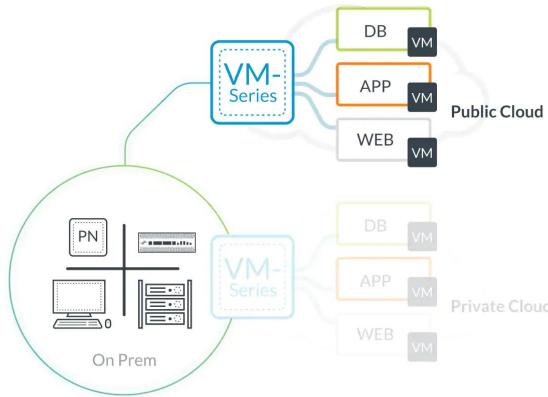
Private Cloud

- Cisco ACI
- Citrix NetScaler SDX
- Kernel-based Virtual Machine (KVM)
- Microsoft Hyper-V
- OpenStack
- VMware ESXi, NSX, vCloud Air



Public Cloud

- Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alibaba Cloud



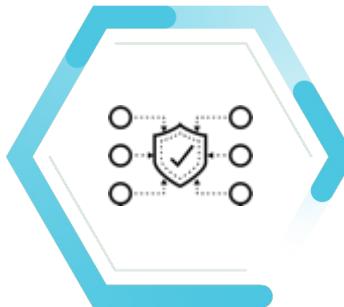
CN-Series (Containerized NGFW)

CN-Series providers comprehensive security for containerized applications



Inbound

Container-level protection against break-ins



East-West

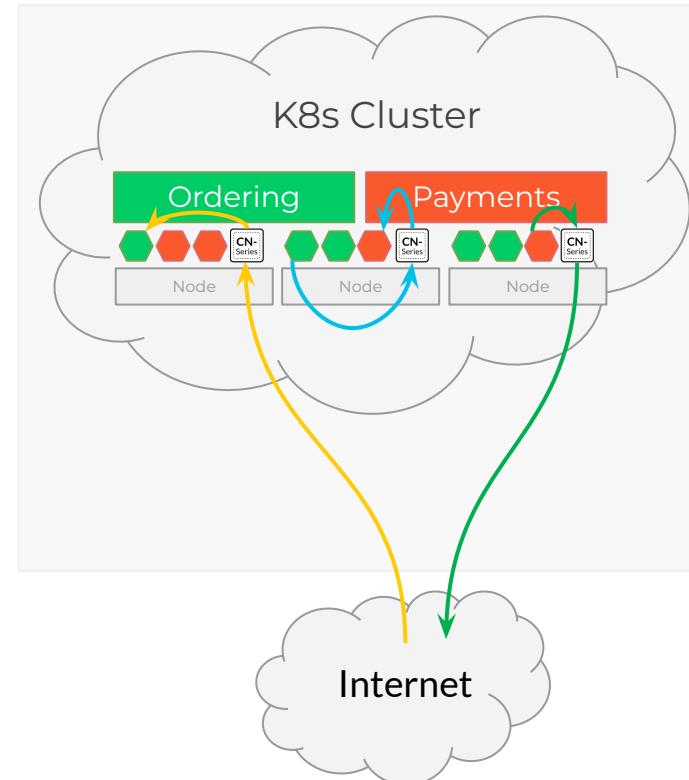
Prevent lateral propagation within container clusters



