paloalto NETWORKS

PCNSE

PCNSE Bootcamp v10.1

Exam Domain #1 Planning & Core Concepts

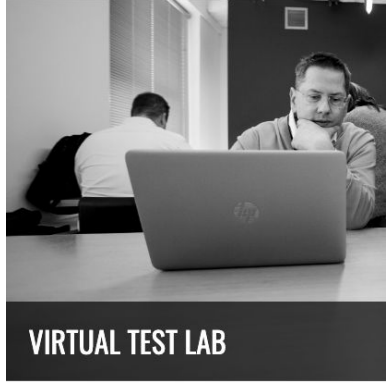
PCNSE Overview

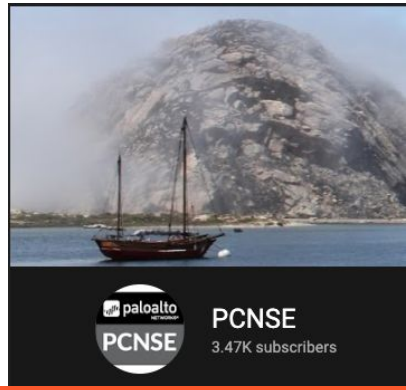
How the Program Works

- 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

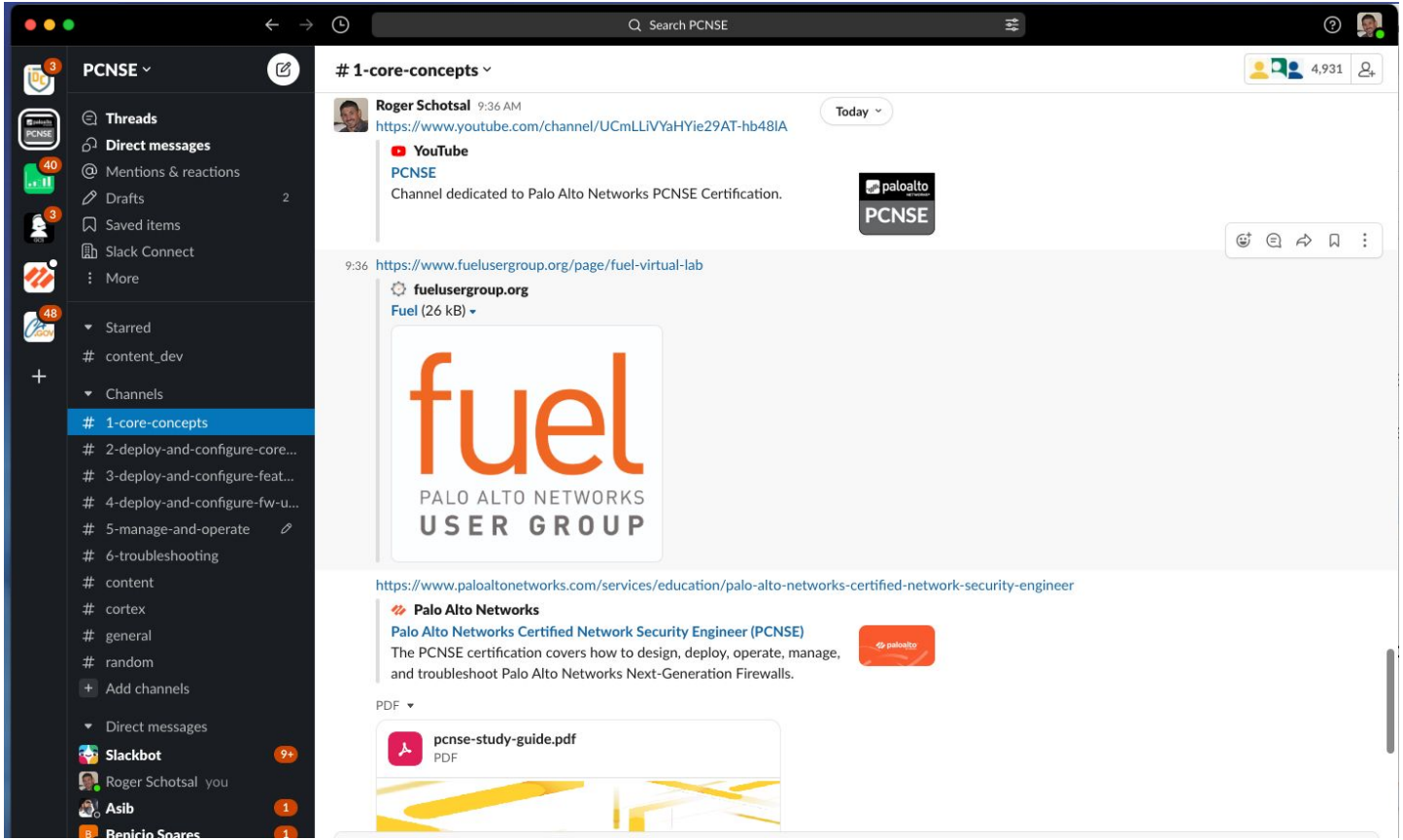
With all the required links and instructions.





slack

Slack Channel



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.

Palo Alto Networks Portfolio

Strata PA-Series
ML-Powered Next-Generation Firewall
App-ID | User-ID | Content-ID | Device-ID

VM-Series
Virtual Next-Generation Firewall
App-ID | User-ID | Content-ID | Device-ID

CN-Series
Containerized Next-Generation Firewall
App-ID | User-ID | Content-ID | Device-ID

Panorama
Firewall Management

Prisma Access
Secure Access Service Edge
FWaaS | Secure Web Gateway | Zero Trust Network Access

Prisma Cloud
Cloud Native Security Platform
Cloud Security Posture Management | Cloud Workload Protection | Cloud Network Security | Cloud Infrastructure Entitlement Management

Prisma SD-WAN
Next-Generation SD-WAN
SD-WAN

Cortex XDR
Extended Detection and Response
Endpoint Threat Prevention | Endpoint Detection & Response | Behavioral Analytics | Managed Detection & Response

Cortex XSOAR
Extended Security Orchestration, Automation and Response
Security Orchestration, Automation & Response | Threat Intelligence Management

Expanse
Attack Surface Management
Internet-Connected Asset Discovery & Mitigation

Crypsis
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

paloalto NETWORKS

The PA-Series Portfolio

PA-400 Series

PA-800 Series*

PA-3400 Series

PA-5400 Series

PA-5450

PA-7000 Series

Small Branches & Remote Locations

Network Perimeter

Large Data Centers

*For customers who need fiber ports

VM-Series NGFW

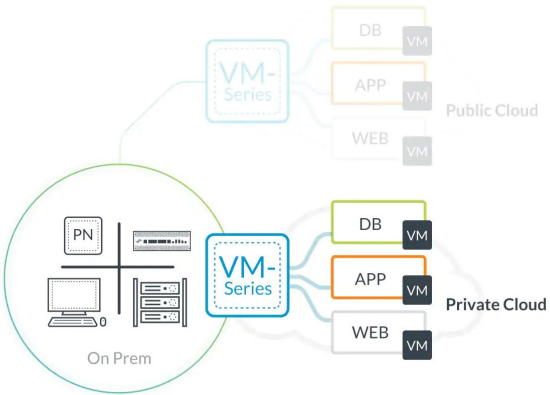
Security Where you need it When you Need it

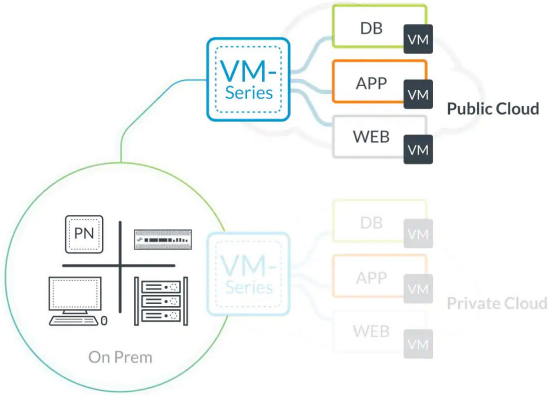
Private Cloud

- 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

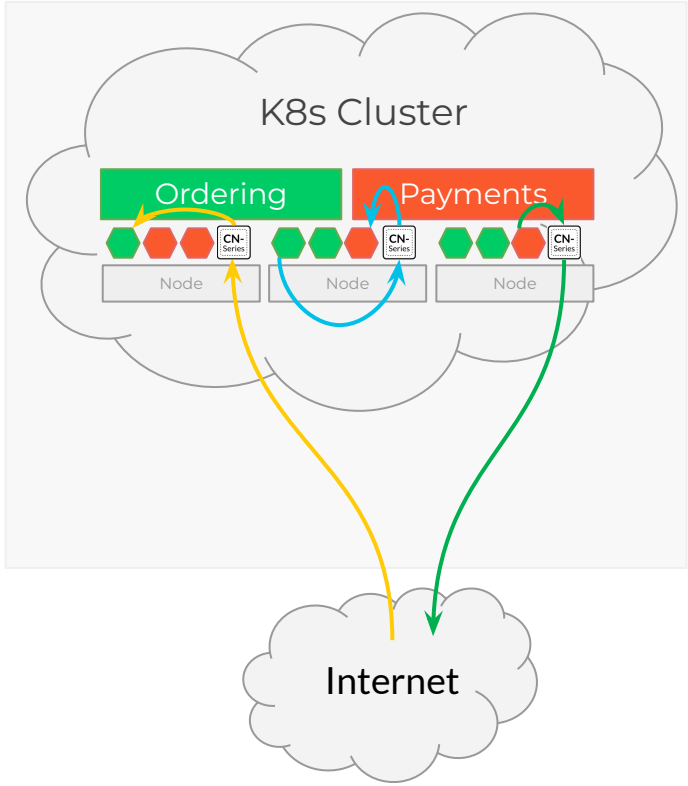
Container-level protection against break-ins

East-West

Prevent lateral propagation within container clusters

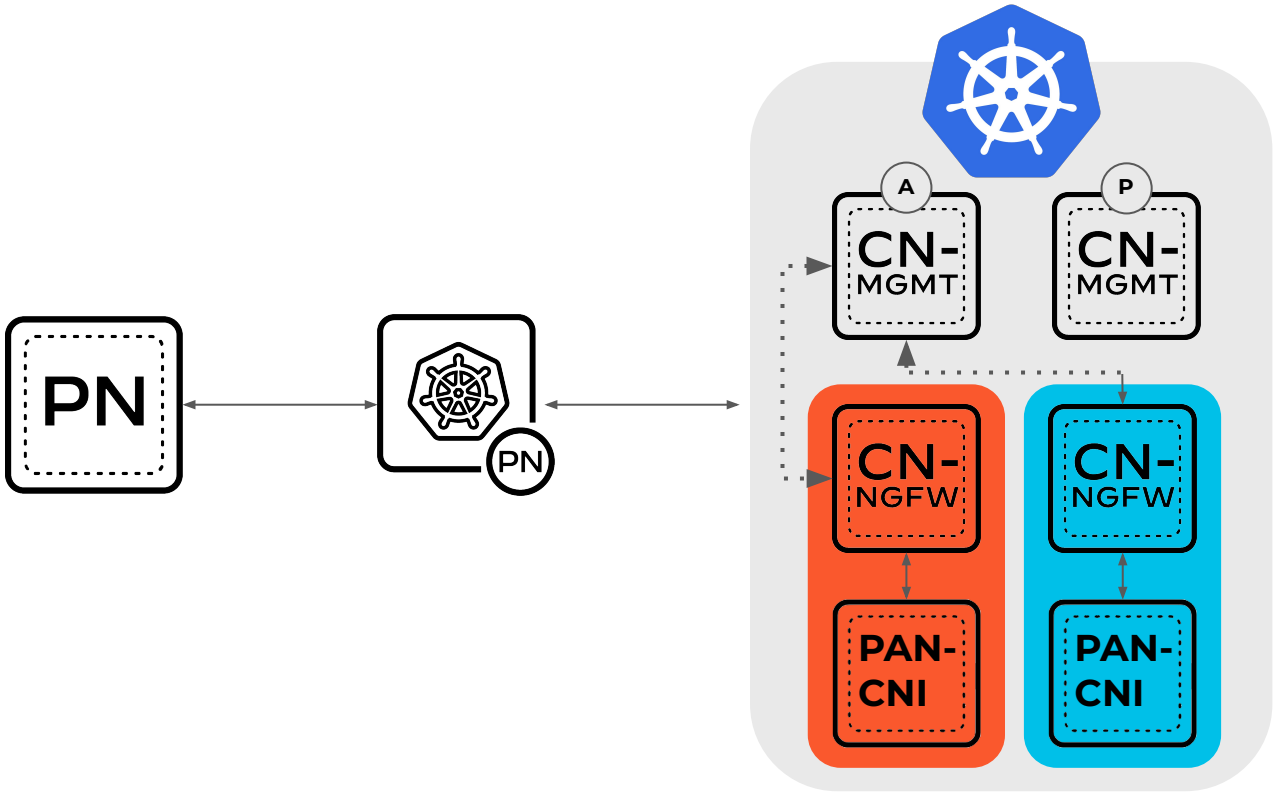
Outbound

Stop data exfiltration with container-context



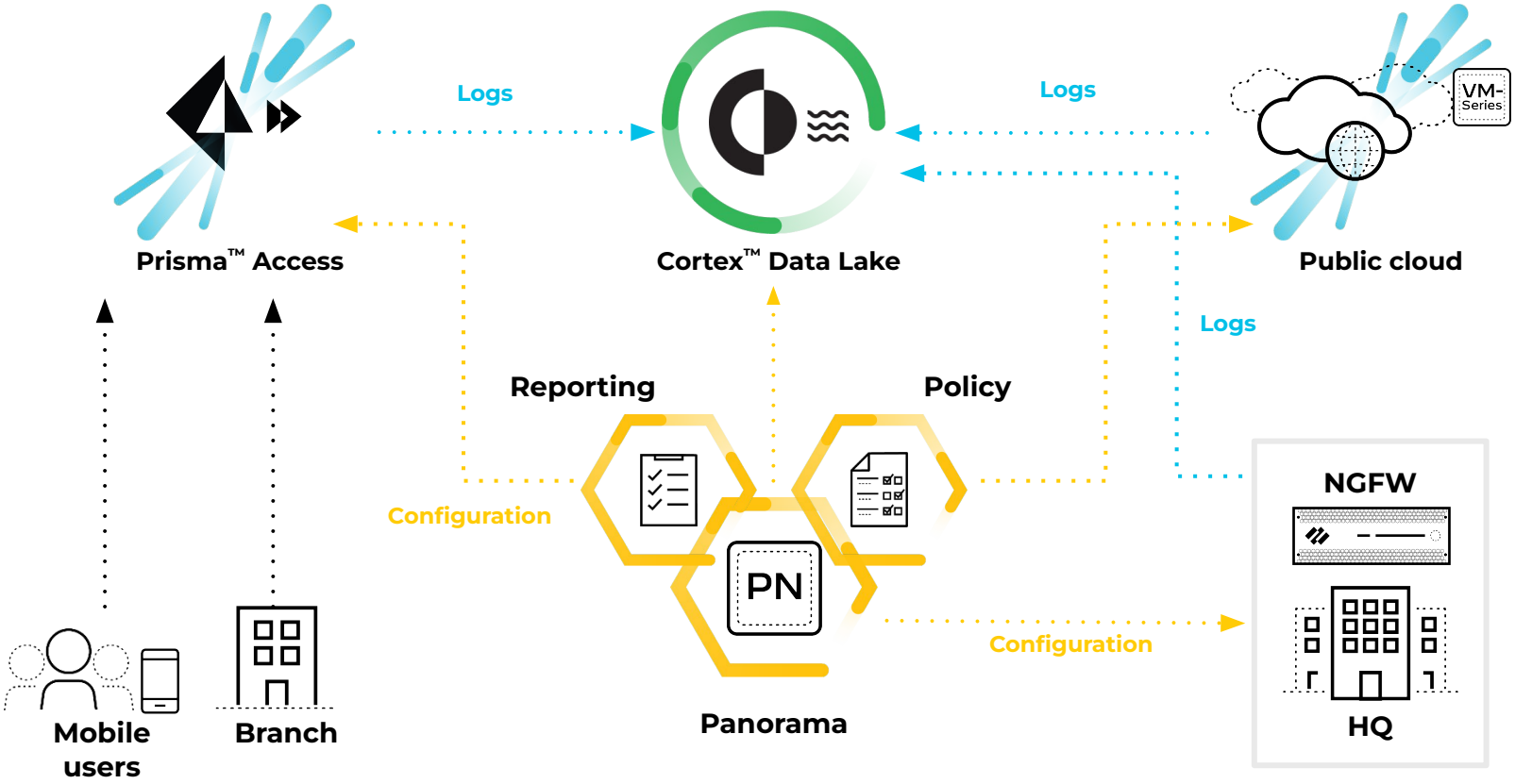
By running a CN-Series NGFW on each node