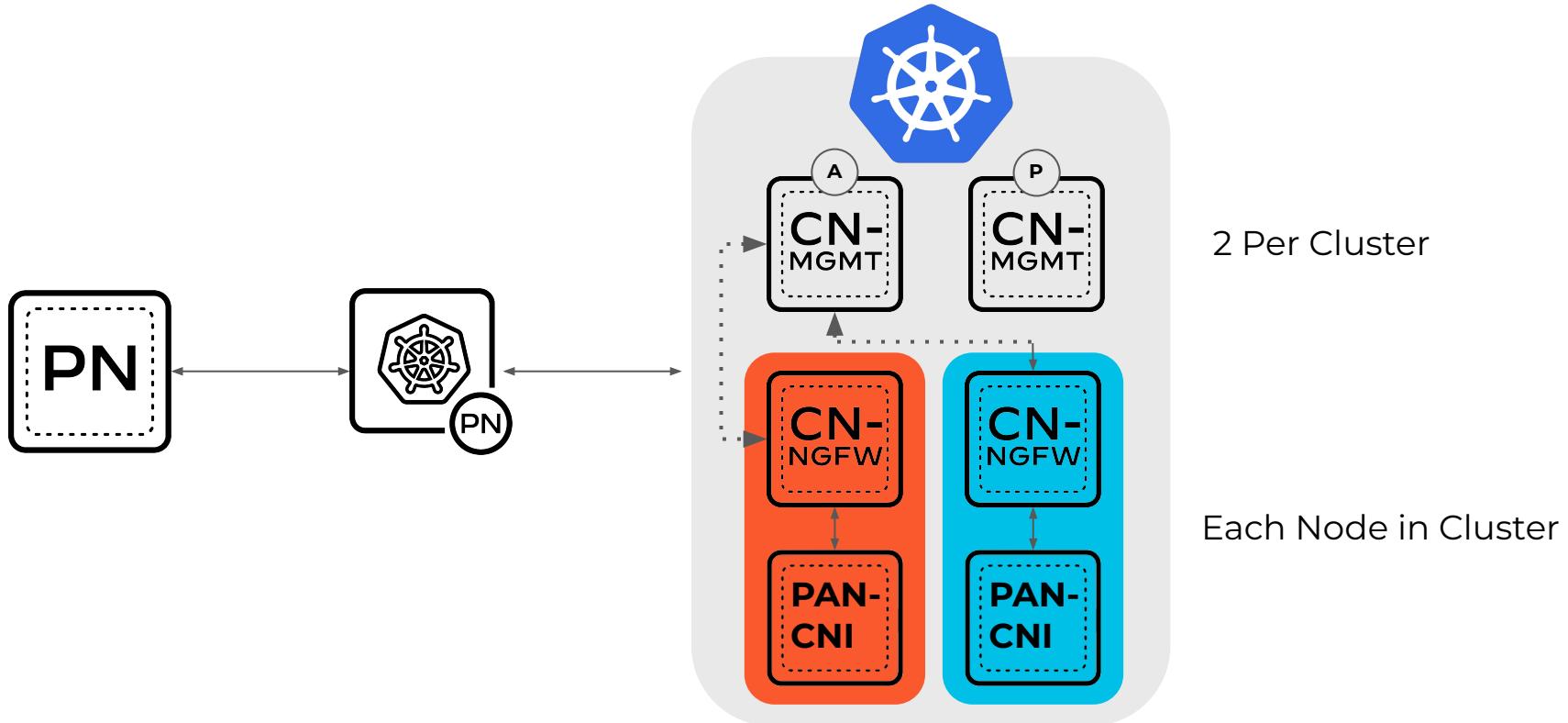
Outbound

Stop data exfiltration with container-context

By running a CN-Series NGFW on each node

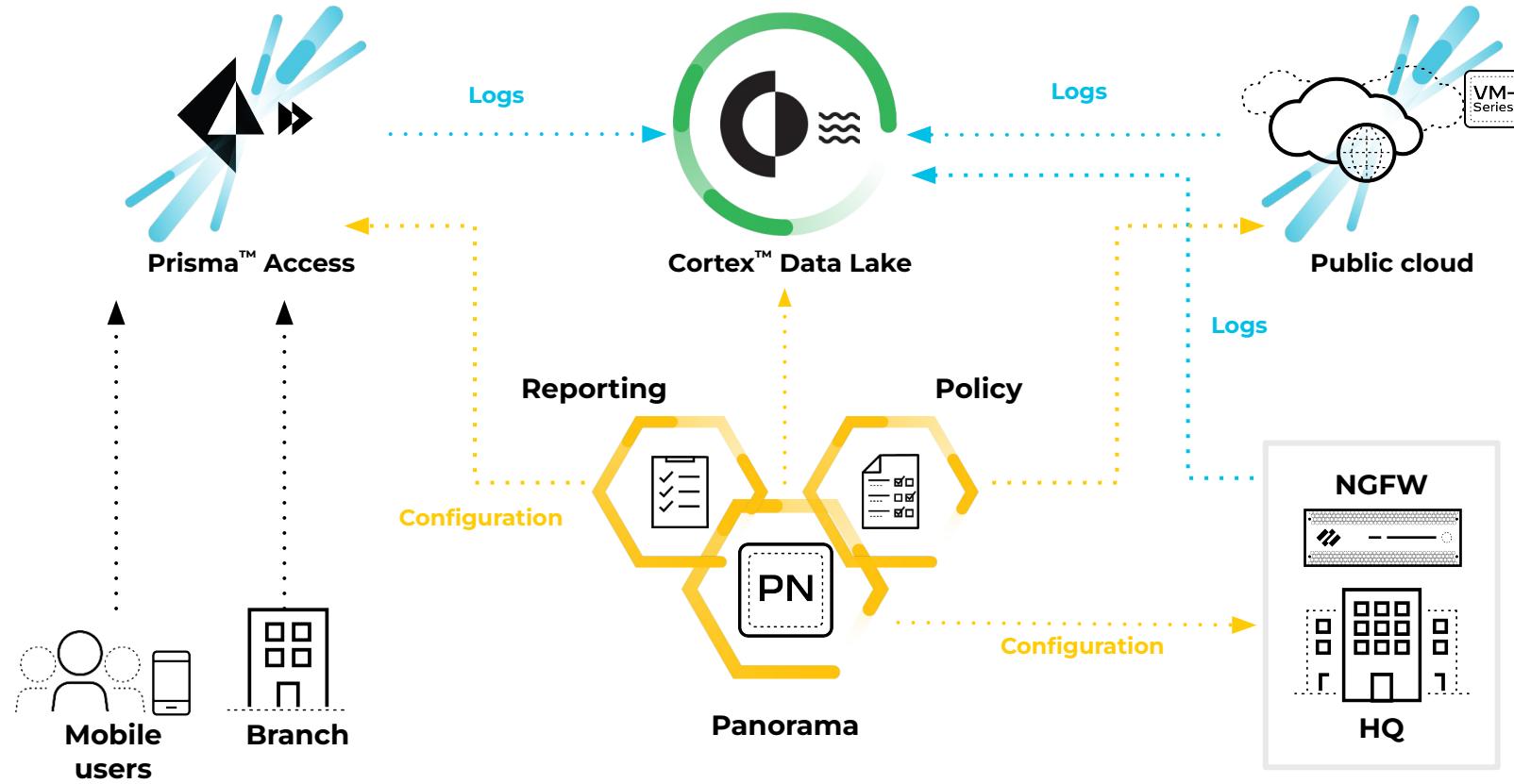


Powered by Familiar Architecture: CN-Series Runs On PAN-OS

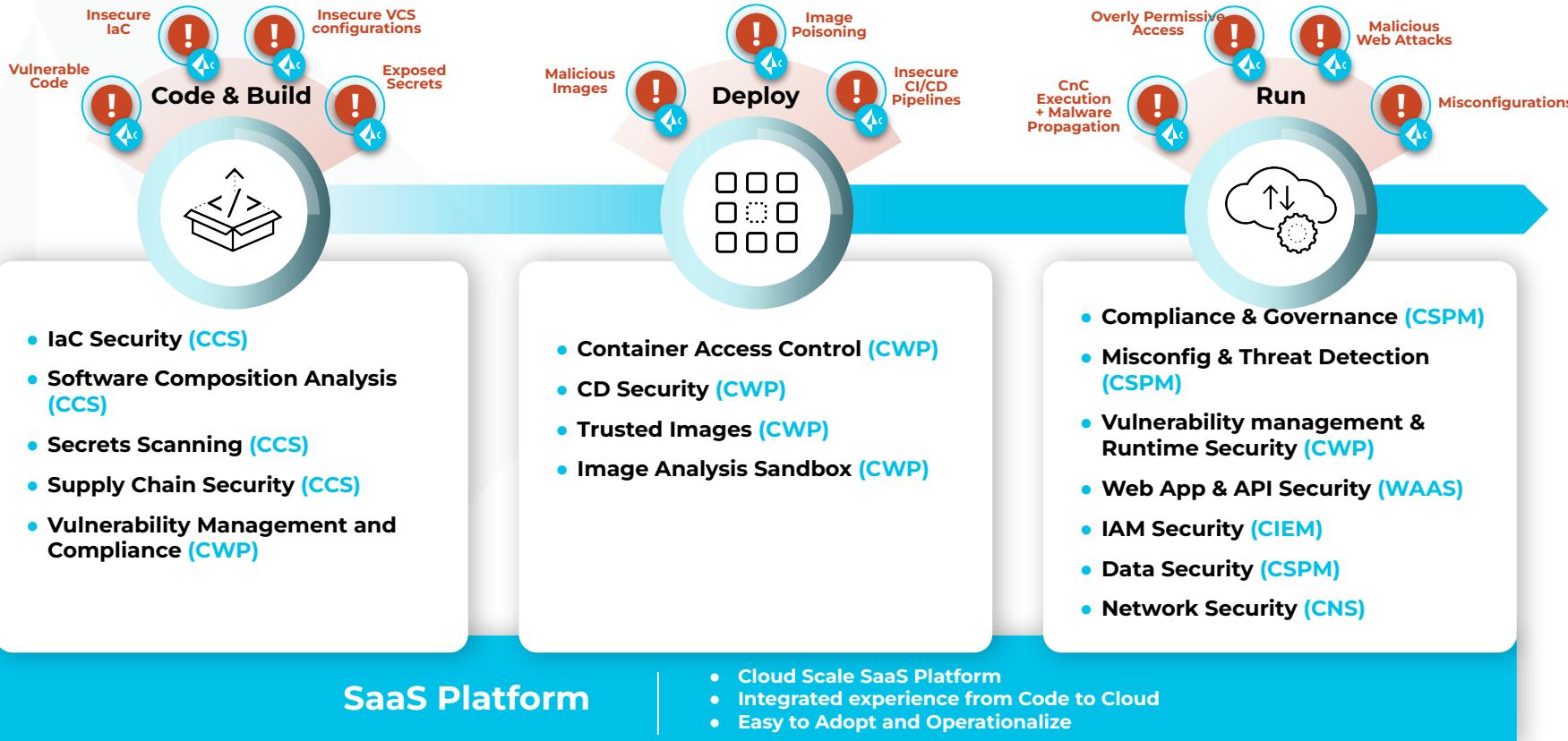


Panorama

Centralized Configuration, Visibility, Logging

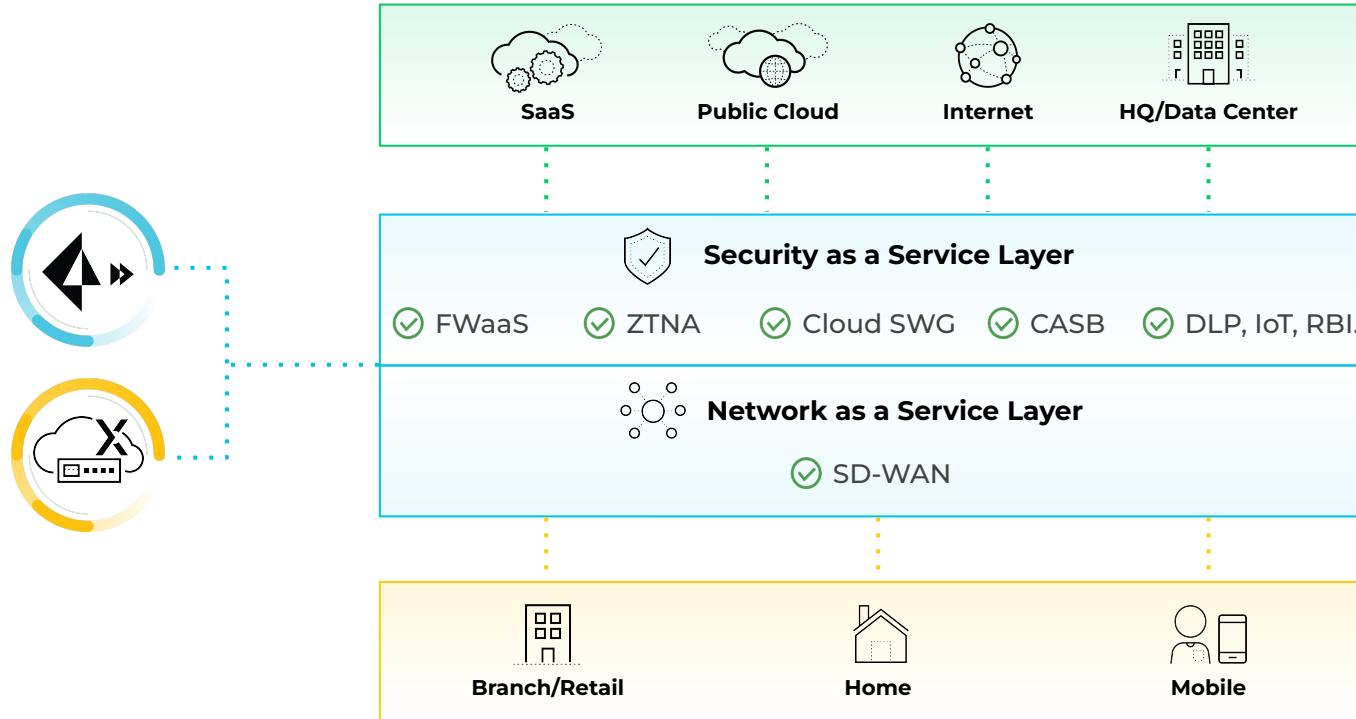


PRISMA CLOUD CAPABILITIES

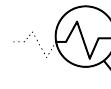
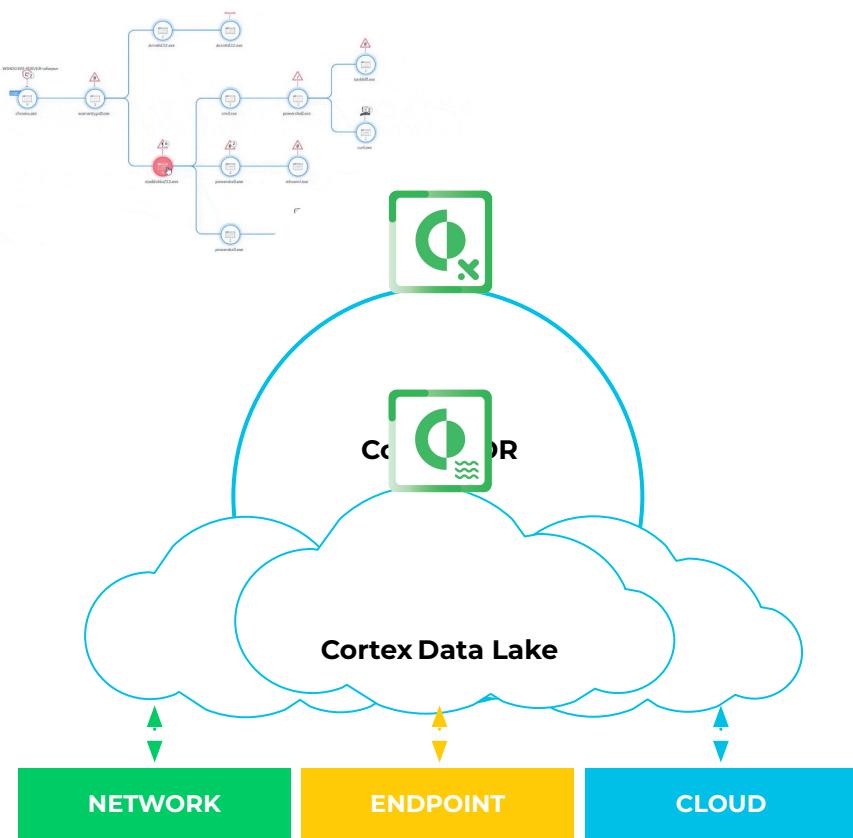


Prisma Access & PRISMA SD-WAN (AKA CloudGenix)

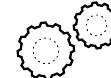
The Industry's Most Comprehensive SASE



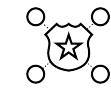
Cortex XDR Detects and Investigates Sophisticated Attacks



Automatically detect attacks using rich data and cloud-based behavioral analytics



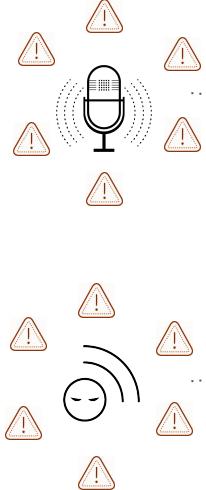
Accelerate investigations by stitching data together to reveal root cause



Tightly integrate with enforcement points to stop threats and adapt defenses

Cortex XSOAR Automates Security Workflows

Alert sources



Bad IP 1.1.1.1



XSOAR

350 + Integrations

Orchestration & Automation

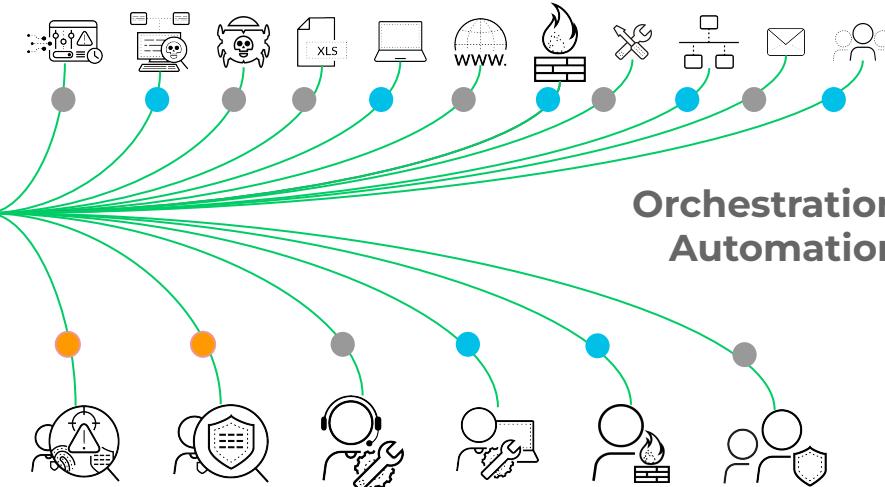
Automated playbooks

Unify threat feeds
with incident alerts

Enrich every tool and
process

Take automated
action with
confidence

External
threat intel
feeds



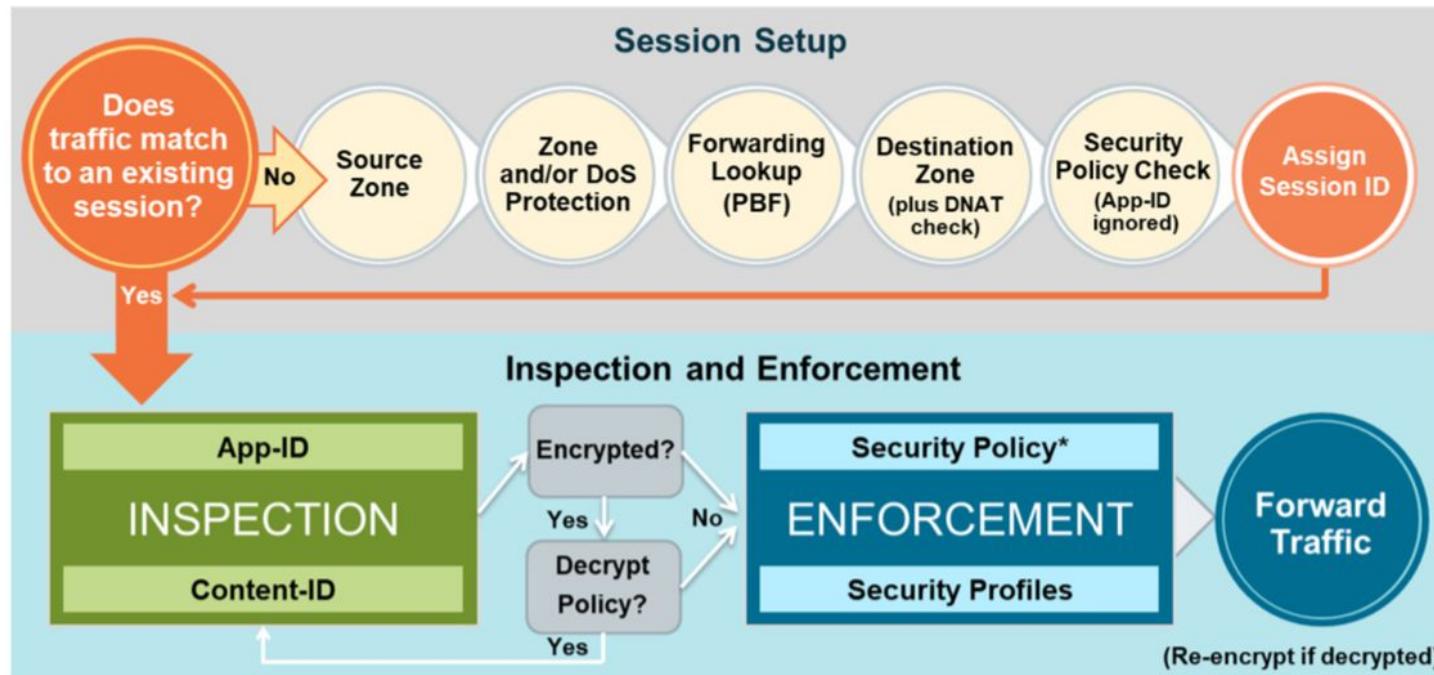
Real-time collaboration | Case management