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

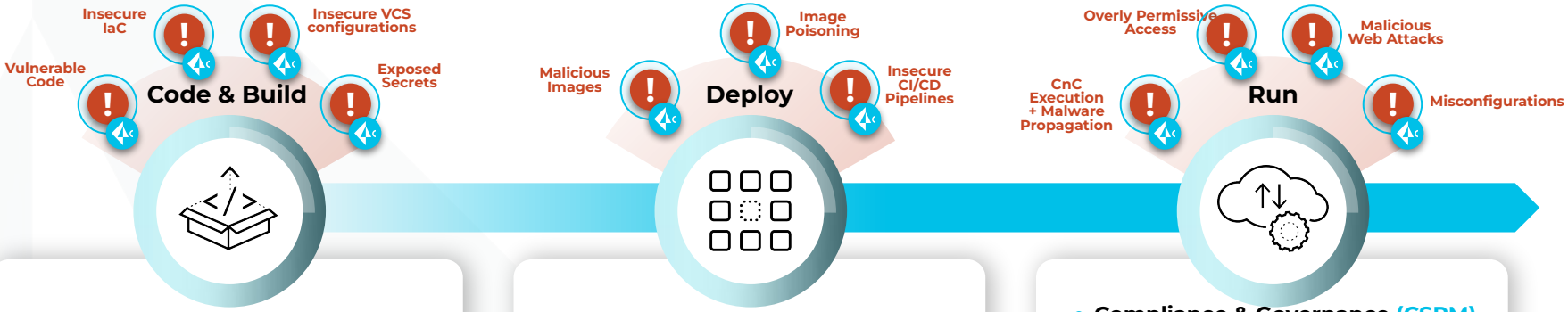


Panorama

Centralized Configuration, Visibility, Logging



PRISMA CLOUD CAPABILITIES



- IaC Security (CCS)
- Software Composition Analysis (CCS)
- Secrets Scanning (CCS)
- Supply Chain Security (CCS)
- Vulnerability Management and Compliance (CWP)

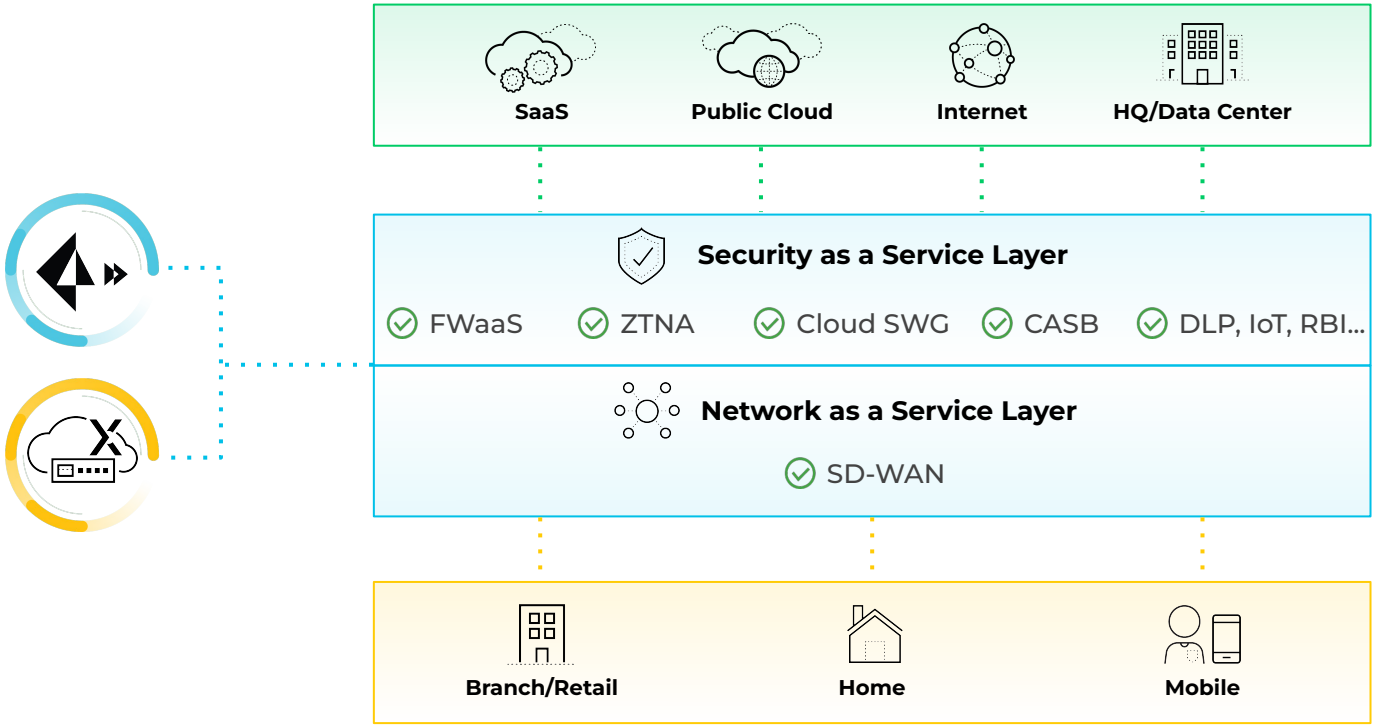
- Container Access Control (CWP)
- CD Security (CWP)
- Trusted Images (CWP)
- Image Analysis Sandbox (CWP)

- Compliance & Governance (CSPM)
- Misconfig & Threat Detection (CSPM)
- Vulnerability management & Runtime Security (CWP)
- Web App & API Security (WAAS)
- IAM Security (CIEM)
- Data Security (CSPM)
- Network Security (CNS)

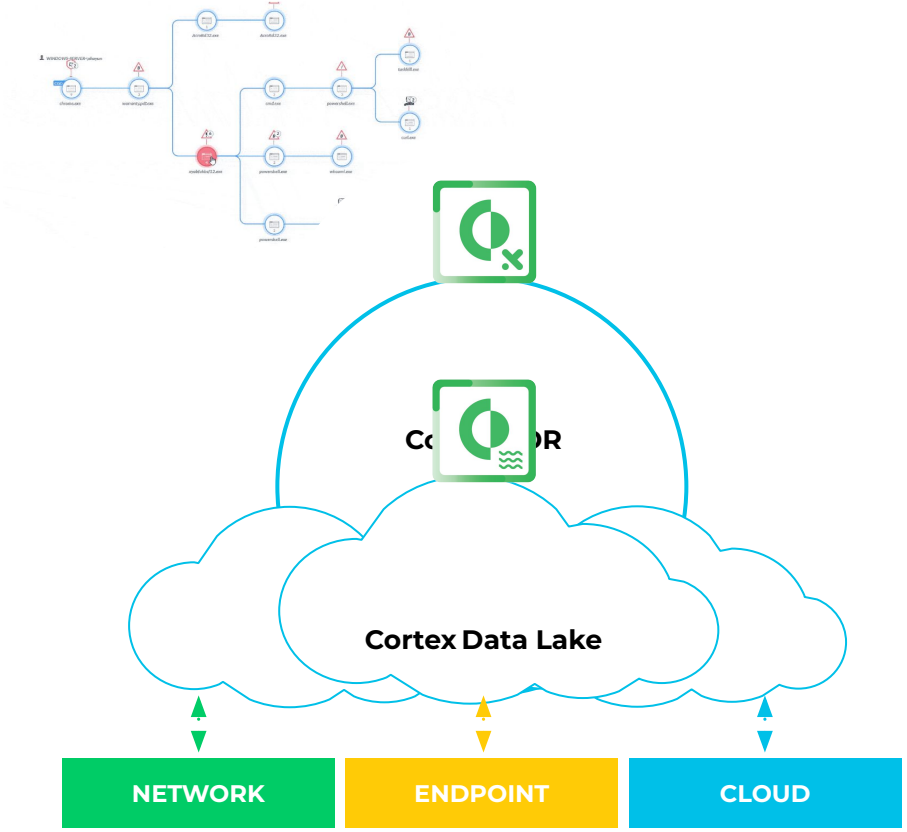
SaaS Platform

- Cloud Scale SaaS Platform
- Integrated experience from Code to Cloud
- Easy to Adopt and Operationalize

Prisma Access & PRISMA SD-WAN (AKA CloudGenix)
The Industry's Most Comprehensive SASE



Cortex XDR Detects and Investigates Sophisticated Attacks

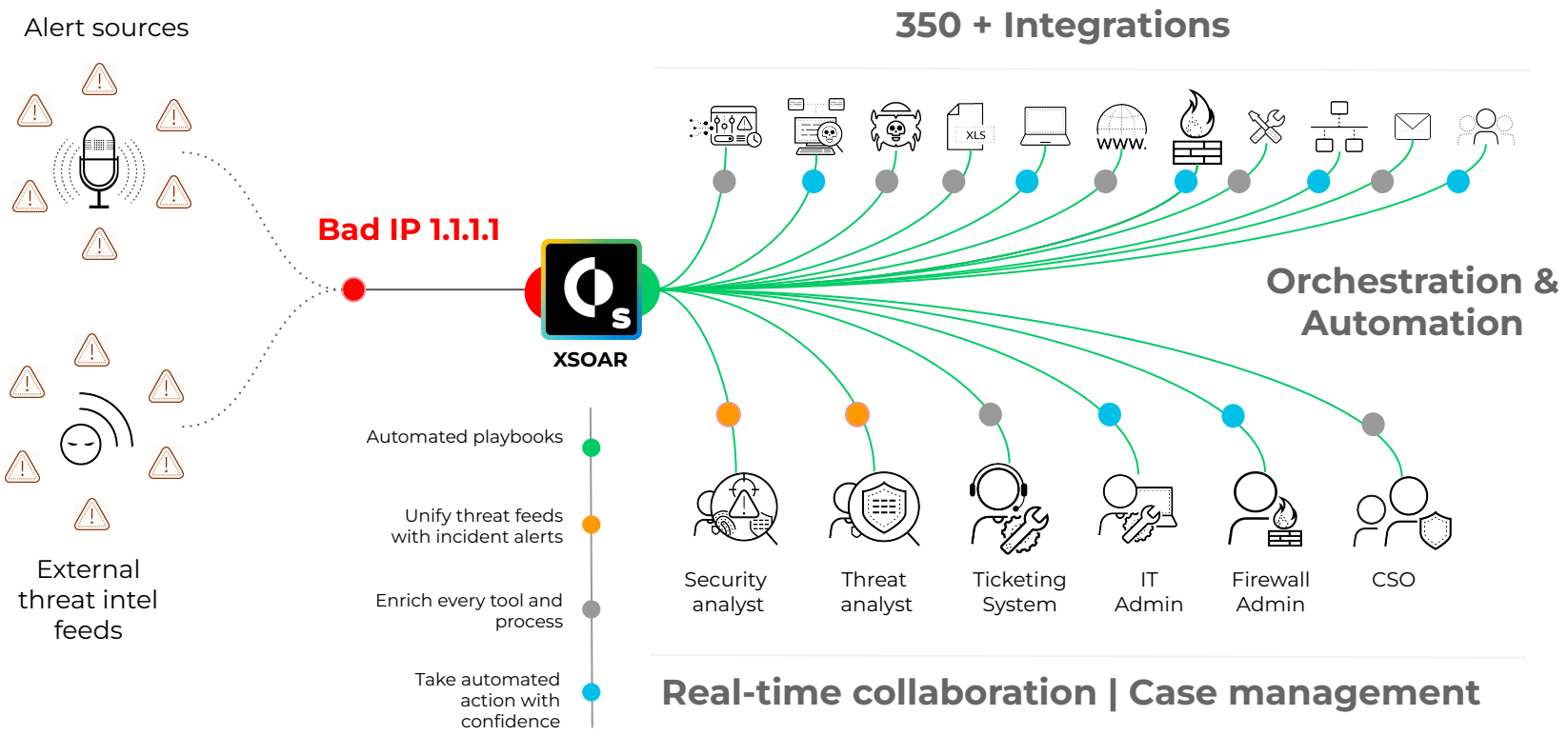


Automatically detect attacks using rich data and cloud-based behavioral analytics

Accelerate investigations by stitching data together to reveal root cause

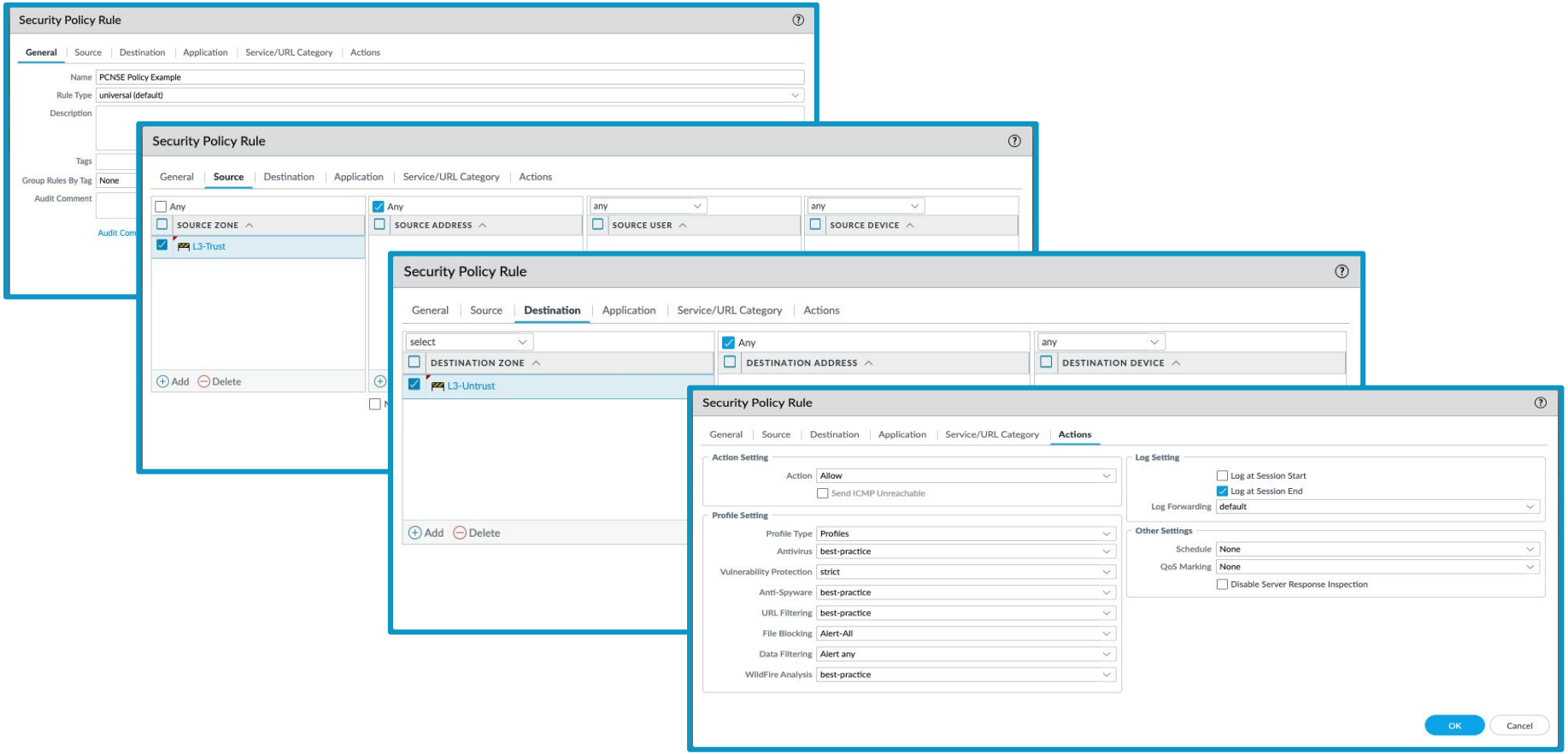
Tightly integrate with enforcement points to stop threats and adapt defenses

Cortex XSOAR Automates Security Workflows

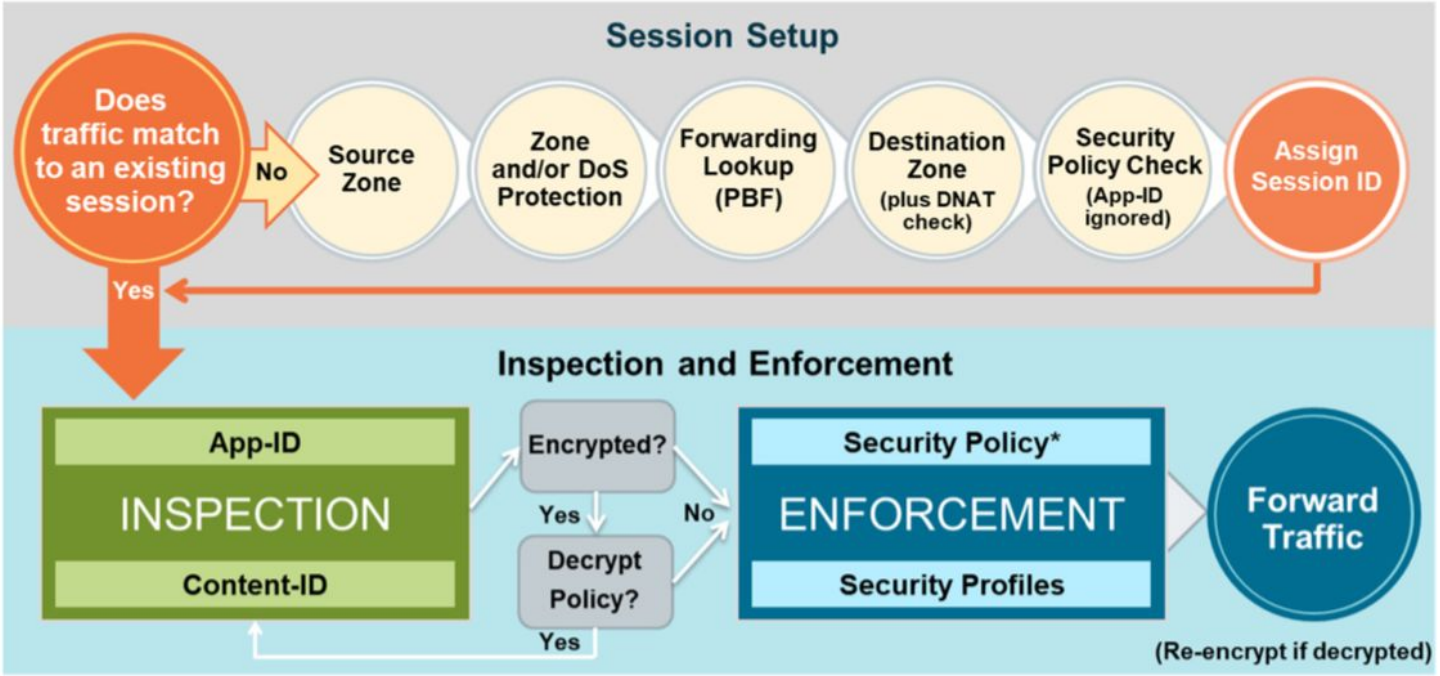


CORTEX
BY PALO ALTO NETWORKS

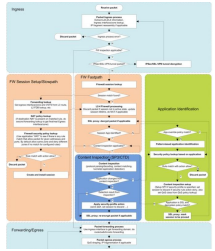
1.1.2 Firewall Components



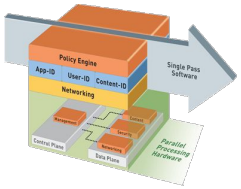
Traffic Processing Sequence



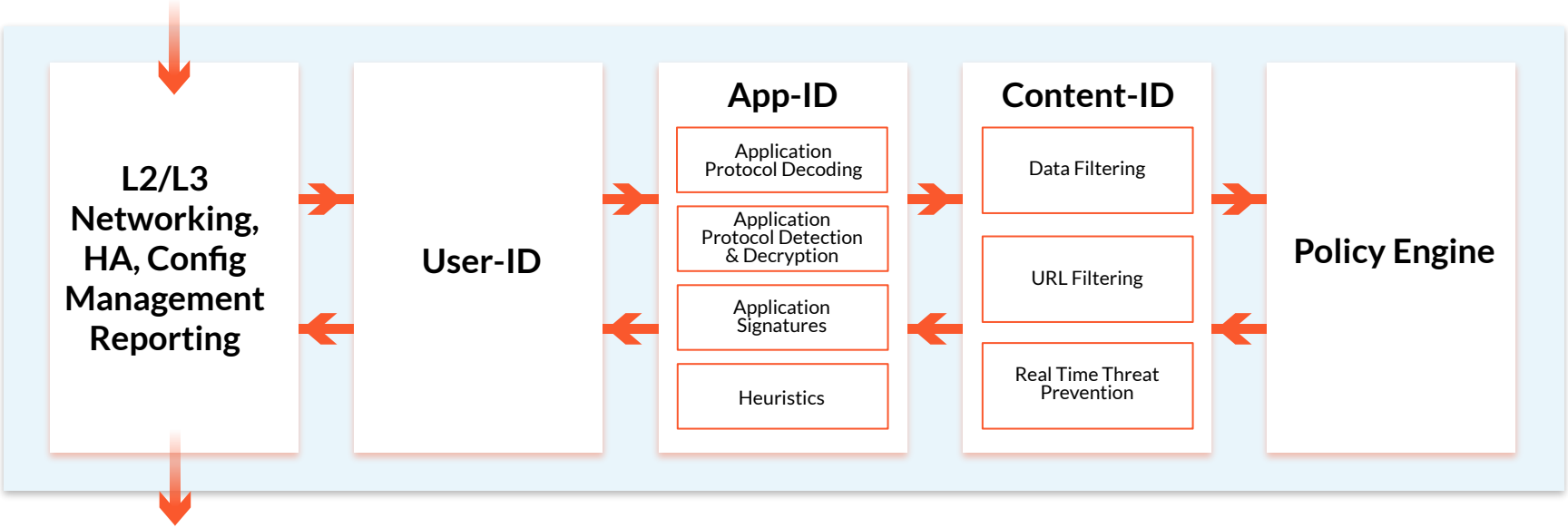
PACKET FLOW SEQUENCE IN PAN-OS
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081