1.1.2 Firewall Components

The screenshot displays a multi-step configuration process for a security policy rule:

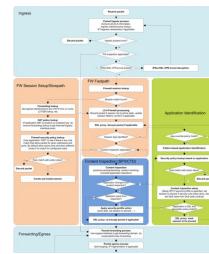
- Outermost Window:** Security Policy Rule (General tab).
 - Name: PCNSE Policy Example
 - Rule Type: universal (default)
 - Description: (empty)
 - Tags: None
 - Group Rules By Tag: None
 - Audit Comment: (empty)
- Second Window:** Security Policy Rule (Source tab).
 - Any
 - SOURCE ZONE: L3-Trust (selected)
- Third Window:** Security Policy Rule (Destination tab).
 - select
 - Any
 - DESTINATION ZONE: L3-Untrust (selected)
- Innermost Window:** Security Policy Rule (Actions tab).
 - Action: Allow (selected)
 - Profile Setting:
 - Profile Type: Profiles
 - Antivirus: best-practice
 - Vulnerability Protection: strict
 - Anti-Spyware: best-practice
 - URL Filtering: best-practice
 - File Blocking: Alert-All
 - Data Filtering: Alert any
 - WildFire Analysis: best-practice
 - Log Setting:
 - Log at Session Start:
 - Log at Session End:
 - Log Forwarding: default
 - Other Settings:
 - Schedule: None
 - QoS Marking: None
 - Disable Server Response Inspection:

Traffic Processing Sequence

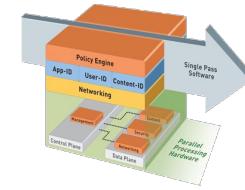


PACKET FLOW SEQUENCE IN PAN-OS

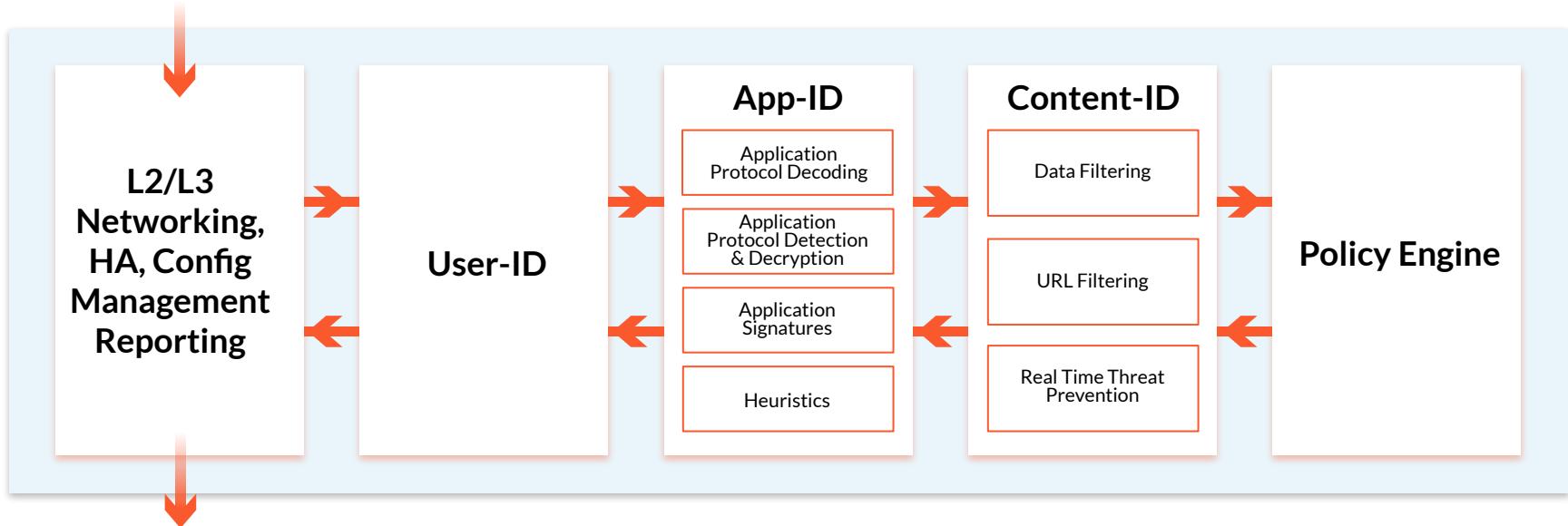
<https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081>



Single-Pass Security Processing



- Conventional traffic inspection tools “daisy-chain” protections, creating inefficiencies and visibility gaps
- Single-Pass Security Processing efficiently evaluates traffic and enforces security policy
- This unique capability makes the approach to preventing threats unique



1.1.3 Identify Panorama Components

The screenshot shows the Palo Alto Networks Panorama web interface. The top navigation bar includes links for Apps, OKTA, mail, LOOP, Products, SE, Sales, PANtech, tech, decks, demo, State, Lucidchart, Workday, SLED FY21 PoP, Vignettes, Qwiklabs, Deloitte, Ticket - ESP, and Reading List. The main menu has tabs for DASHBOARD, ACC, MONITOR, POLICIES (highlighted with a red box), OBJECTS (highlighted with a red box), NETWORK, and DEVICE. The POLICIES and OBJECTS tabs are currently active.

The left sidebar contains sections for Panorama, Device Group (All), Export, Global Filters (Risk, Sanctioned State, Show system events), Application View, and Application View (Risk, Bytes, Sessions, Threats, Content, URLs, Users, Source). The Application View table lists various applications with their risk levels, bytes transferred, sessions, threats, content, URLs, users, and source.

The central and right panels show network activity and user activity. The Network Activity section includes tabs for Application Usage, Threat Activity, Blocked Activity, Tunnel Activity, GlobalProtect Activity, and SSL Activity. The Application Usage section displays a treemap of application categories like internet-utility, media, unknown, collaboration, and business-systems. The User Activity section shows a line graph of bytes sent and received over time (12:15 to 13:00) and a table of user activity details.

1.1.4 Understand the PAN-OS Subscriptions & the Features they Enable

Threat Prevention Eliminates Known Threats



Detect and block
Exploitation



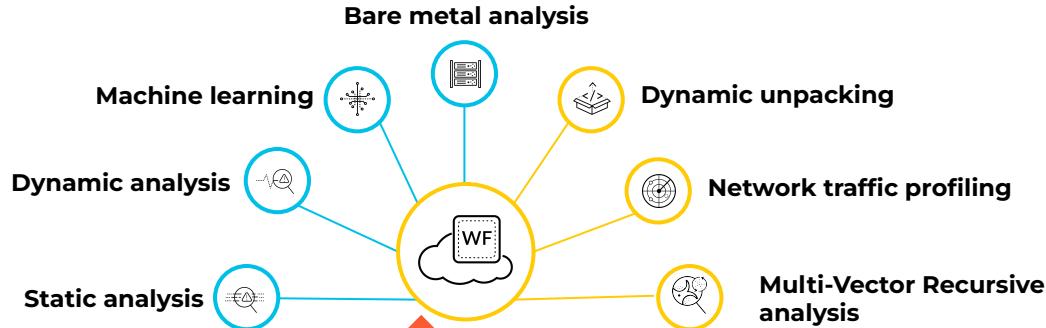
Based on Content
Not hash



Research grade
signatures

Combine with WildFire & URL Filtering: Protected at every stage of the attack lifecycle, including from both known and unknown threats

Detect and Prevent New Threats with WildFire Malware Analysis



Network

Endpoint

Cloud

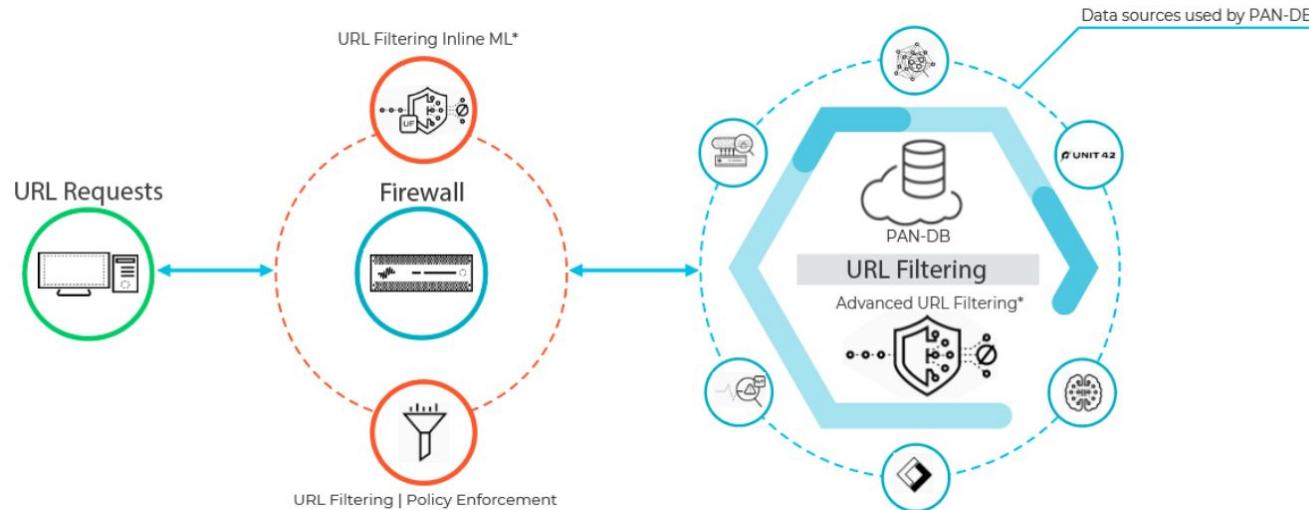
Partner
Ecosystem

Data collected from a vast
global community

Analysis techniques far beyond
traditional sandboxing

Automated protection against
multiple attack variants

URL Filtering Protection - PAN DB



Provides protections from both known and unknown threats based on PAN-DB classification. **Inline and real time.**

URL Filtering Profile (Read Only)

MODEL	DESCRIPTION	ACTION
Phishing Detection	Machine Learning engine to dynamically identify credential phishing pages	alert
Javascript Exploit Detection	Machine Learning engine to dynamically detect Javascript based exploitation attacks	block

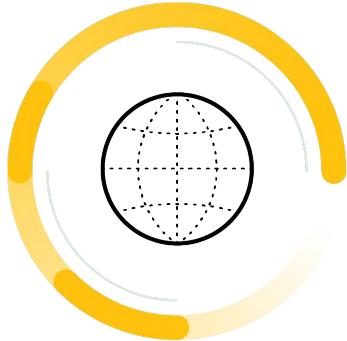
DNS Security



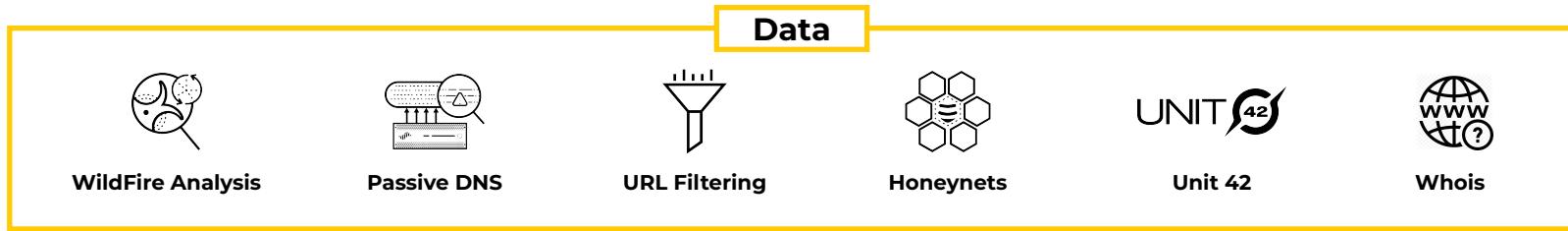
Blocks known
bad domains



Stops malicious DNS
traffic with ML and
predictive analytics



Integration with
NGFW means it
cannot be bypassed

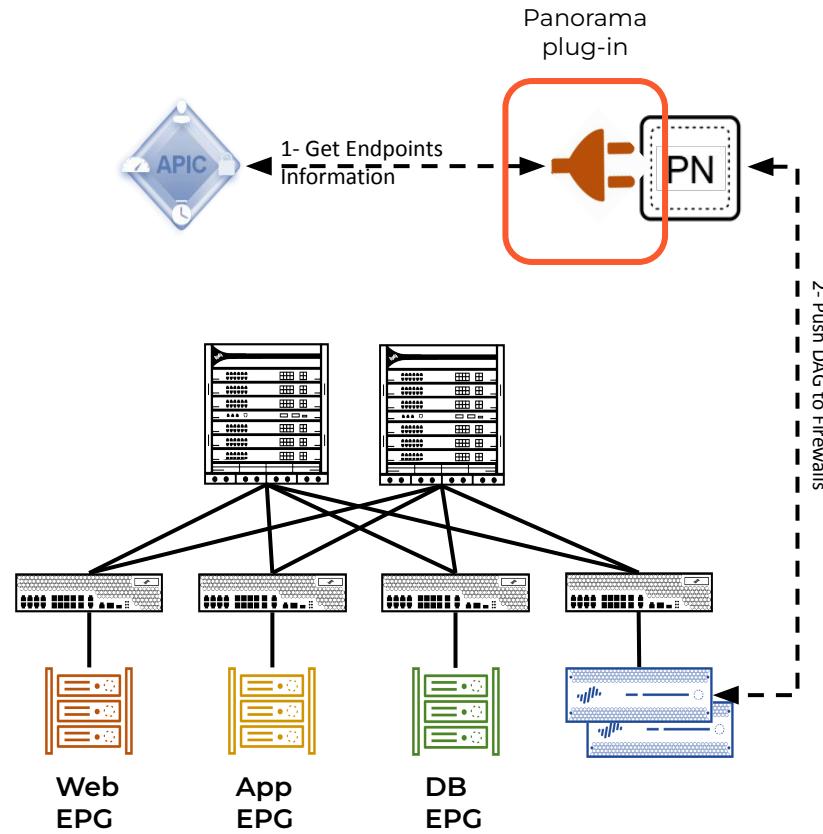


1.1.5 Understand Plug-in Components

Palo Alto Networks **plug-ins** manage the communication between Panorama and/or NGFW, Prisma Access and external systems.

In the diagram to the right the **plug-in** is managing the communication with a Cisco ACI APIC.

In public cloud use cases the **plug-in** manages the communication between a VM-Series NGFW and and the public cloud providers management interface API.



About Panorama Plugins

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-plugins/about-panorama-plugins#id181P8K0FOLT>

1.1.6 Heatmaps & Best Practice Assessment (BPA) reports

paloalto networks		Trending	Serial Number & Vsys	Zones	Zone Type	Area of Architecture	Tags	Rule Detail	Go to Best Practice Assessment	Security Policy Capability Adoption Heatmaps							
Source Zone	Destination Zone	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire		Threat Prevention (IPS)				URL-Filtering						
					WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %	
Lokalnettet_L3,VPN	untrust_vr1	27	26	1	100.0	100.0	92.3	100.0	100.0	100.0	100.0	0.0	92.4	96.3	92.3	100.0	
Lokalnettet_L3	untrust_vr1	18	16	2	100.0	100.0	56.3	93.8	100.0	93.8	100.0	0.0	36.9	55.6	100.0	100.0	
Lokalnettet_L3,Trust_DC,VPN	untrust_vr1	6	6	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	
any	untrust_vr1	5	0	5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	60.0	0.0	100.0	
Kjeller,Kontor,Stue	Kjeller,Kontor,Stue	3	3	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	33.3	100.0	
Clientless_VPN,Lokalnettet_L3,VPN	untrust_vr1	3	3	0	100.0	100.0	66.7	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	
Clientless_VPN,Lokalnettet_L3,Trust_DC,VPN	untrust_vr1	2	2	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	50.0	100.0	100.0	
Lokalnettet_L3,VPN,untrust_vr1	GP_Clientless_Portal,Management,untrust_vr1	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0	
untrust_GP	untrust_GP	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	100.0	100.0	
untrust_GP,untrust_vr1	untrust_GP,untrust_vr1	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	
untrust_vr1	untrust_vr1	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	
Garasje,Kjeller,Kontor,Stue	Garasje,Kjeller,Kontor,Stue	1	1	0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	0.0	0.0	0.0	100.0	
Grand Total:				77	65	12	98.5	98.5	75.4	96.9	98.5	96.9	98.5	0.0	59.7	74.0	87.7

Example of Security Rulebase Checks

Security Rulebase Checks

Perform best practice checks against security rulebase for each vsys instance.

Vsys

All

Only show records with warnings

Security Rulebase vsys: vsys1

Best Practice Check Results ⓘ

- ✓ Regional Deny Rules (Pass)
- ✗ Disabled Rules (Fail): It is recommended to remove disabled rules. (3 disabled rules exist)
- ✗ Interzone Deny Rule with Logging (Fail): It is recommended to have an any/any interzone deny rule with Log at Session End enabled
- ✗ Intrazone Deny Rule with Logging (Fail): It is recommended to have an any/any intrazone deny rule with Log at Session End enabled
- ✓ Malware / Phishing Deny Rule (Pass)
- ✗ HIP Profiles used in Rules (Fail): It is recommended to use HIP Profiles in rulebase
- ✗ User ID Rules without User ID enabled on Zone (Fail): The following zones do not have User ID enabled, but User ID is used on the rule: any (1 rule)

Security Best Practice Checks

Regional Deny Rules

Description

Ensure there is at least one rule denying traffic from certain regions in security rulebase

Rationale

Region-based rules help in having control in either allowing or denying traffic from certain region or nation. Regions are prebuilt in the firewall and we can add them in source or destination address fields in the security policy. For instance, if a company has offices in country A, B and C and if the company starts noticing surge in traffic (DoS or flood) from a country X, which they are not expecting, then they can create a region-based policy to deny any traffic coming from the source region X.

Reference URL(s)

<https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Block-Traffic-Based-Upon-Countries/ta-p/52217>

Disabled Rules

Description

Ensure no disabled rules exist in security rulebase

Rationale

Disabled rules are in place only because these security rules were created for temporary reasons, testing reasons, created long time ago which are not in use now or so on and they are currently not necessary to the network. If a security rule is not necessary in the network then it has to be deleted. We should have only the required policies configured.

Interzone Deny Rule with Logging

Description

Ensure there is an any/any interzone deny rule with Log at Session End in security rulebase

Rationale

Firewall has a default security policy at the end of security rulebase for interzone traffic to be denied. This rule is of type interzone. The policy ensures that interzone traffic is not permitted by default and if we have to permit traffic between two different zones then it has to be explicitly configured between those two zones. The default Interzone rule does not have 'log at session end' option enabled. Also, we cannot modify this setting for this rule. It is necessary to log traffic that is getting denied if it is interzone to identify any threat activity. With the default rule, as logging is not enabled, we would not have visibility and hence, this Interzone rule has to be configured to log the traffic matching this policy.

Reference URL(s)

<https://live.paloaltonetworks.com/t5/Management-Articles/What-are-Universal-Intrazone-and-Interzone-Rules/ta-p/57491>

1.2 Determine & asses appropriate interface types for various environments

Types of Interfaces

Palo Alto Networks firewalls support several different interface types: TAP mode, virtual wire mode, Layer 2, Layer 3, and aggregate.

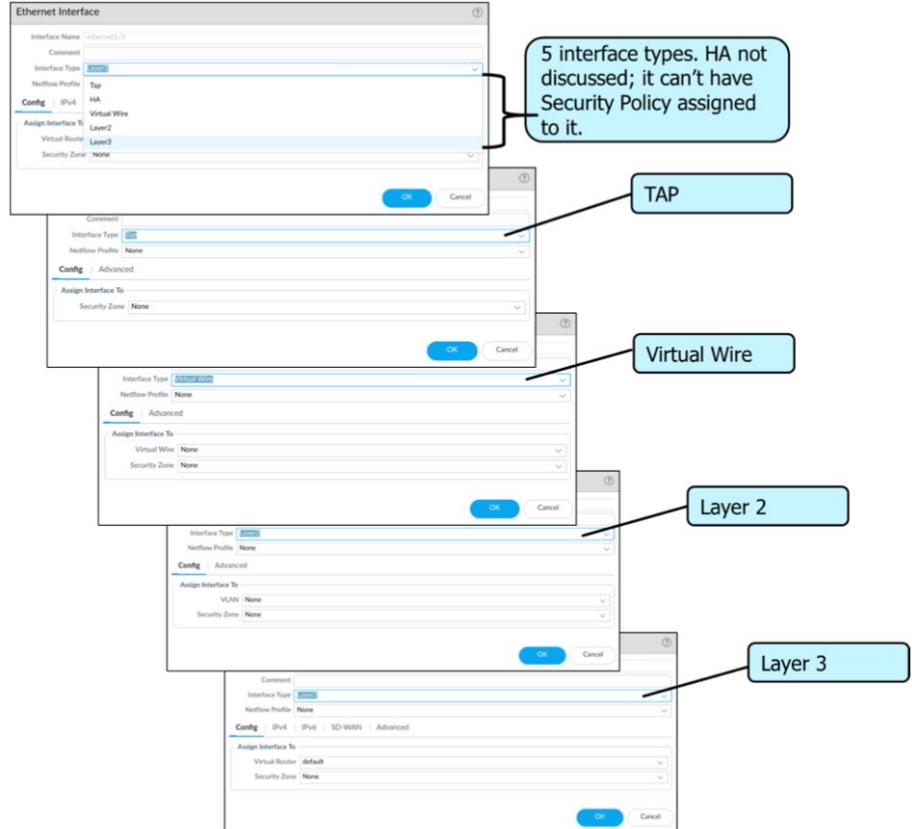
A single firewall can freely intermix interface types to meet any integration need. The decision about which interface configuration to choose depends on functional need and existing network integration requirements.

1.2.1 Layer 2 interfaces

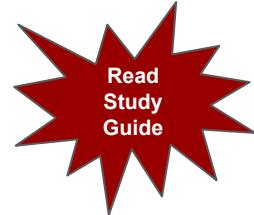
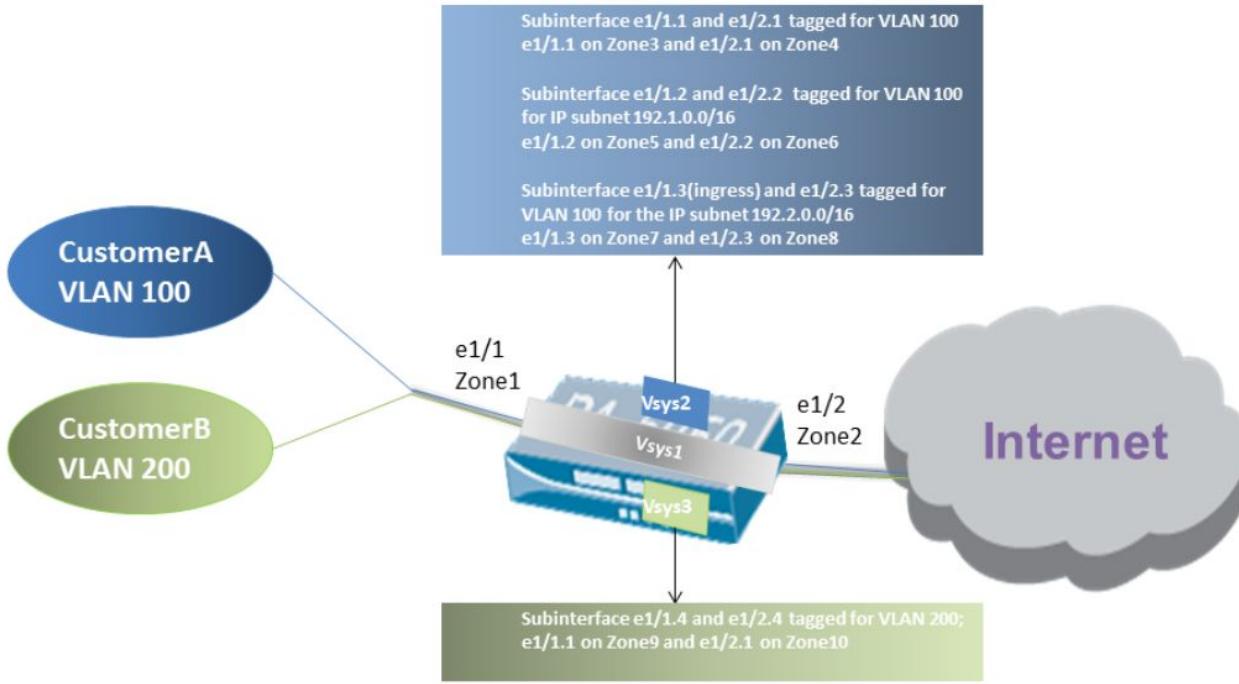
1.2.2 Layer 3 interfaces

1.2.3 Virtual Wire interfaces

1.2.4 Tap interfaces



1.2.5 Subinterfaces



1.2.6 Tunnel Interfaces

Tunnel Interface

Interface Name: tunnel . 67

Comment: PCNSE Example Tunnel Interface

Netflow Profile: PCNSE NetFLOW

Config | IPv4 | IPv6 | Advanced

Assign Interface To:

Virtual Router	default
Security Zone	vpn

OK Cancel

PAN-OS Site-2-Site VPN based on route based approach. Tunnel interface is used to establish VPN connectivity. Traffic is routed through tunnel via routes pointed to tunnel interface.