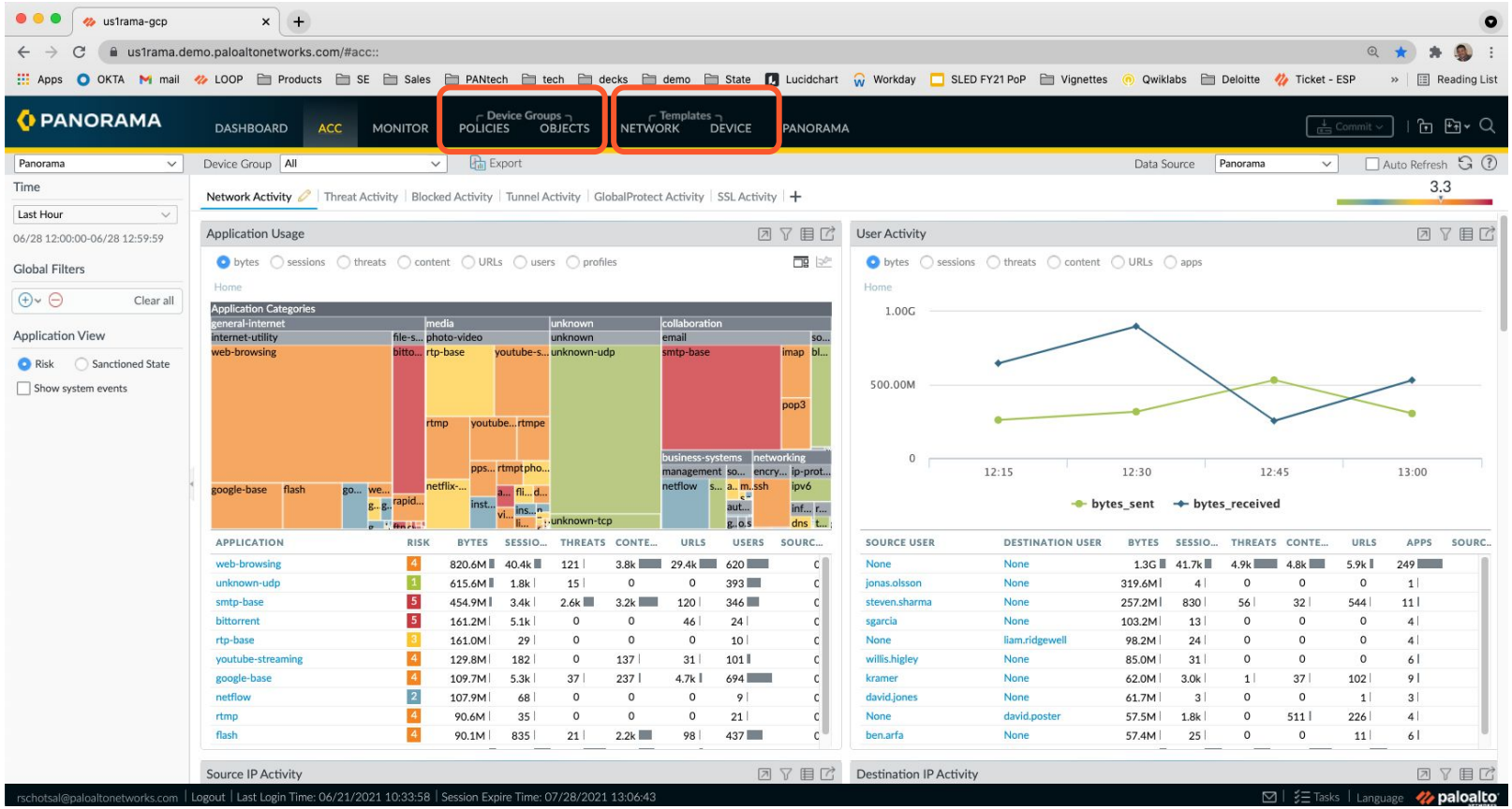
Single-Pass Security Processing



- 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



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

Threat Prevention Eliminates Known Threats

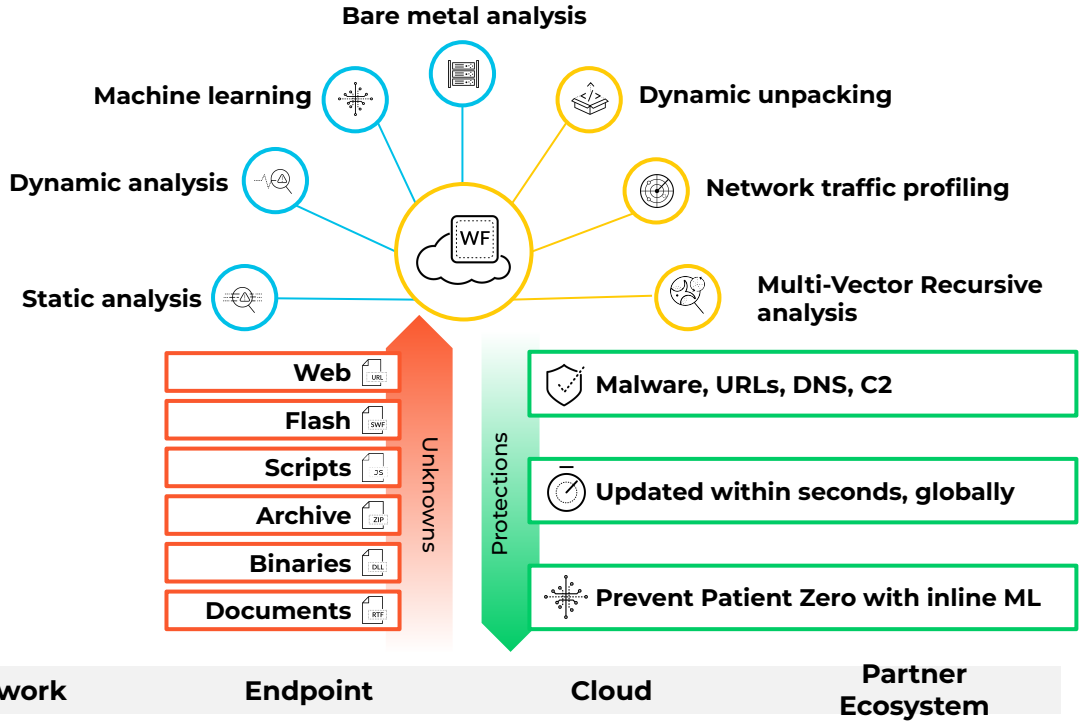
Detect and block Exploitation

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

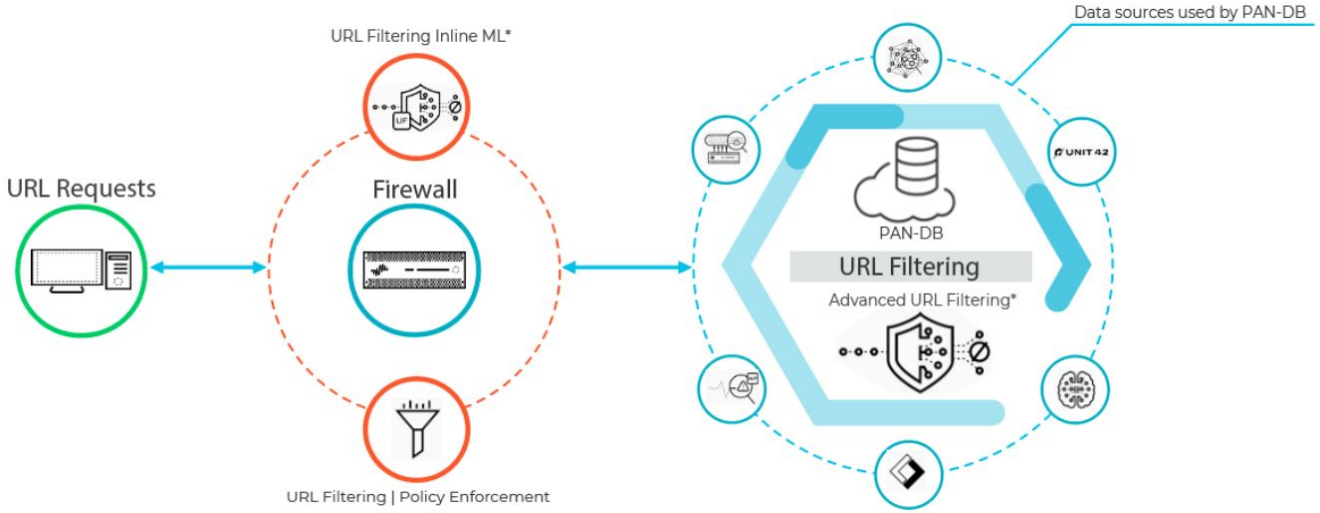


Data collected from a vast global community

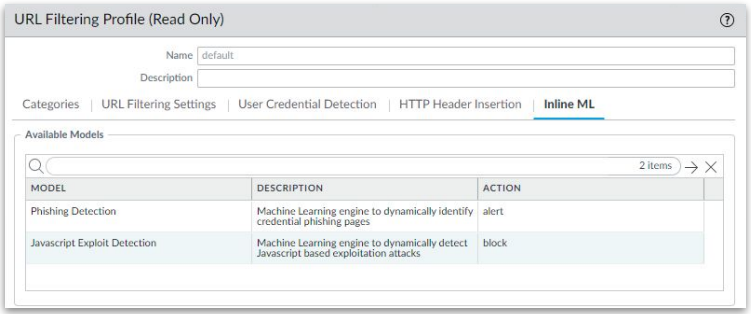
Analysis techniques far beyond traditional sandboxing

Automated protection against multiple attack variants

URL Filtering Protection - PAN DB



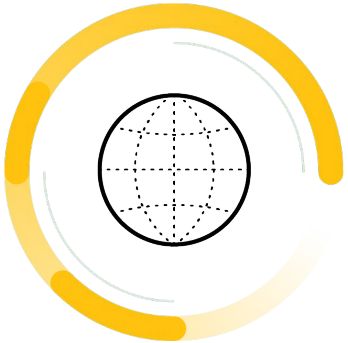
Provides protections from both known and unknown threats based on PAN-DB classification. **Inline and real time.**



DNS Security

Blocks known bad bomains

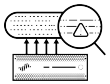
Stops malicious DNS traffic with ML and predictive analytics



Integration with NGFW means it cannot be bypassed

Data

WildFire Analysis



Passive DNS

URL Filtering

Honeynets

Unit 42

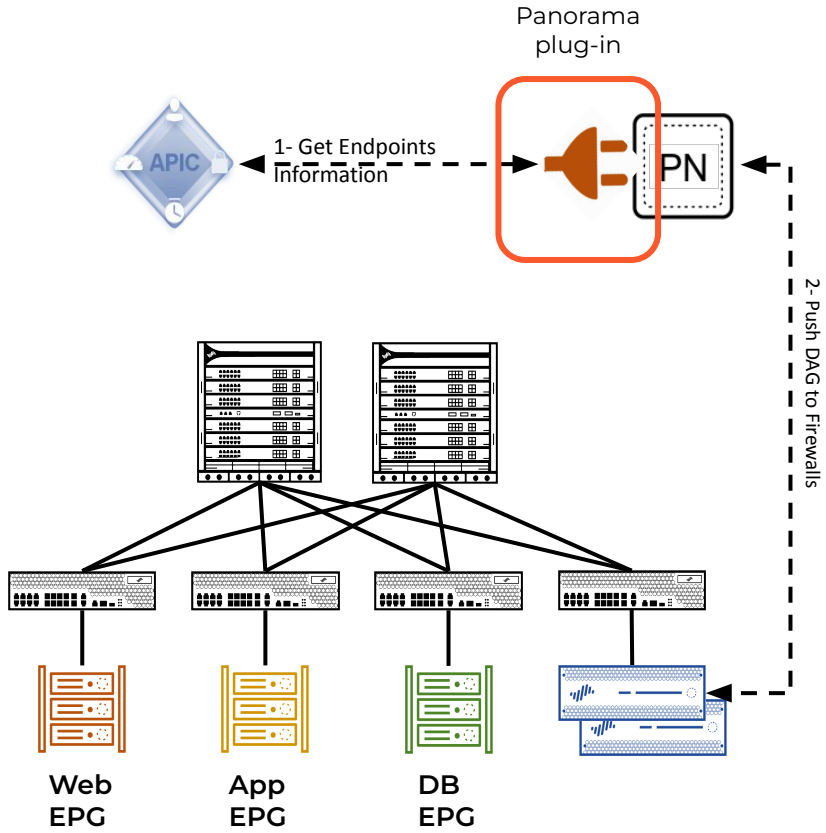
Whois

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.

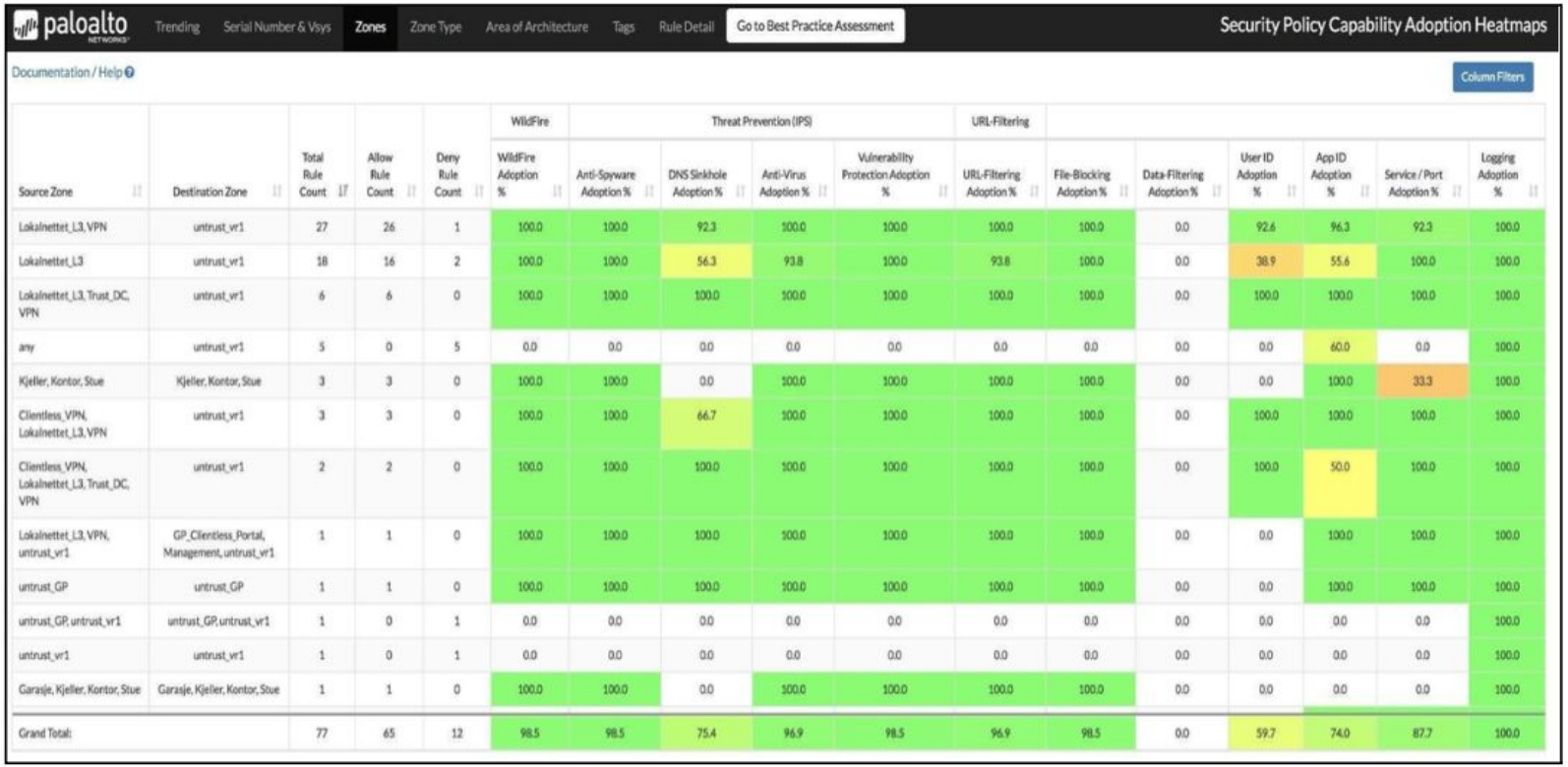
In the diagram to the right the **plug-in** is managing the communication with a Cisco ACI APIC.

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#id181P8K0F0LT

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

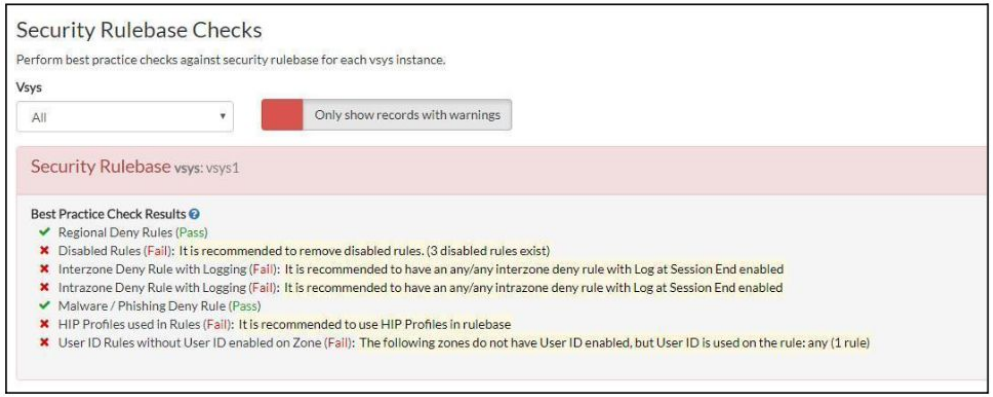
Security Policy Capability Adoption Heatmaps

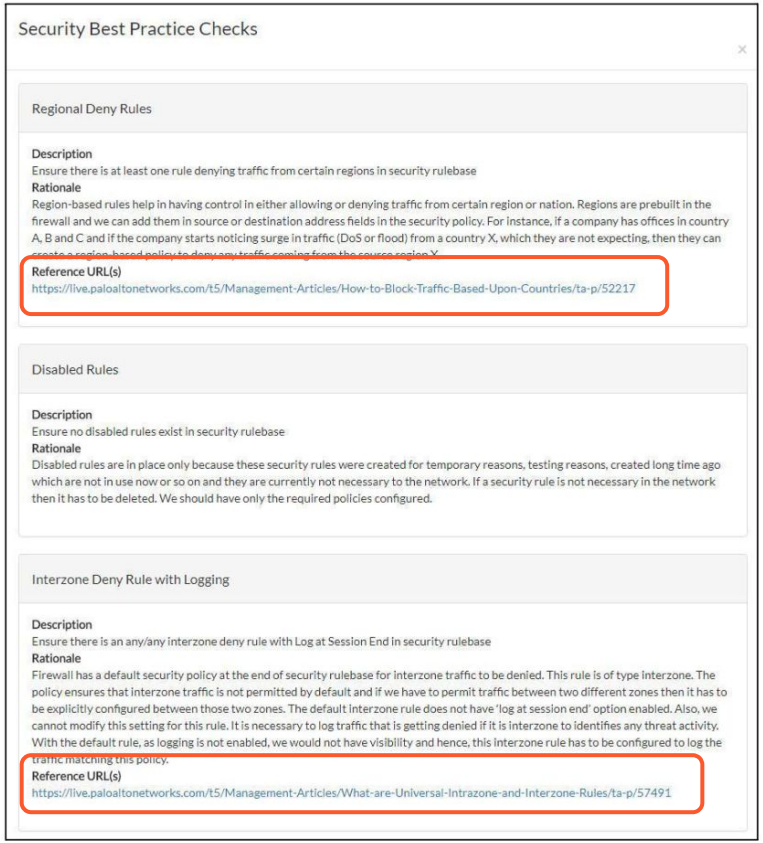
Documentation / Help

Column Filters

					WildFire	Threat Prevention (IPS)				URL-Filtering						
Source Zone	Destination Zone	Total Rule Count	Allow Rule Count	Deny Rule Count	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	92.6	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	38.9	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	100.0

Example of Security Rulebase Checks





Note: BPA have embedded links to videos & live article that will show you exactly how to remediate the issues detected in the configuration

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.

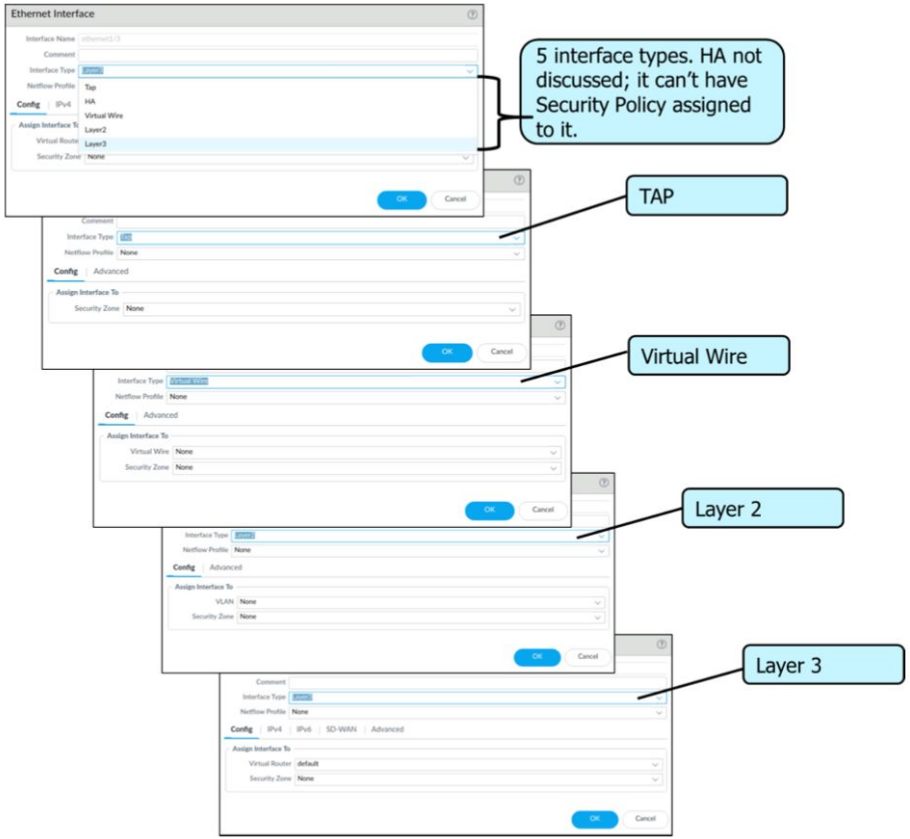
A single firewall can freely intermix interface types to meet any integration need. The decision about which interface configuration to choose depends on functional need and existing network integration requirements.

1.2.1 Layer 2 interfaces

1.2.2 Layer 3 interfaces

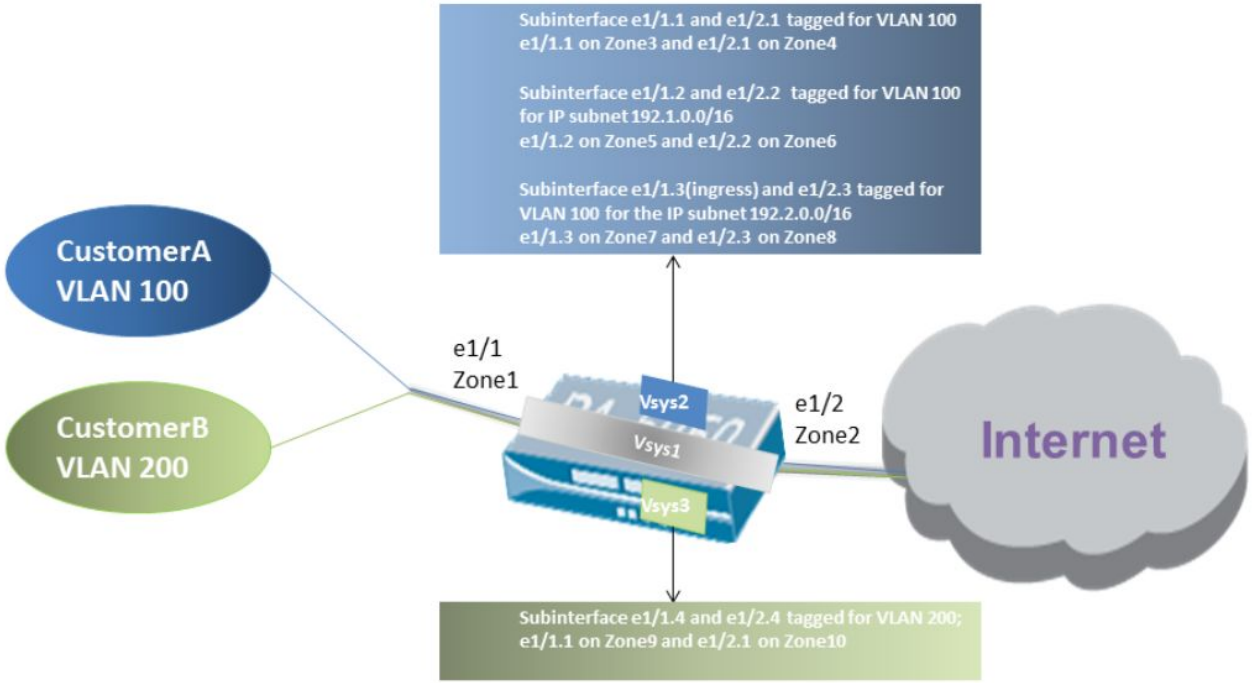
1.2.3 Virtual Wire interfaces

1.2.4 Tap interfaces



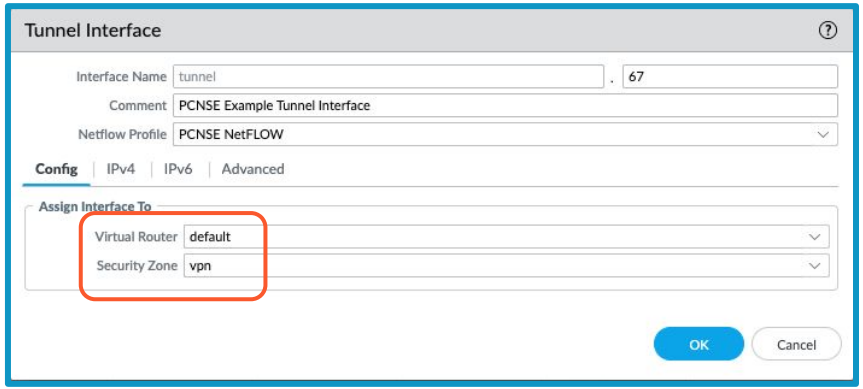
 |

1.2.5 Subinterfaces

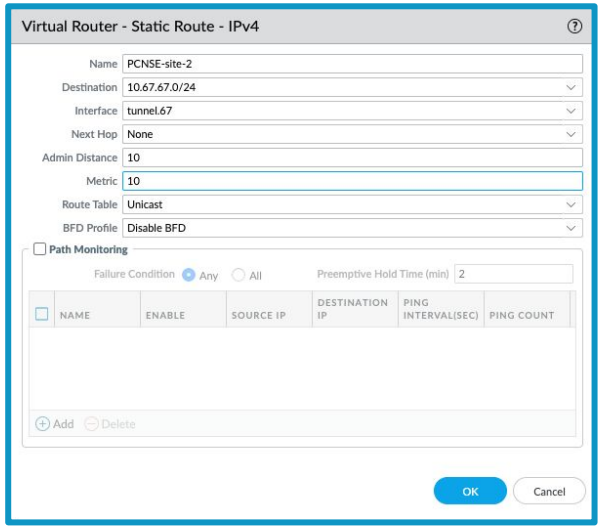


Read Study Guide

1.2.6 Tunnel Interfaces



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

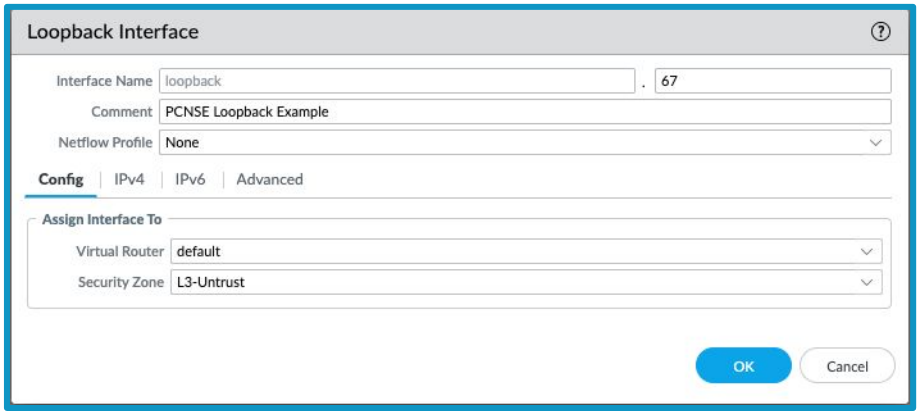
- Assigned to virtual router
- Assigned to Security Zone
- IP Address only required for “Tunnel Monitoring” or “Dynamic Routing Protocols” (BGP or OSPF)

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

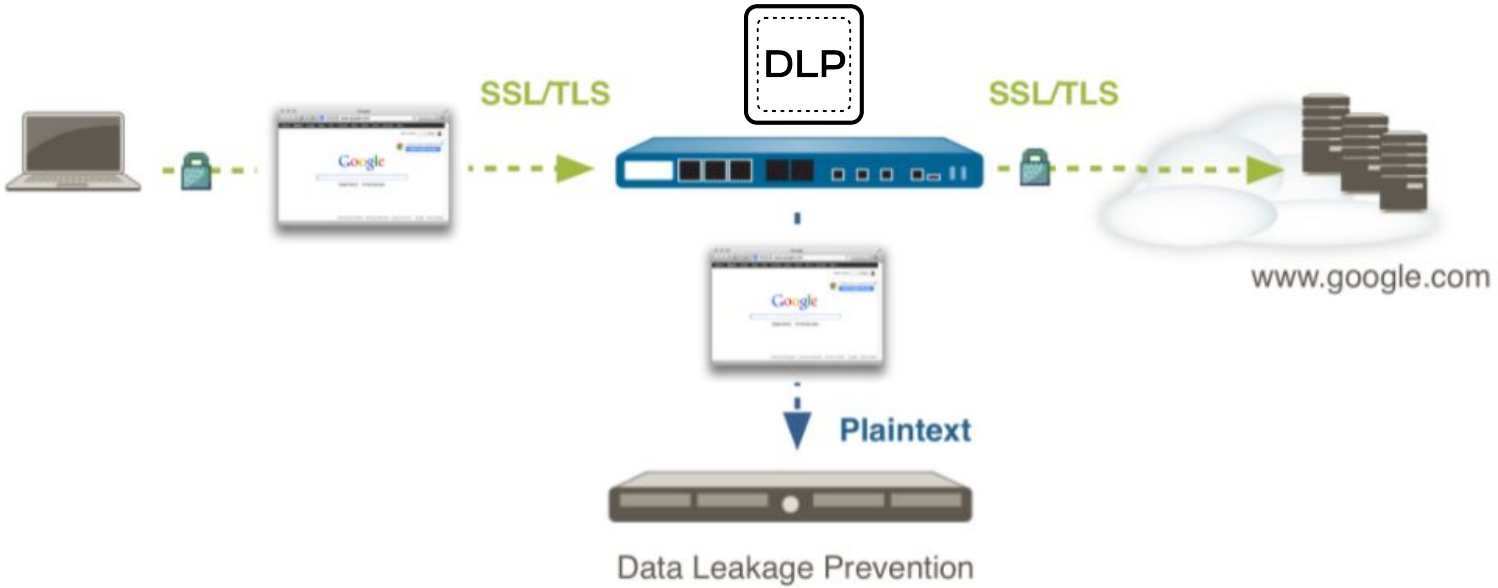
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html

1.2.8 Loopback Interfaces



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

1.2.8 Decrypt Mirror Interfaces

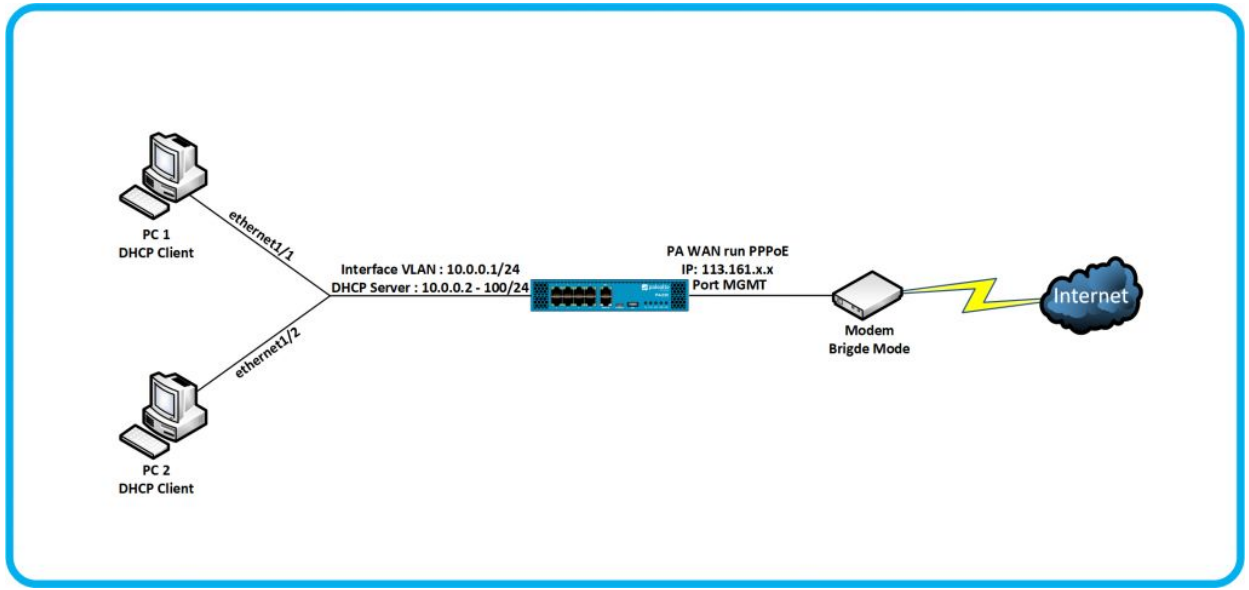


How to Configure Decrypt Mirror:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGDCA0

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

1.2.8 VLAN Interfaces

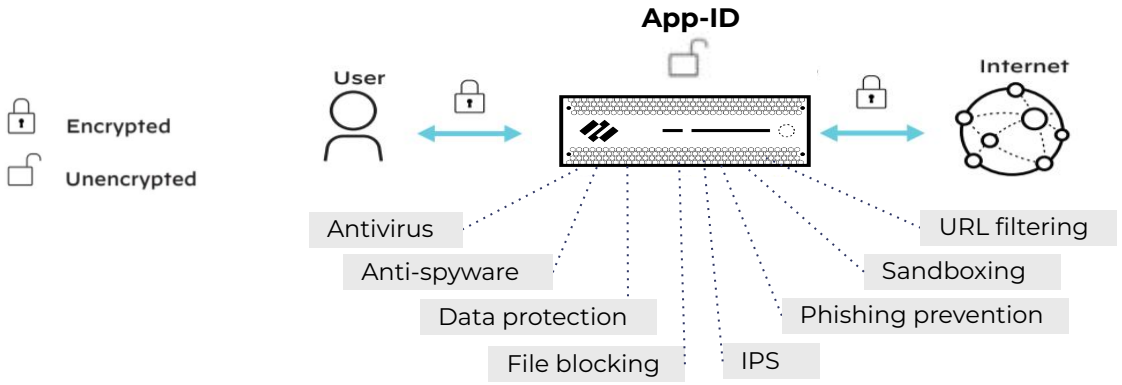
Logical interface useful in conjunction with L2 interface physical type to provide L3 switching