Tunnel Interface

- Assigned to virtual router
- Assigned to Security Zone
- IP Address only required for “Tunnel Monitoring” or “Dynamic Routing Protocols” (BGP or OSPF)

Virtual Router - Static Route - IPv4

Name	PCNSE-site-2
Destination	10.67.0.24
Interface	tunnel.67
Next Hop	None
Admin Distance	10
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

Path Monitoring

Failure Condition: Any All Preemptive Hold Time (min): 2

NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

+ Add - Delete

OK Cancel

1.2.7 Aggregate Interfaces

Media can differ (copper & optic) but - speed (1 GB / 10 GB) & type (L2/L3) must stay the same
You can group 8 interfaces maximum

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html>

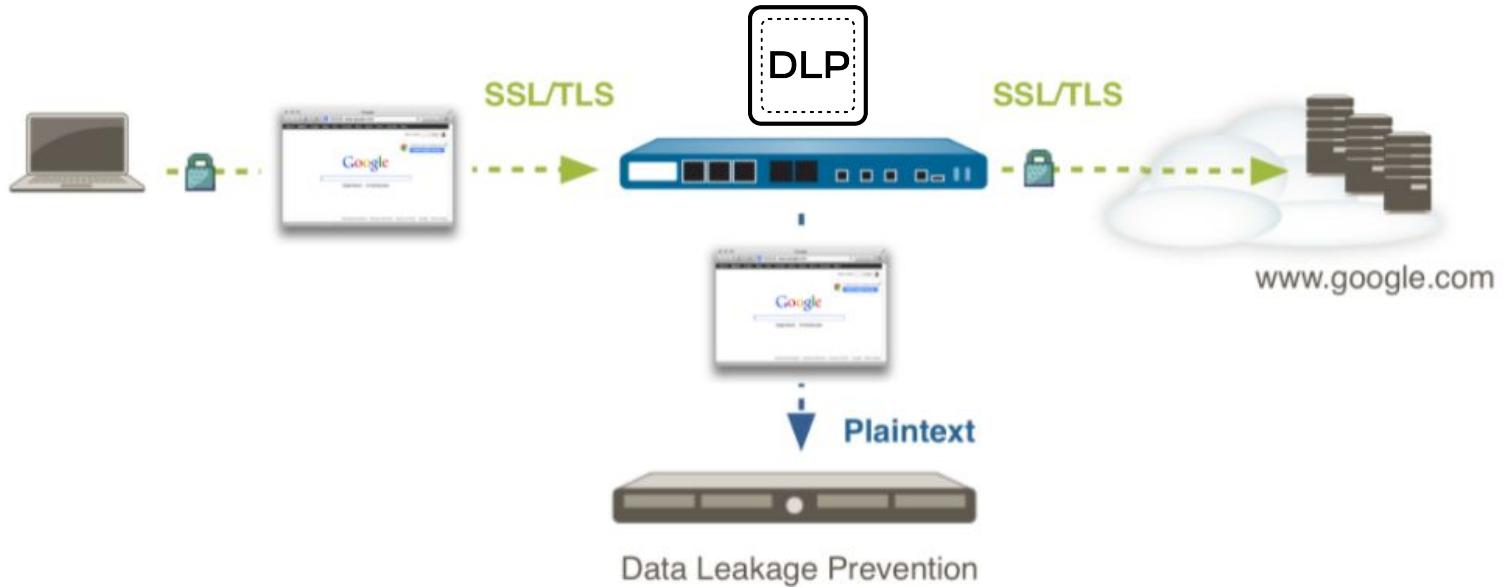
1.2.8 Loopback Interfaces

The screenshot shows the 'Loopback Interface' configuration dialog. At the top, it displays the 'Interface Name' as 'loopback' and the 'Comment' as 'PCNSE Loopback Example'. Under 'Netflow Profile', it shows 'None'. Below these fields are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced', with 'Config' currently selected. In the 'Assign Interface To' section, the 'Virtual Router' is set to 'default' and the 'Security Zone' is set to 'L3-Untrust'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Loopback Interface Uses

Router-ID (used BGP/OSPF)
NAT Tricks
DNS sinkhole Destinations
GP Service Interfaces

1.2.8 Decrypt Mirror Interfaces



How to Configure Decrypt Mirror:

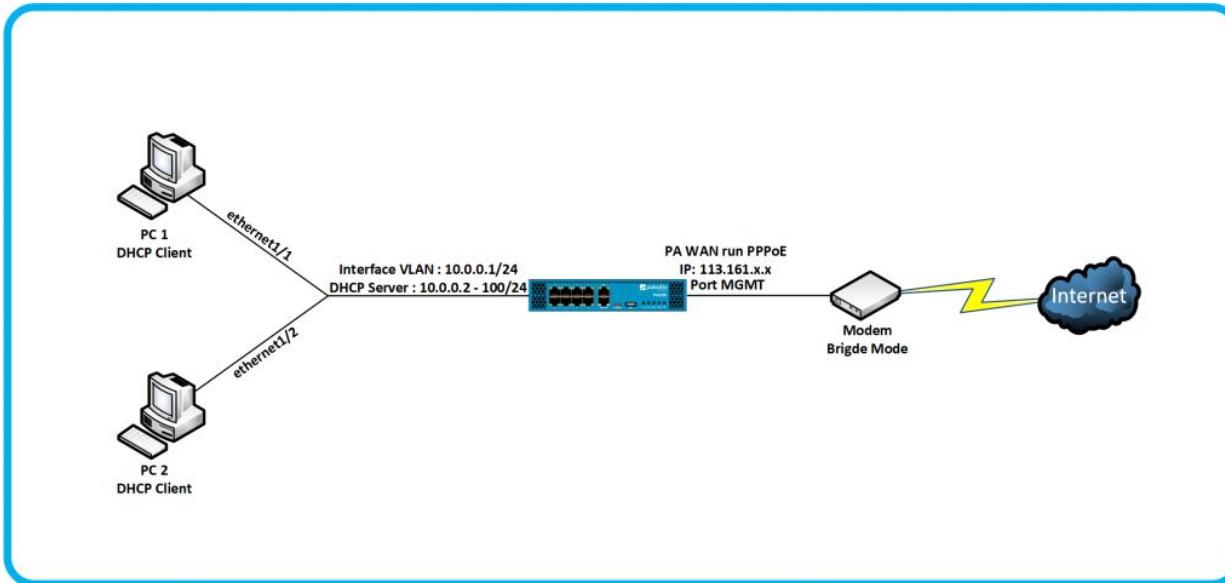
<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGDCA0>

Decryption Mirroring:

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-concepts/decryption-mirroring.html>

1.2.8 VLAN Interfaces

Logical interface useful in conjunction with L2 interface physical type to provide L3 switching

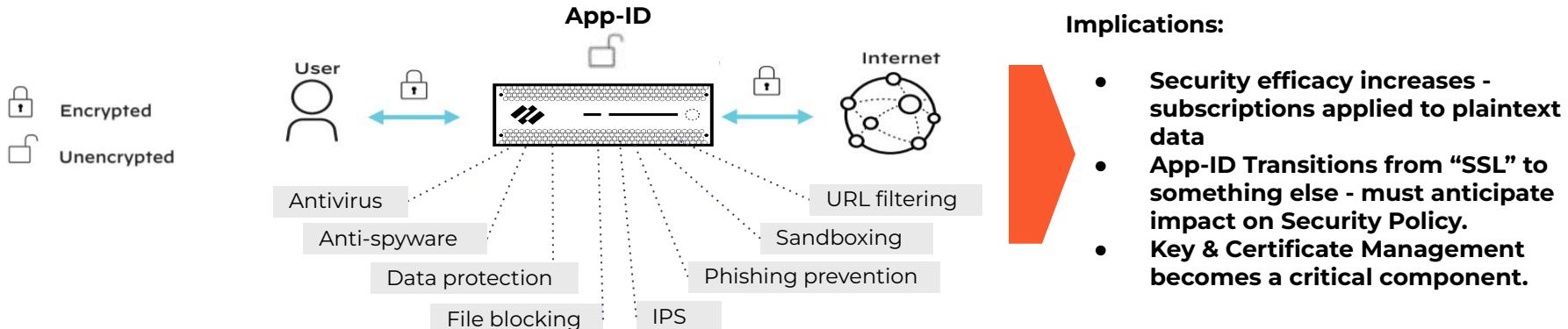


How Do I Configure a VLAN Interface:

<https://techbast.com/2021/03/palo-alto-firewall-how-config-vlan-interface.html>

1.3 Identify decryption deployment strategies

1.3.1 Risks and implications of enabling decryption



Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.

Offers rich visibility into TLS traffic — such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more — even without decrypting.

Control over use of legacy TLS protocols, insecure ciphers, and incorrectly configured certs to mitigate risks.

Easy deployment of decryption and built-in logs to troubleshoot issues, such as applications with pinned certs.

Flexibly decrypt based on URL category, source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.

Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics purposes

1.3.2 Use Cases

Reasons to Deploy Decryption in Your Environment



Phishing and Credential Attacks

Identify and prevent corporate computer and internet usage policy violations



Data Loss and Compliance Check

Stop the loss of sensitive data such as personally identifiable information (PII), intellectual property (IP)



Threat

Prevent the transmit of harmful files, malware, virus and spyware. Stop command and control callbacks.



Inside Behavior

Identify malicious, negligent, and non-compliant users, along with infected devices

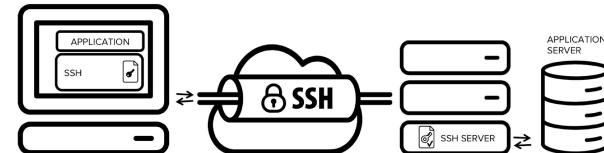
1.3.3 Decryption Types

SSL Decryption

- Policy Based
- Outbound Decryption
 - Forward Proxy
- Inbound Decryption
 - Stream Based
 - Reverse Proxy (PFS ciphers)
- Certificate Requirements - Outbound
 - NGFW as Trusted 3rd Party
 - Self Signed
 - Subordinate CA from PKI
 - Generates Certs on behalf of destination sites
- Certificate Requirements - Inbound
 - Public/Private key pair

SSH Decryption

- Policy Based
- SSH Proxy
- “ssh-tunnel” App-ID to prevent circumvention of security policy controls
- Note: changes ssh fingerprint, implementation issue for automated processes during implementation time. Notification planning is warranted.



1.3.4 Decryption Profiles & Certificates

Certificates Used with Decryption	Description
Forward Trust (used for SSL Forward Proxy decryption)	The certificate the NGFW presents to clients during decryption if the site the client is attempting to connect to has a certificate signed by a CA that the NGFW <u>trusts</u> .
Forward Untrust (used for SSL Forward Proxy decryption)	The certificate the NGFW presents to clients during decryption if the site the client is attempting to connect to has a certificate signed by a CA that the NGFW does not trust .
SSL Inbound Inspection	The certificates of the servers on your network you want to perform inbound inspection of traffic. Import both the <u>server certificate</u> and the <u>private key</u> .