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



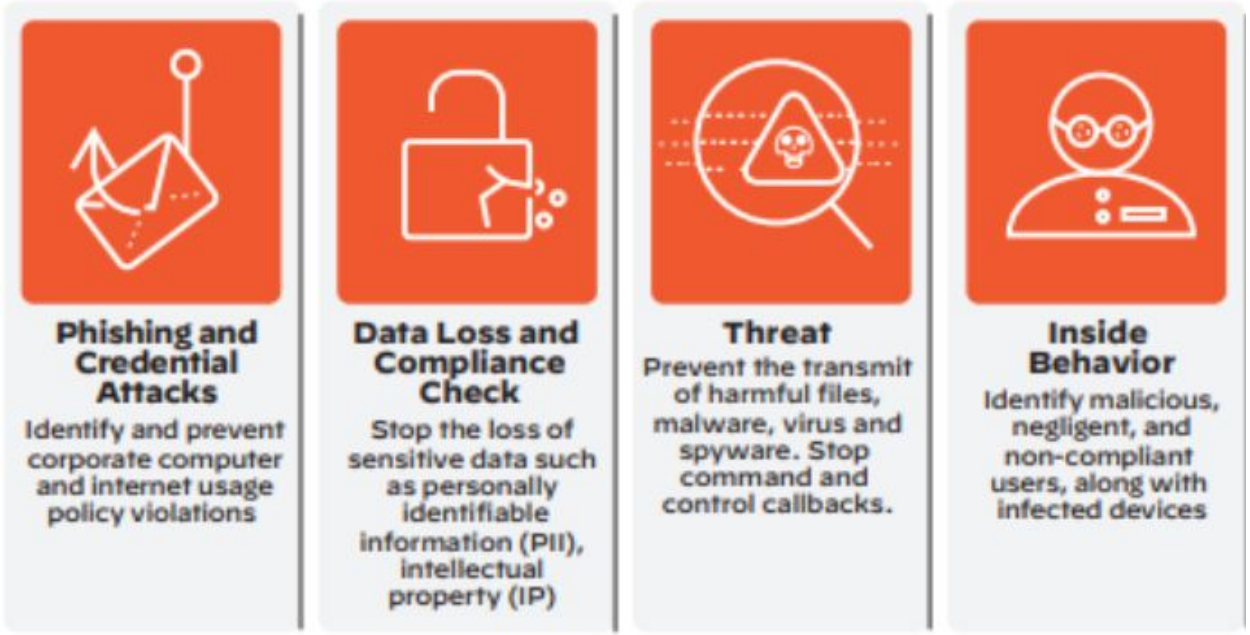
Implications:

- **Security efficacy increases - subscriptions applied to plaintext data**
- **App-ID Transitions from "SSL" to something else - must anticipate impact on Security Policy.**
- **Key & Certificate Management becomes a critical component.**

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



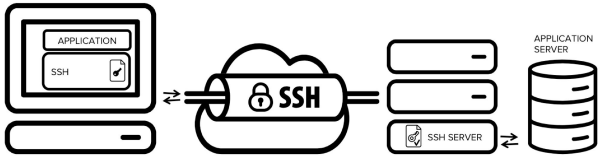
1.3.3 Decryption Types

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.

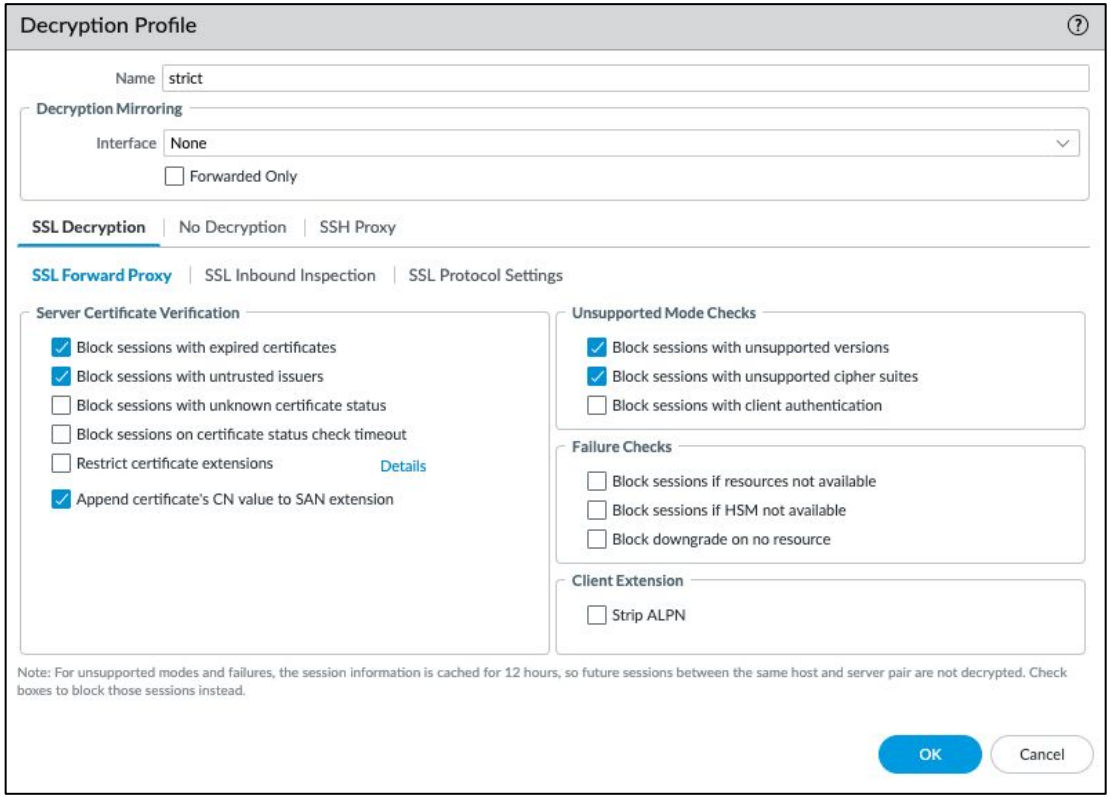


 |

1.3.4 Decryption Profiles & Certificates

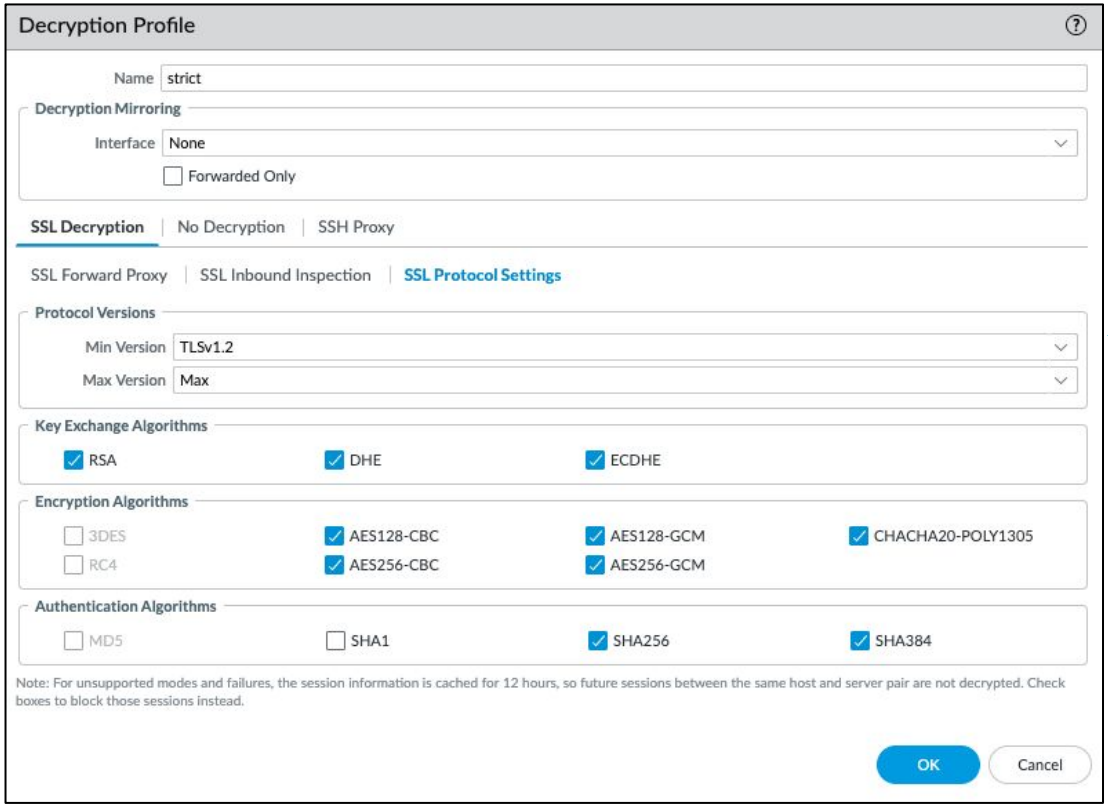
Certificates Used with Decryption	Description
Forward Trust (used for SSL Forward Proxy decryption)	The certificate the NGFW presents to clients during decryption if the site the client is attempting to connect to has a certificate signed by a CA that the NGFW trusts.
Forward Untrust (used for SSL Forward 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 server certificate and the private key.

Protect Users from Bad Sites



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

Granular Control on Ciphers



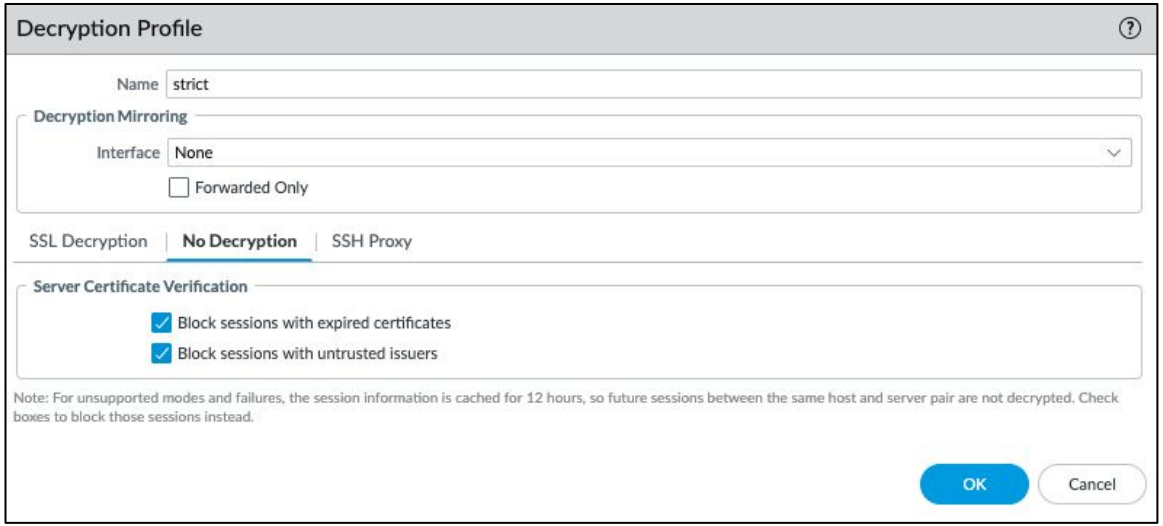
- Avoid weak protocols and ciphers

Minimum TLS version

Control Ciphers

 |

Control Application Behavior



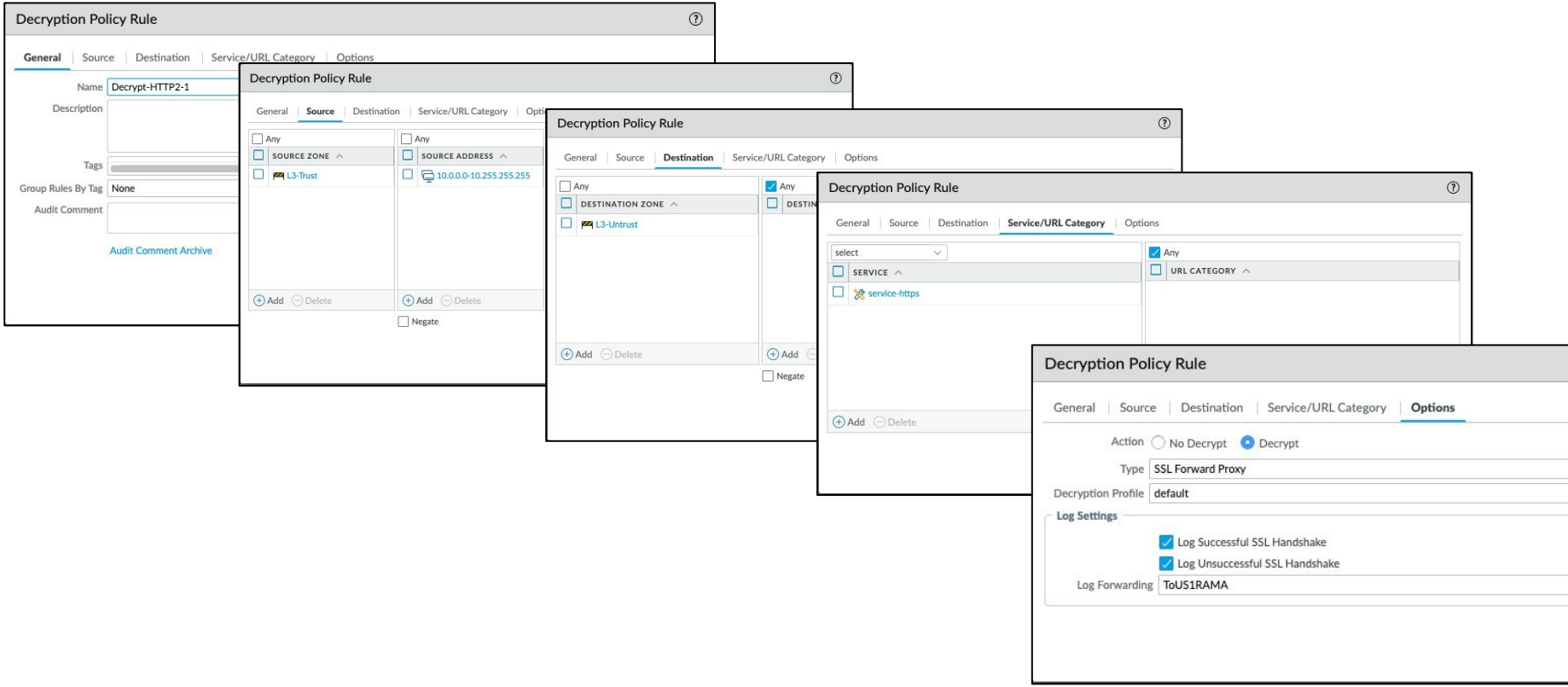
- Block Anonymizers

Decryption Deep Dive!