Protect Users from Bad Sites

Decryption Profile

Name: strict

Decryption Mirroring:

Interface: None
 Forwarded Only

SSL Decryption: No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | SSL Protocol Settings

Server Certificate Verification:

- Block sessions with expired certificates
- Block sessions with untrusted issuers
- Block sessions with unknown certificate status
- Block sessions on certificate status check timeout
- Restrict certificate extensions [Details](#)
- Append certificate's CN value to SAN extension

Unsupported Mode Checks:

- Block sessions with unsupported versions
- Block sessions with unsupported cipher suites
- Block sessions with client authentication

Failure Checks:

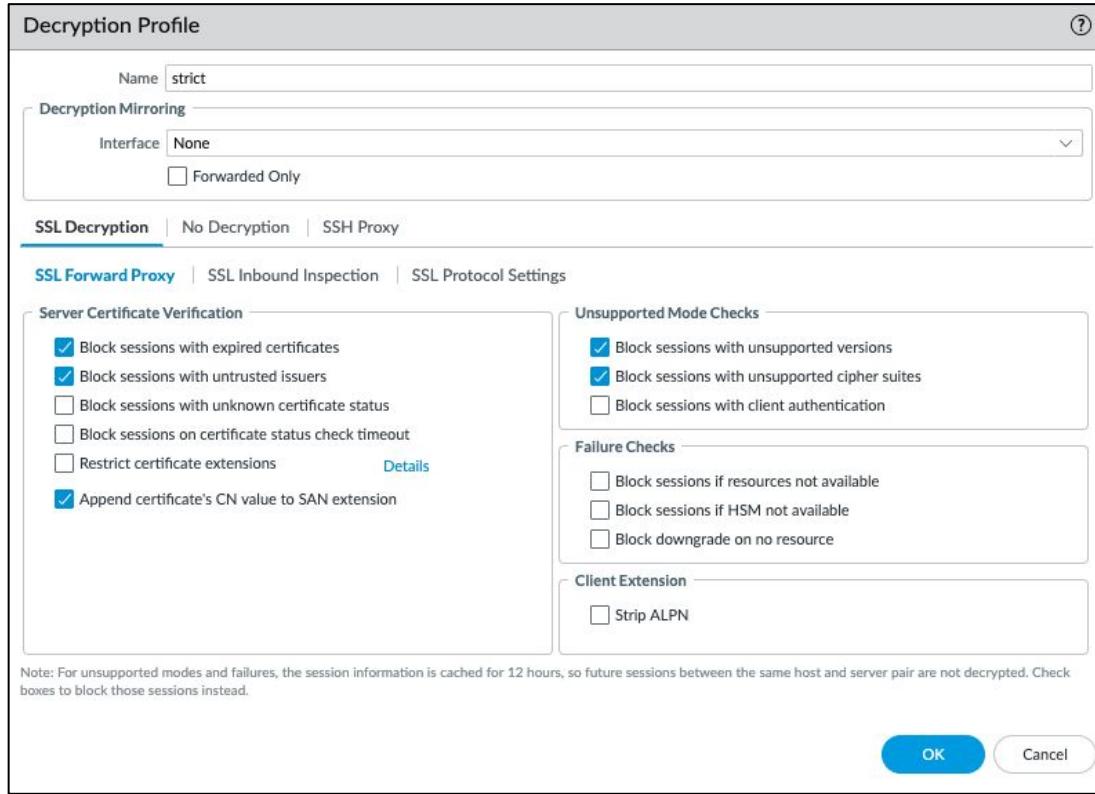
- Block sessions if resources not available
- Block sessions if HSM not available
- Block downgrade on no resource

Client Extension:

- Strip ALPN

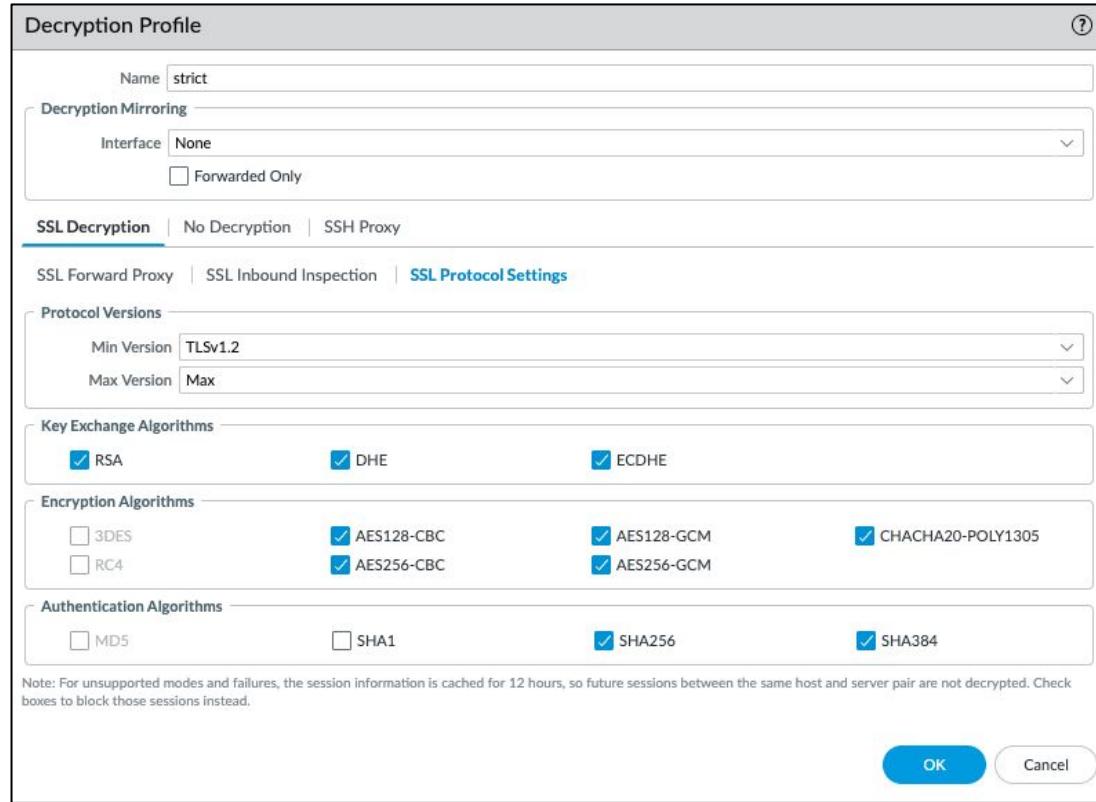
Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

OK Cancel

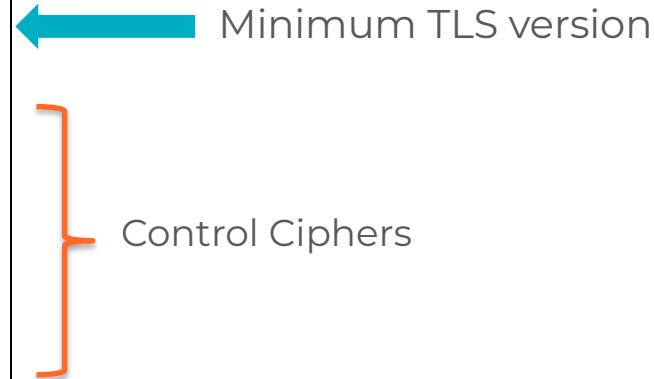


- Don't let users “click through” to sites with bad certificates
- Don't allow undecryptable sessions

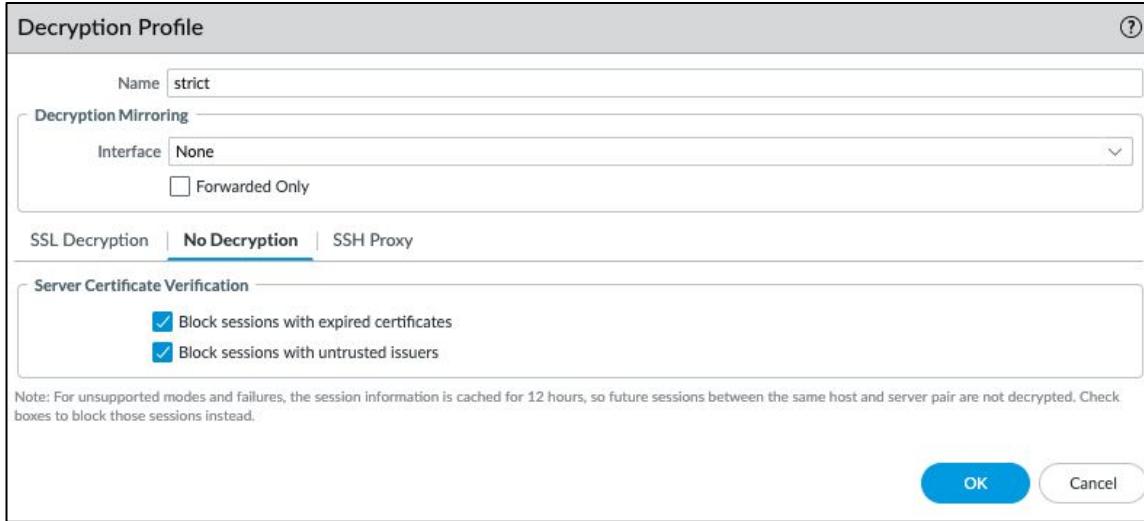
Granular Control on Ciphers



- Avoid **weak** protocols and ciphers



Control Application Behavior



- Block Anonymizers

Decryption Deep Dive!

Decrypting Decryption: <https://www.youtube.com/watch?v=7LWRULh8z18>

Have you ever wondered how Secure Socket Layer (SSL) works? Have you ever been perplexed about what a Client Hello or a Server Hello is? Or do you want to really understand how a Next-Generation Firewall (NGFW) performs decryption? Then this episode is for you! Shakti will be your decryption mentor by showing exactly how the process of SSL Forward Proxy decryption happens!

1.3.5 Decryption Policy in the Firewall

The image displays four overlapping windows of a firewall configuration interface, specifically for defining a Decryption Policy Rule named "Decrypt-HTTP2-1".

- General Tab:** Shows the rule name "Decrypt-HTTP2-1", a description field, and a "Tags" section indicating "None".
- Source Tab:** Configures the source zone as "L3-Trust" and the source address as "10.0.0.10-10.255.255.255".
- Destination Tab:** Configures the destination zone as "L3-Untrust" and the destination address as "Any".
- Service/URL Category Tab:** Configures the service as "service-https" and the URL category as "Any".
- Options Tab:** Set to "Decrypt" and "SSL Forward Proxy". It also includes a "Decryption Profile" dropdown set to "default" and "Log Settings" for SSL handshake logs.

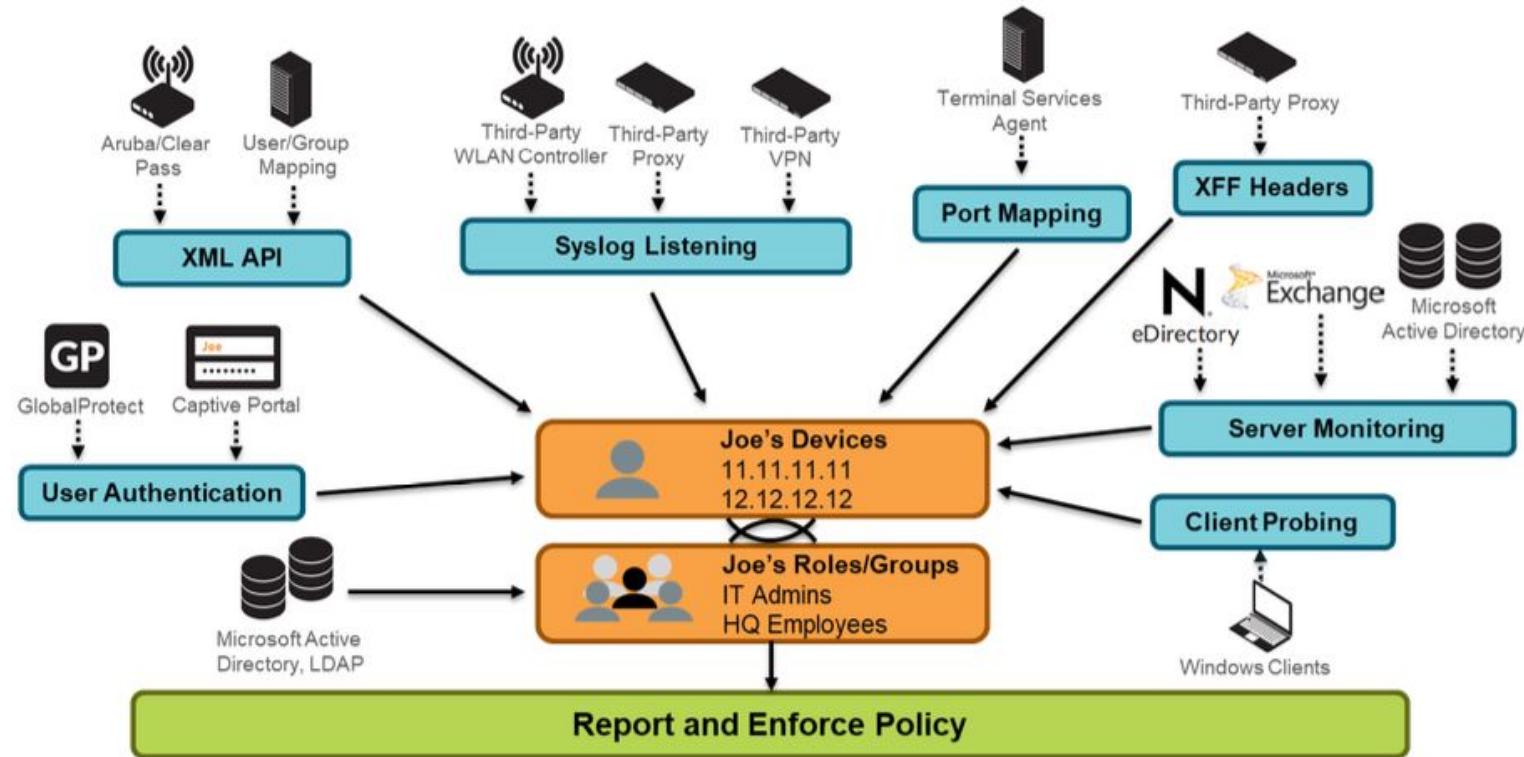
1.3.6 Configure SSH Proxy

The screenshot shows the configuration of a Decryption Policy Rule named "SSH Proxy Rule". The interface is divided into four main tabs: General, Source, Destination, and Options.