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

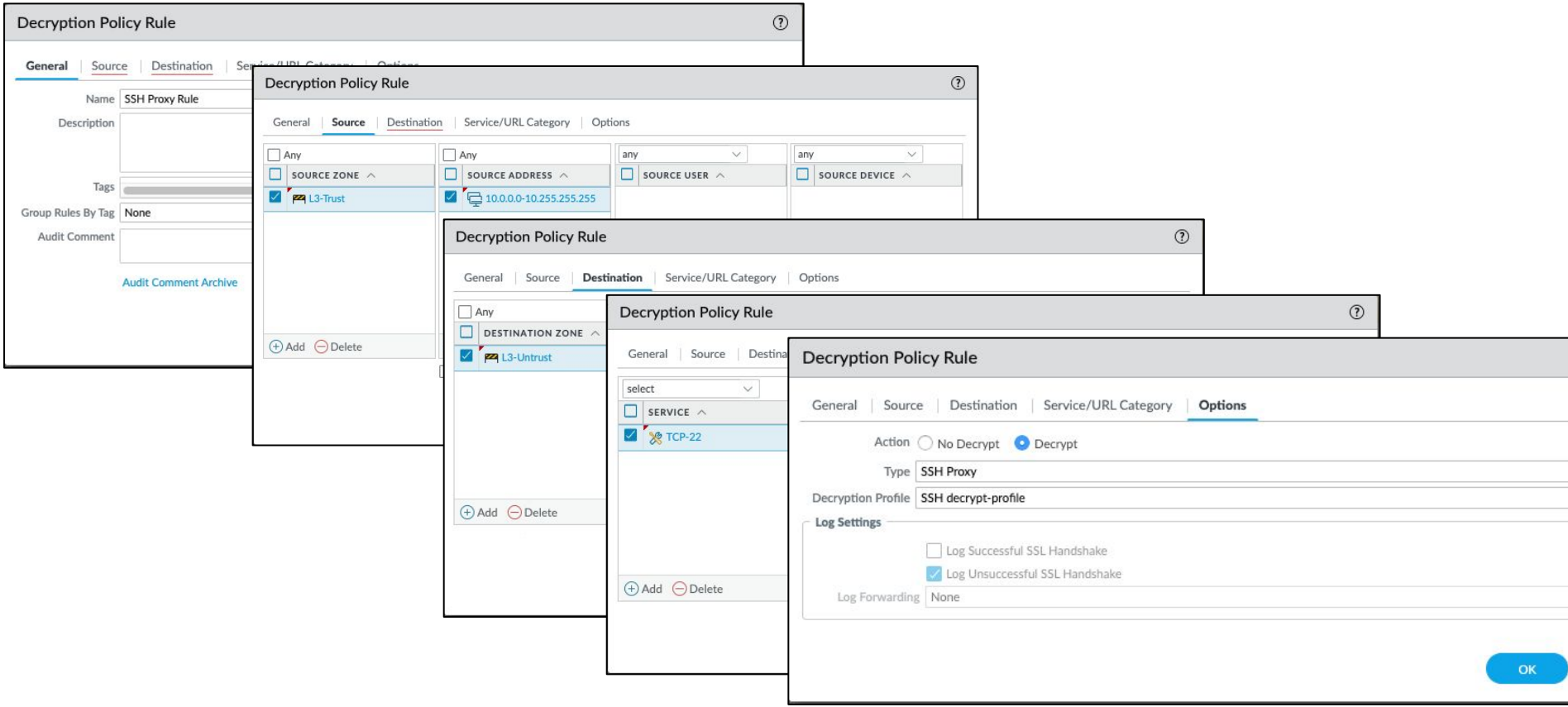
Have you ever wondered how Secure Socket Layer (SSL) works? Have you ever been perplexed about what a Client Hello or a Server Hello is? Or do you want to really understand how a Next-Generation Firewall (NGFW) performs decryption? Then this episode is for you! Shakti will be your decryption mentor by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

1.3.5 Decryption Policy in the Firewall



 |

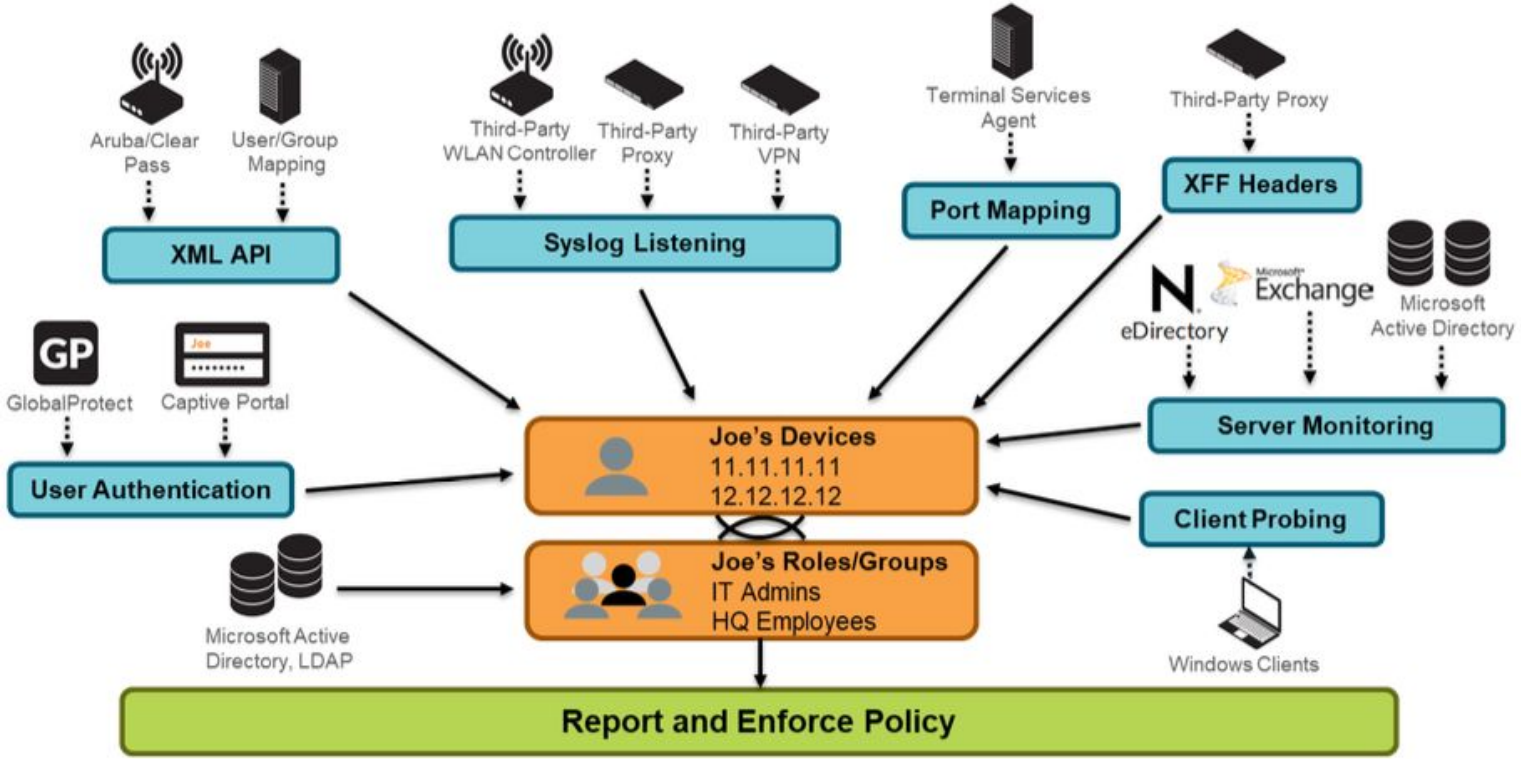
1.3.6 Configure SSH Proxy



 |

1.4 Enforce User-ID

1.4.1 Methods of building user-to-IP mappings.

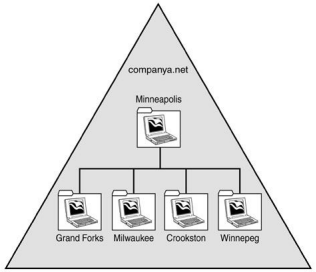


 |

1.4.2 Determine if User-ID agent or agentless should be used
1.4.3 Compare & Contrast User-ID Agents

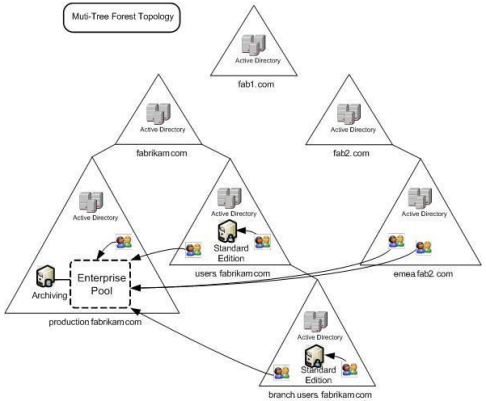
Agentless (PAN-OS) - Built-in Agent

- 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



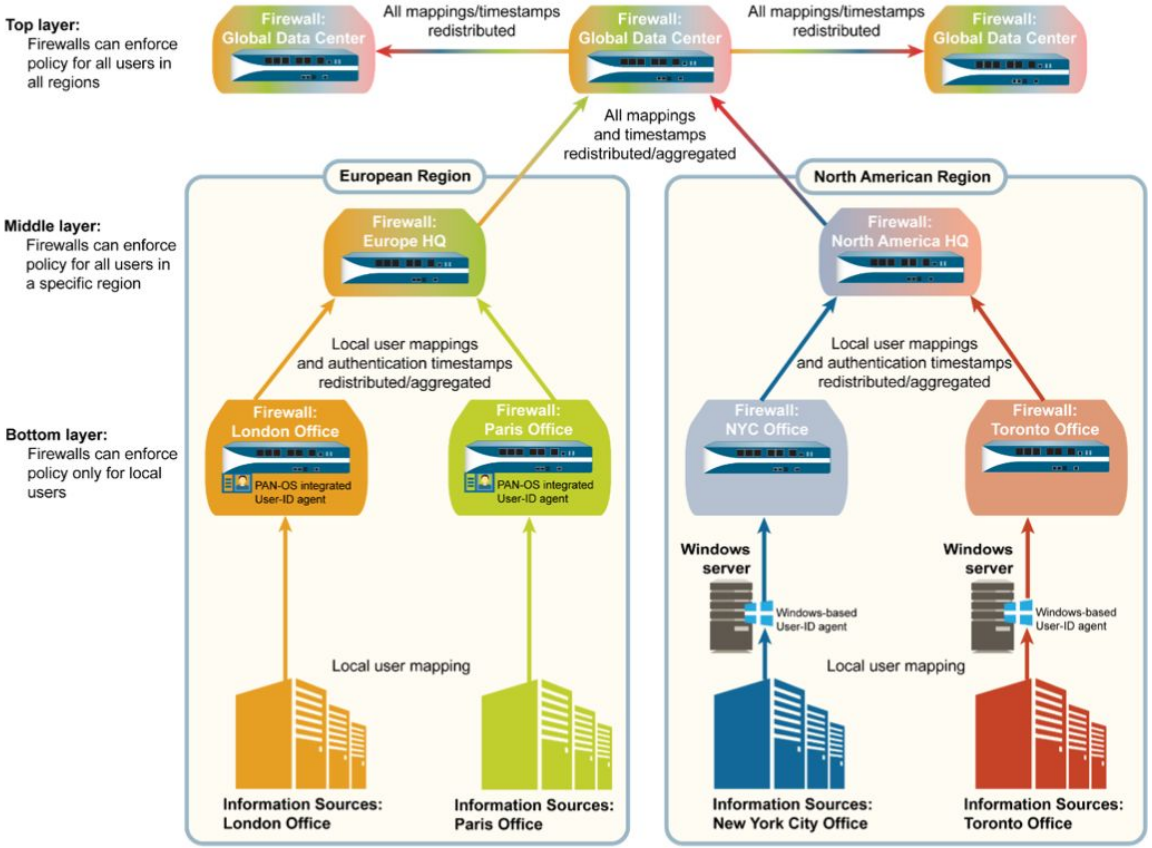
User-ID Agent (Windows)

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

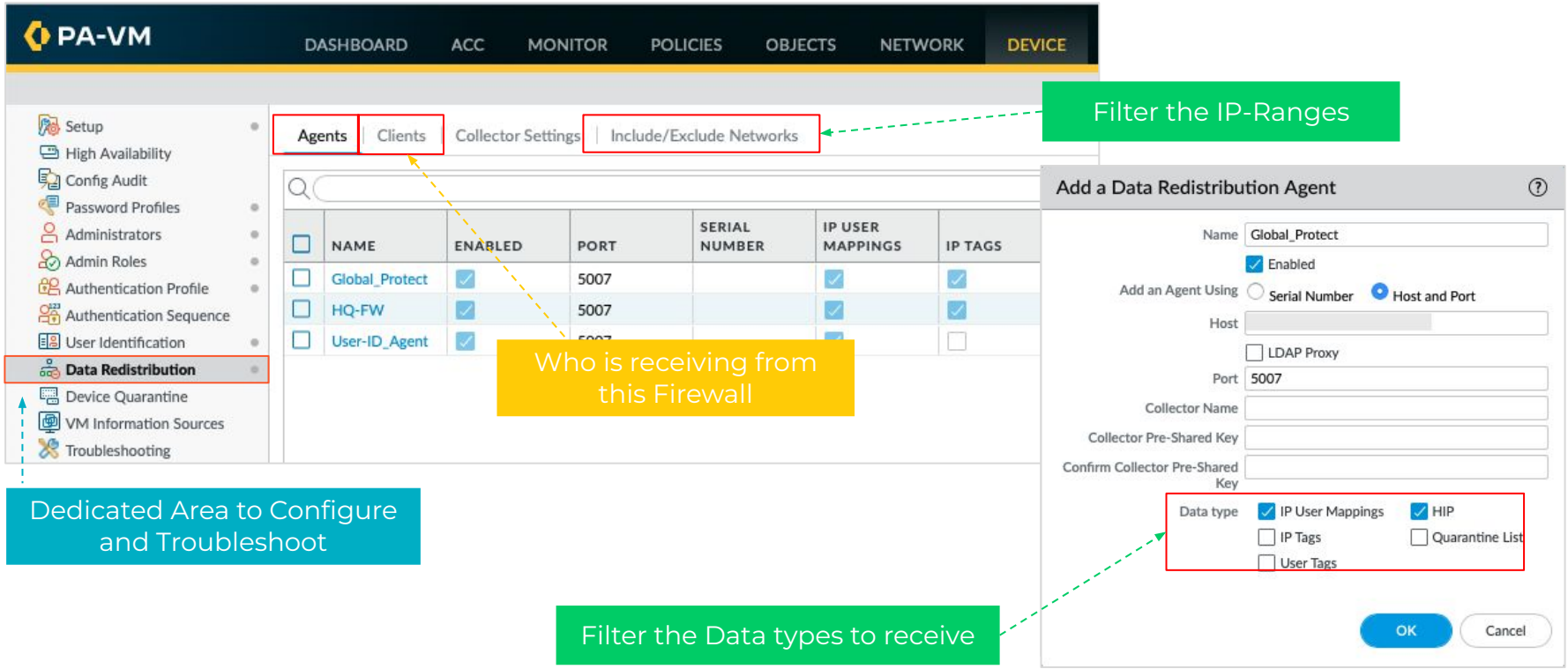


 |

1.4.4 Methods of User-ID Redistribution



User Meta-Data Redistribution: Easy Configuration



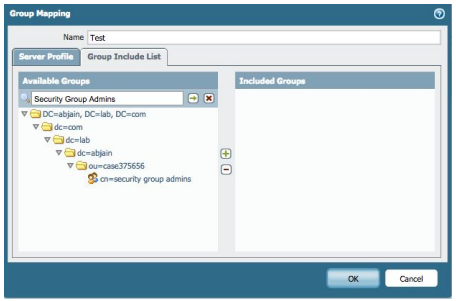
1.4.5 Methods of Group Mapping

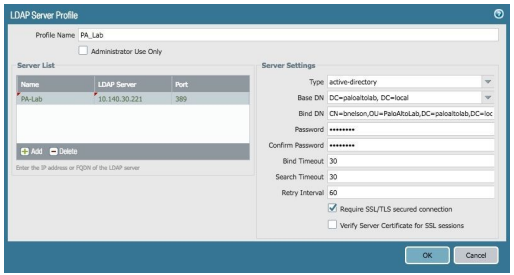
Single Domain Group Mapping

- 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 the being placed on the PAN-OS device.