- General Tab:** Shows the rule name "SSH Proxy Rule", a description field, and a "Tags" section containing "L3-Trust".
- Source Tab:** Displays source criteria: "Any", "SOURCE ZONE" (set to "any"), "SOURCE ADDRESS" (set to "any"), "SOURCE USER" (set to "any"), and "SOURCE DEVICE" (set to "any").
- Destination Tab:** Displays destination criteria: "Any", "DESTINATION ZONE" (set to "any"), and "SERVICE" (set to "TCP-22").
- Options Tab:** Contains settings for Action (set to "Decrypt"), Type ("SSH Proxy"), and Decryption Profile ("SSH decrypt-profile"). It also includes Log Settings for "Log Successful SSL Handshake" (unchecked) and "Log Unsuccessful SSL Handshake" (checked), and a Log Forwarding field set to "None".

1.4 Enforce User-ID

1.4.1 Methods of building user-to-IP mappings.

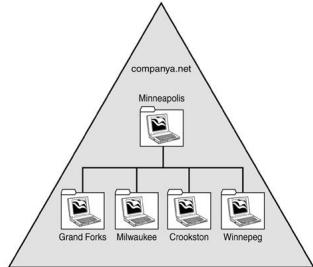


1.4.2 Determine if User-ID agent or agentless should be used

1.4.3 Compare & Contrast User-ID Agents

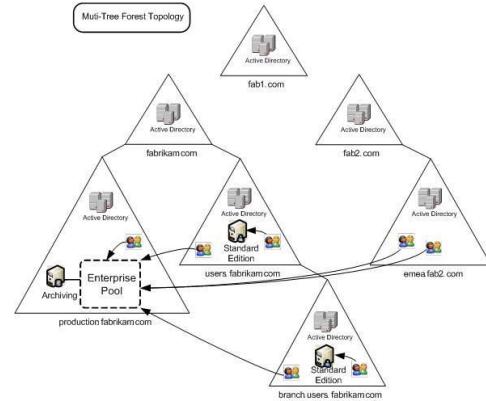
Agentless (PAN-OS) - Built-in Agent

- Small/Medium Deployment
- <10 Domain Controllers
- Redistribution of User-ID Between PAN-OS Devices Collected from AD, GP or Captive Portal.
- Convenient - potentially close to resources

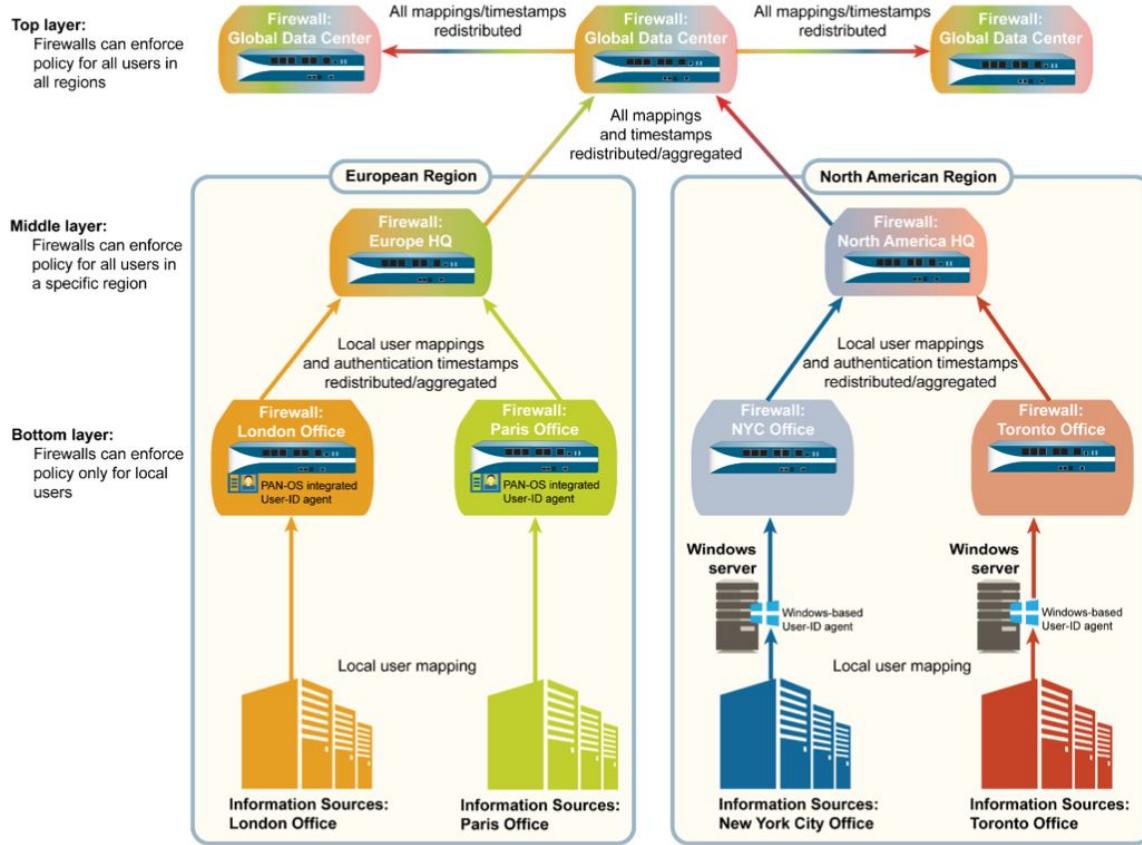


User-ID Agent (Windows)

- Medium/Large Deployment
- >10 Domain Controllers
- Multi-Domain Architecture
- Windows 2008 or Later
- Scalable



1.4.4 Methods of User-ID Redistribution



User Meta-Data Redistribution: Easy Configuration

The screenshot shows the PA-VM interface with the following components:

- Top Navigation Bar:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted).
- Left Sidebar:** Setup, High Availability, Config Audit, Password Profiles, Administrators, Admin Roles, Authentication Profile, Authentication Sequence, User Identification, **Data Redistribution** (highlighted), Device Quarantine, VM Information Sources, Troubleshooting.
- Main Content Area:** A table listing Agents. The columns are NAME, ENABLED, PORT, SERIAL NUMBER, IP USER MAPPINGS, and IP TAGS. Three agents are listed: Global_Protect, HQ-FW, and User-ID_Agent, all with Port 5007 and checked in both IP User Mappings and IP Tags columns.
- Red Boxes and Annotations:**
 - A red box surrounds the "Agents" tab in the navigation bar.
 - A red box surrounds the "Include/Exclude Networks" tab in the navigation bar.
 - A yellow box contains the text "Who is receiving from this Firewall".
 - A green box contains the text "Filter the IP-Ranges".
 - A green box contains the text "Filter the Data types to receive".
- Right Panel:** "Add a Data Redistribution Agent" dialog box.
 - Fields: Name (Global_Protect), Enabled (checked), Add an Agent Using (Host and Port selected), Host (empty), Port (5007), Collector Name (empty), Collector Pre-Shared Key (empty), Confirm Collector Pre-Shared Key (empty).
 - Buttons: OK, Cancel.
 - Data type:** A red box highlights the "Data type" section with three checkboxes:
 - IP User Mappings
 - IP Tags
 - HIP
 - Quarantine List
 - User Tags

Dedicated Area to Configure
and Troubleshoot

Filter the IP-Ranges

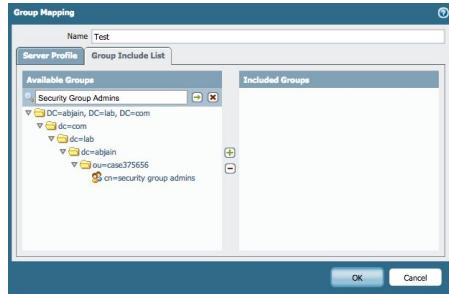
Who is receiving from
this Firewall

Filter the Data types to receive

1.4.5 Methods of Group Mapping

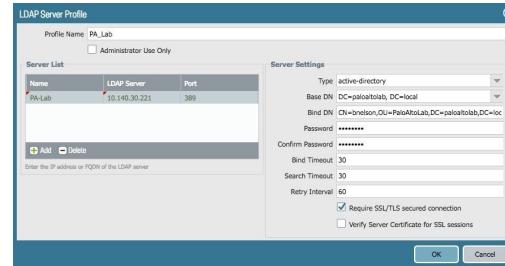
Single Domain Group Mapping

- Use a LDAP Server Profile to retrieve group-to-user mappings from a domain controller.
- Use the **User Identification → Group Mapping Settings → Group Include List filter** to eliminate unwanted groups from being placed on the PAN-OS device.

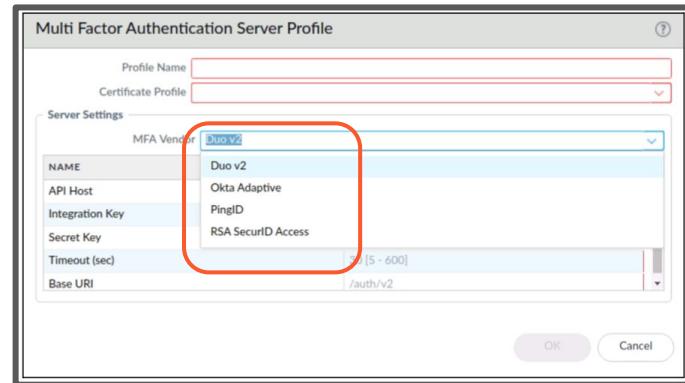
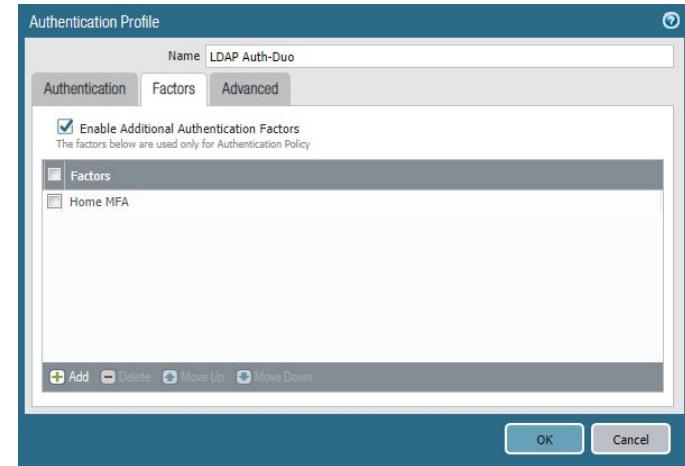
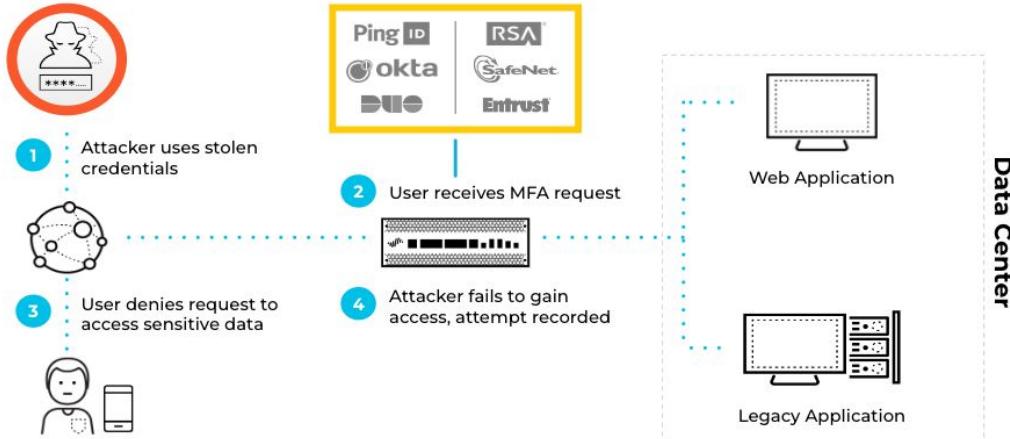


Multi-Domain Group Mapping

- Use a LDAP Server Profile to retrieve group-to-user mappings from to domain controller - in each domain or forest.
- Make sure usernames come across uniquely - append domain names to usernames (domain\username or username@domain.local)



1.4.6 Server Profile & Authentication Profile



PCNSE Prep: Authentication Policy with MFA
<https://www.youtube.com/watch?v=GjyMotd5YuE>

1.5 Determine when to use Authentication policy and methods for doing so

1.5.1 Purpose of, and use case for, Authentication policy

Authentication Policy Rule

	Name	Tags	Source Zone	Address	User	HIP Profile	Destination Zone	Address	Service	Authentication Enforcement	Log Settings	Hit Count
1	Exclude-Auth-rule	none	L3-Trust	any	any	any	L3-Untrust	any	service-http service-https	default-no-captive-portal		80
2	CP-Auth-Rule	none	L3-Trust	any	any	any	L3-Untrust	any	service-http service-https	AzureAD-web-form-Sh...	Log Authentication Tim...	31707

Authentication Policy is triggered for access to specific resources - the idea is to “Step-up” authentication to sensitive resources. Authentication Policy defines when that is appropriate.