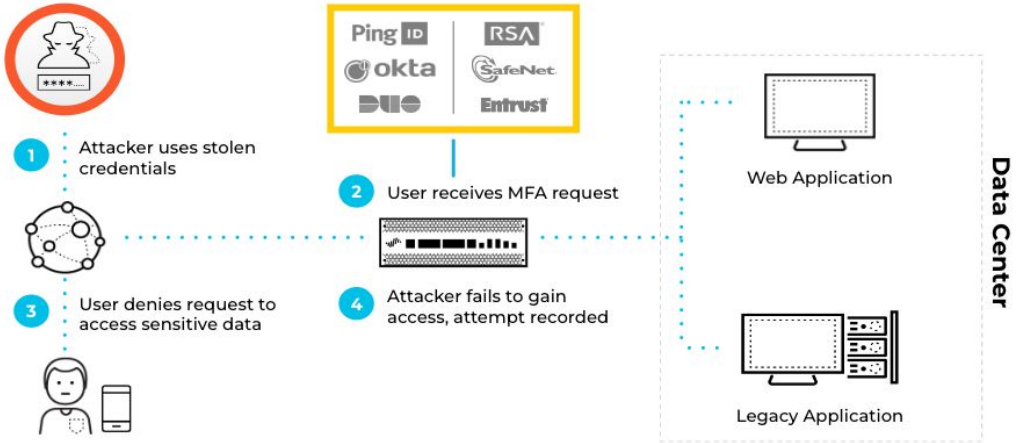
Multi-Domain Group Mapping

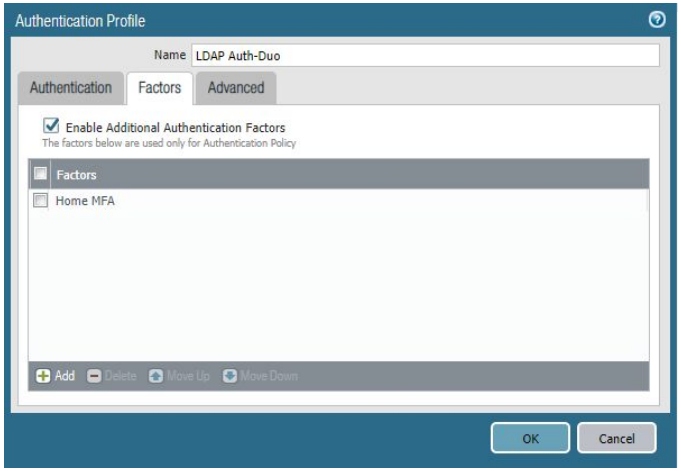
- Use a LDAP Server Profile to retrieve group-to-user mappings from to domain controller - in each domain or forest.
- Make sure usernames come across uniquely - append domain names to usernames (domain\username or username@domain.local)

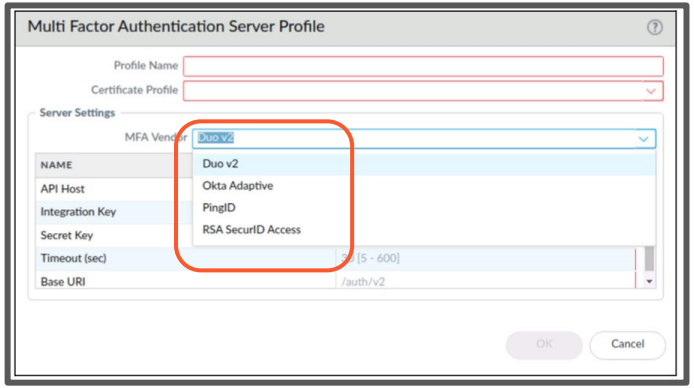




1.4.6 Server Profile & Authentication Profile







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

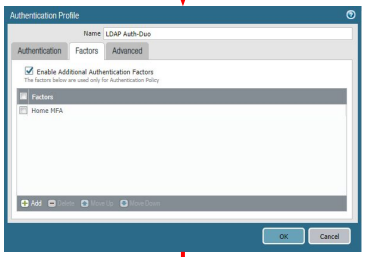
	Name	Tags	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Service	Authentication Enforcement	Log Settings	Hit Count
1	Exclude-Auth-rule	none	L3-Trust	any	any	any	L3-Untrust	any	service-http service-https	default-no-captive-portal		80
2	CP-Auth-Rule	none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

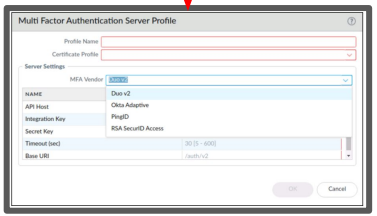
Note: the the authentication is enabled through captive portal capability.

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

AD Authentication via Authentication Profile - 1st Factor

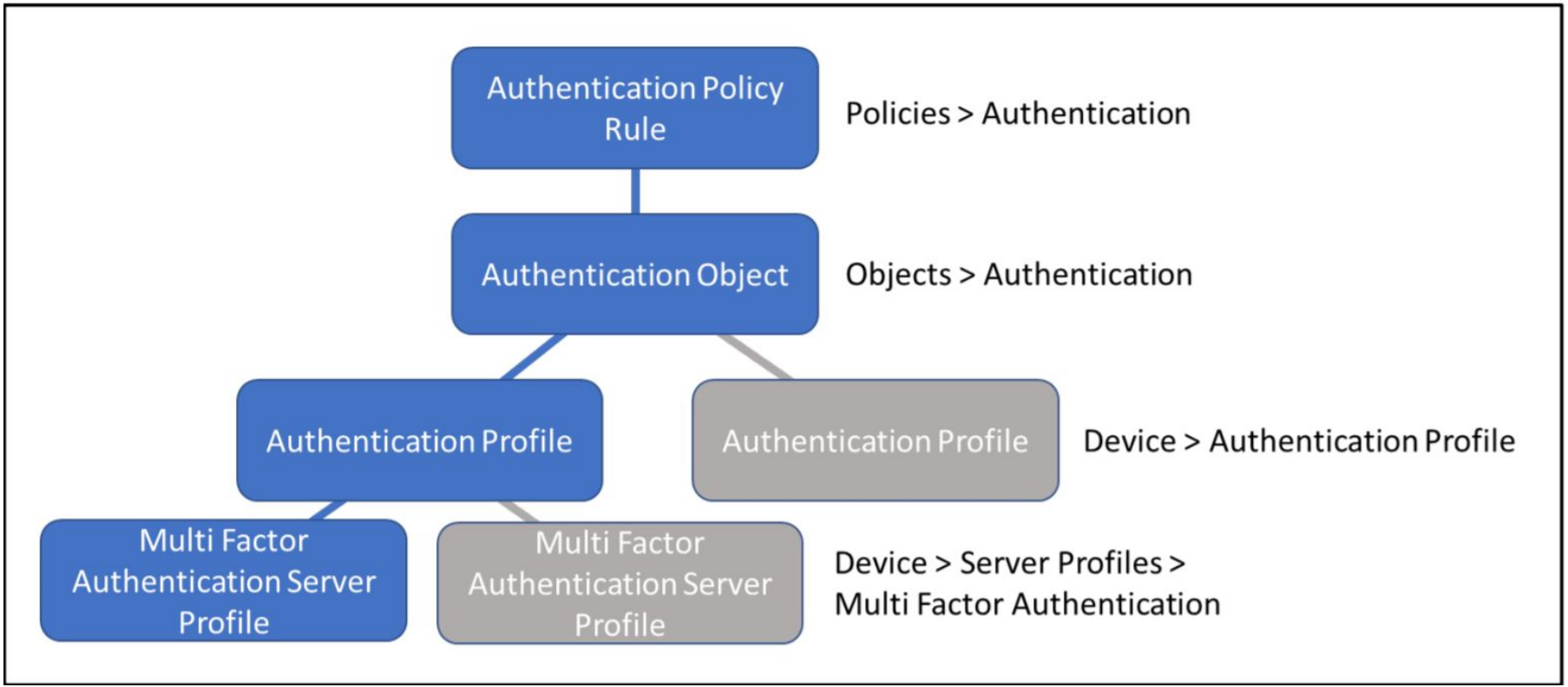


MFA Authentication via Additional Factors - 2nd Factor



1.5.2 Dependencies

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



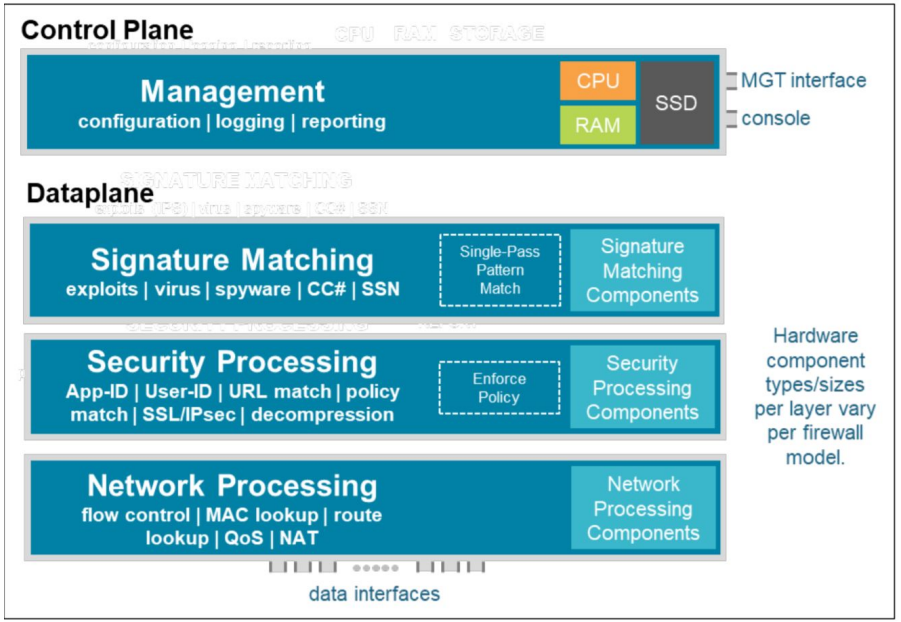
1.6 Differentiate between the fundamental functions that reside on the management plane and data plane

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.

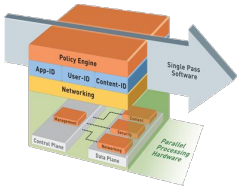
Functions That Reside in the Management Plane

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

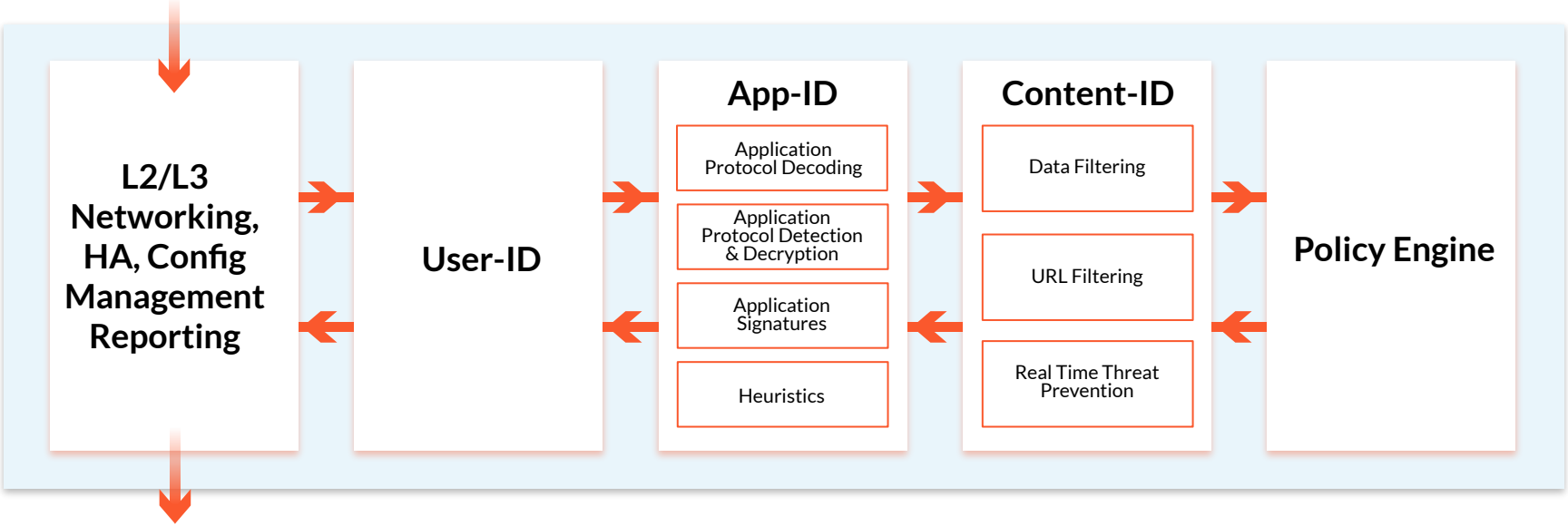


PA-220 Architecture

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

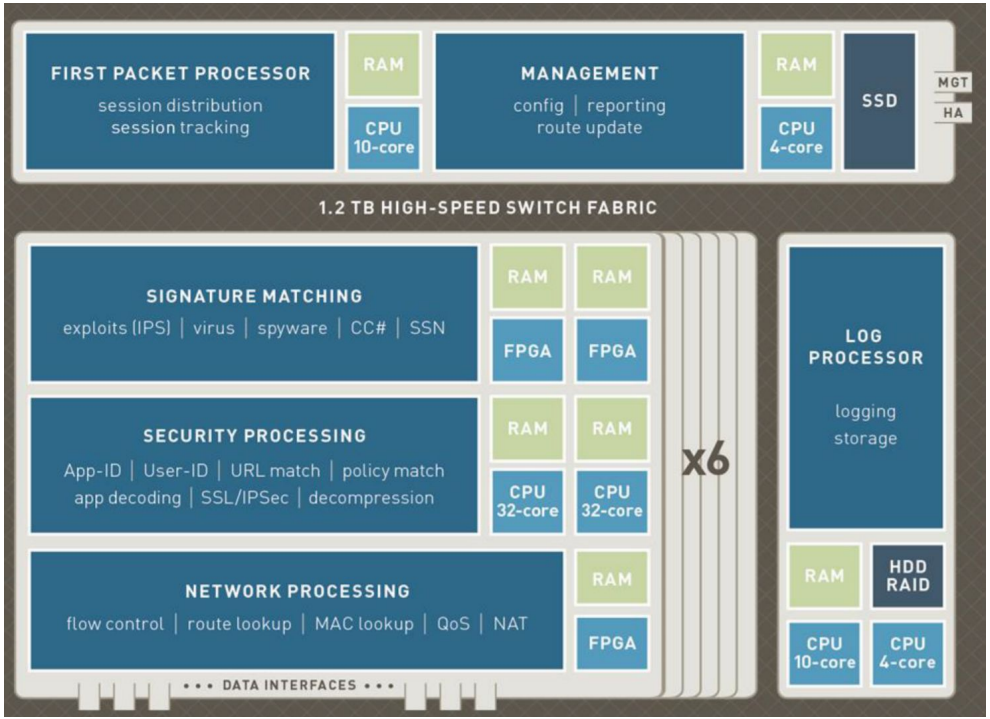


 |

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