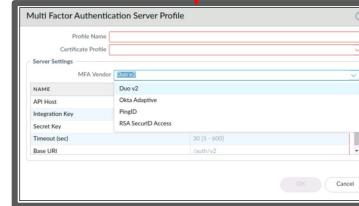
Note: the authentication is enabled through captive portal capability.

PCNSE Prep: Authentication Policy with MFA
<https://www.youtube.com/watch?v=GjyMotd5YuE>

AD Authentication via Authentication Profile - 1st Factor

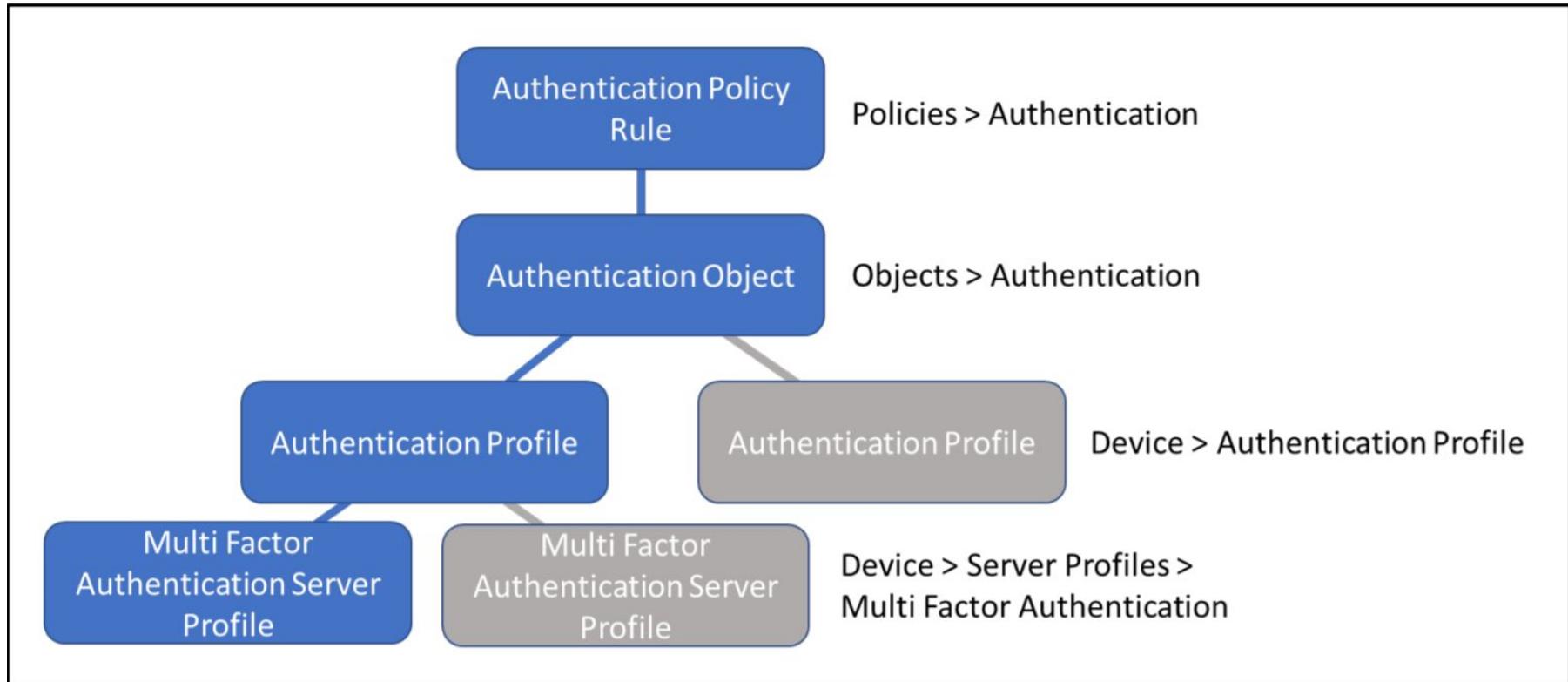


MFA Authentication via Additional Factors - 2nd Factor



1.5.2 Dependencies

The following figure shows the relationship of the required objects to configure the Authentication policy rule.



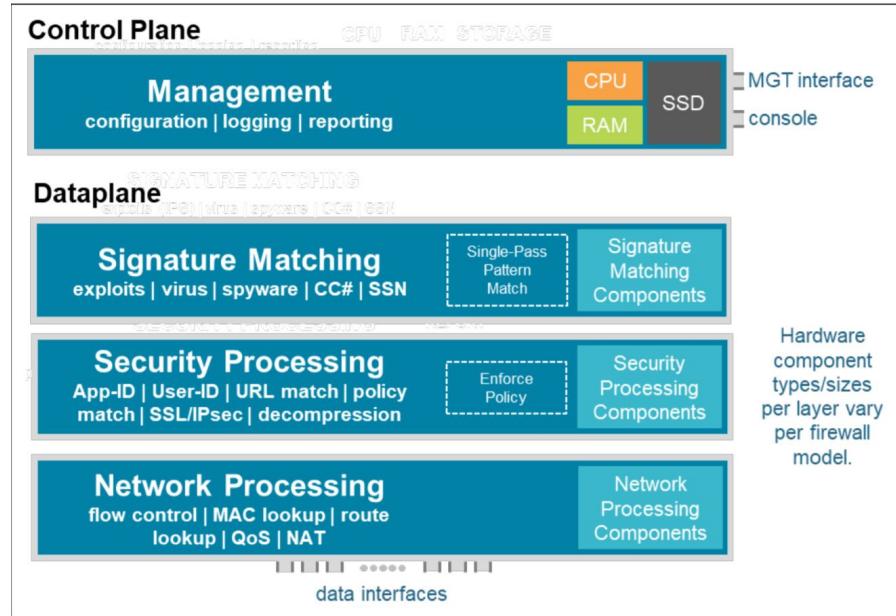
1.6 Differentiate between the fundamental functions that reside on the management plane and data plane

1.9.1 Identify functions that reside on the management plane.

Palo Alto Networks maintains the management plane and data-plane separation to protect system resources.

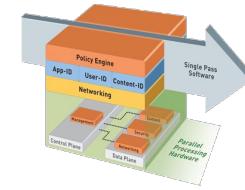
Functions That Reside in the Management Plane

- Configuration management
- Logging
- Reporting functions
- User-ID agent process
- Routing Protocols

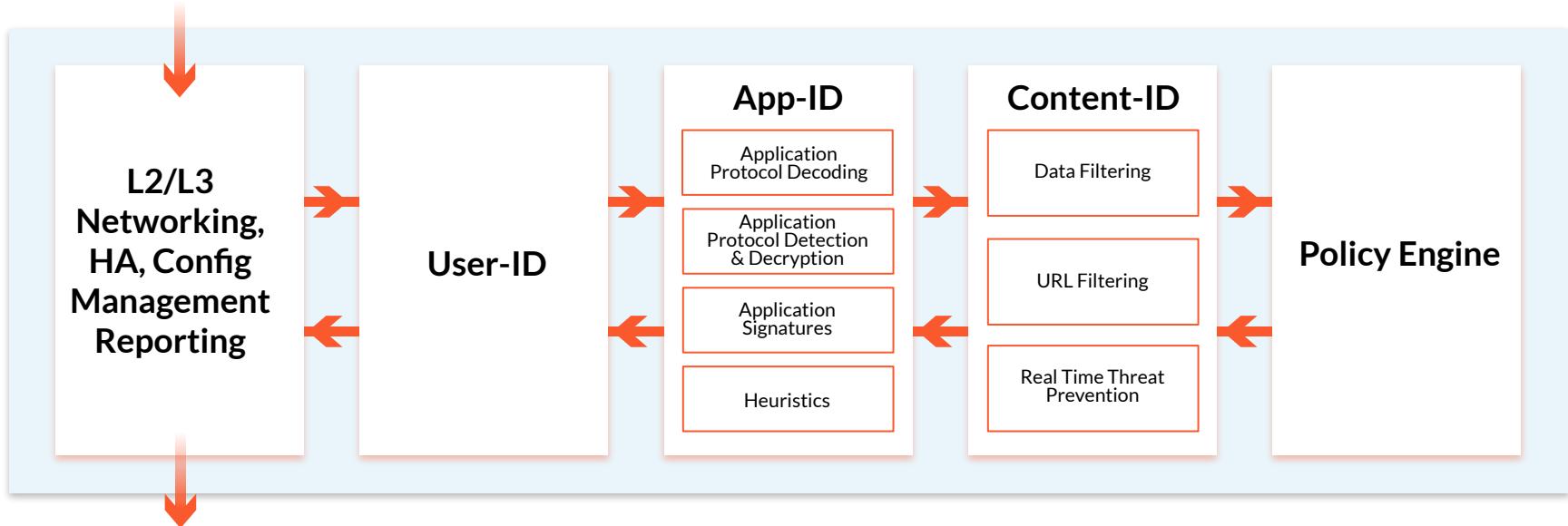


PA-220 Architecture

Single-Pass Security Processing



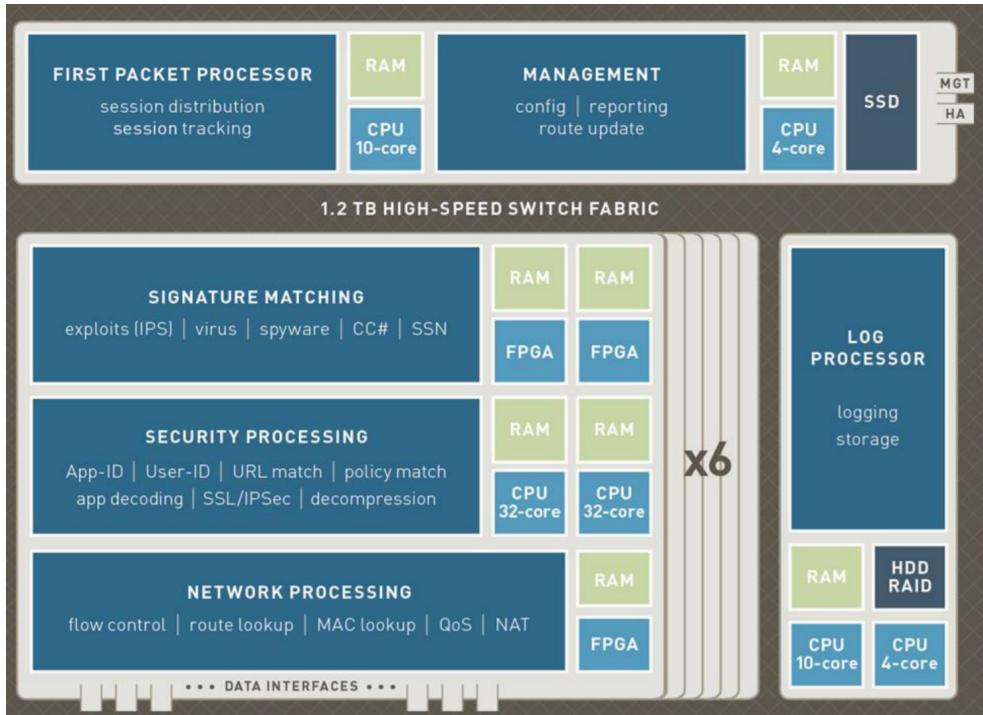
- Conventional traffic inspection tools “daisy-chain” protections, creating inefficiencies and visibility gaps
- Single-Pass Security Processing efficiently evaluates traffic and enforces security policy
- This unique capability makes the approach to preventing threats unique



Functions That Reside in the Data Plane

The following figure provides an overview of the PA-7000 Series architecture.

On the PA-7000 Series firewalls, dedicated log collection and processing is implemented on a separate card.



PA-7000 Architecture