Palo Alto Solutions, Services, and Tools

As of early 2026, the Palo Alto Networks landscape has shifted significantly, particularly in the "Tools" domain where legacy engineering utilities have been deprecated in favor of AI-driven cloud management. Below is a breakdown of the current Solutions, Services, and Tools, tailored to your engineering profile.

1. Critical Engineering Tool Updates (2025-2026)

For network security engineers accustomed to "IronSkillet" and "Expedition," the toolset has undergone a major transformation.

- **Expedition (End-of-Life):** As of January 2025, the **Expedition** migration tool (formerly Migration Tool 3.0) is officially End-of-Life (EOL) and no longer supported.[1] [2]
- **IronSkillet (Superseded):** The IronSkillet "Day 1" configuration templates are now considered stagnant. They have been functionally replaced by **Strata Cloud Manager (SCM)**, which integrates best-practice logic directly into the management plane.[1]
- **BPA+ (Best Practice Assessment Plus):** The standalone BPA tool has evolved into **BPA+** and is now embedded within SCM and AIOps for NGFW. It not only reports issues but provides a "remediation engine" that can automatically generate CLI commands to fix configuration gaps.[1]
- **Automation SDKs:** While GUI tools are consolidating, the **PAN-OS Python SDK**, **pan-python**, and **Ansible Galaxy collections** remain the standard for programmable automation. [1]

2. Core Solutions Portfolio

The portfolio remains divided into three primary pillars, with deep integration of "Precision AI" Copilots across all platforms.[3]

Strata (Network Security)

- **Form Factors:** Includes **PA-Series** (Hardware NGFW), **VM-Series** (Virtual), and **CN-Series** (Container).
- **Management:**
  - **Strata Cloud Manager (SCM):** The unified management platform for NGFWs and SASE, replacing Panorama for many modern deployments.
  - **Panorama:** Remains the centralized manager for on-premise heavy environments but is increasingly being bridged to SCM for AIOps features.

- **New Features: Strata Copilot** (AI assistant for querying logs and configurations).[3]

Prisma (Cloud Security & SASE)

- **Prisma SASE:** Combines **Prisma Access** (SSE/Security) and **Prisma SD-WAN** (Networking).
- **Prisma Cloud:** The Cloud Native Application Protection Platform (CNAPP) covering CSPM, CWPP, and Code Security.
- **Cortex Cloud:** A newer branding emergence in late 2025 that merges elements of Prisma Cloud with Cortex threat detection capabilities.[4] [5]

Cortex (Security Operations)

- **Cortex XSIAM:** The autonomous SOC platform that has largely subsumed separate SIEM/XDR workflows.
- **Cortex XDR:** Extended Detection and Response.
- **Cortex XSOAR:** Security Orchestration, Automation, and Response.
- **Cortex Xpanse:** Attack Surface Management (ASM).

3. Services & Support

- **Unit 42:** The threat intelligence and incident response division. They provide retainers for IR and feed threat data directly into the products (e.g., DNS Security, WildFire).
- **Consulting Services:** Includes QuickStart services for new implementations and specialized architectural reviews.

4. Certification & Education (2026 Framework)

The certification program has been restructured into role-based tracks (Network, Cloud, Operations) with four proficiency levels.[6] [7]

Level	Network Security Track	Cloud Security Track	Security Operations Track
Foundational	**PCCET** (Entry-level cybersecurity)	—	—
Professional	**PCNSA** (Administrator)	**PCCSE** (Prisma Cloud)	**PCDRA** (Detection & Response)
Specialist	**PCNSE** (Engineer - Strata/Panorama)	**Prisma SASE Professional**	**PCSAE** (Automation - XSOAR)
Architect	**NetSec-Pro** (Network Security Professional)	—	—

Note: The **NetSec-Pro** certification (which matches your study profile) is positioned as an advanced credential focusing on architectural design and hybrid environments.[8] [6]

⁂

Security and NAT policy creation

Creating Security and NAT policies in the Palo Alto Networks ecosystem requires navigating two different management paradigms in 2026: the traditional **Panorama/Local** interface and the modern **Strata Cloud Manager (SCM)**. However, the underlying packet processing logic—the most common source of configuration errors—remains identical across both.

1. The Golden Rule: Packet Flow Logic

The most critical concept for creating valid policies is understanding the "Life of a Packet" inside the firewall. Failure to follow this logic is the primary reason for traffic drops after configuring NAT.

"Security Match: Pre-NAT IP, Post-NAT Zone"
When the firewall evaluates a packet against your **Security Policy**, the packet has effectively gone through a NAT *lookup* (to determine the egress zone) but the IP address has not yet been translated.[17] [18]

Policy Field	Match Criteria (What to put in the rule)
Source Zone	**Real Source Zone** (Where the packet came from)
Source IP	**Real (Pre-NAT) IP** (The original IP of the sender)
Dest. Zone	**Post-NAT Zone** (The zone where the *translated* IP would theoretically sit)
Dest. IP	**Real (Pre-NAT) IP** (The public/VIP IP the sender is *trying* to reach)

- **Example (Web Server VIP):** If you have a web server at `10.1.1.5` (DMZ) reachable via Public IP `203.0.113.5` (Untrust), your **Security Policy** must allow traffic to Dest IP `203.0.113.5` (Public), but Dest Zone `DMZ`.

2. NAT Policy Creation

NAT policies translate addresses (Source or Destination) and are evaluated *before* Security Policies to determine the "Post-NAT Zone".[19]

Source NAT (SNAT)

Used to allow internal users to access the internet using a public IP.

- **Dynamic IP and Port (DIPP):** The standard "Many-to-One" or PAT. Maps thousands of internal hosts to a single interface IP.
- **Dynamic IP:** "Many-to-Few." Selects the next available IP from a pool.
- **Creation Tip:** In the **Original Packet** tab, match your internal Source Zone/Subnet. In the **Translated Packet** tab, typically select "Dynamic IP and Port" and "Interface Address" (your external interface).[20]

Destination NAT (DNAT)

Used to publish internal servers to the internet.

- **Bi-directional:** When creating a Static NAT for a server, you can check "Bi-directional" to automatically create the reverse SNAT rule (allowing the server to initiate outbound connections using its VIP).[21]
- **Creation Tip:** Always ensure your Destination Zone in the NAT rule matches the *ingress* interface (e.g., "Untrust"), not the server's actual zone.

3. Management Differences: SCM vs. Panorama

In 2026, the workflow differs depending on your management plane.

Strata Cloud Manager (SCM)

SCM has replaced the strict "Device Group vs. Template" separation with a unified **Folder** structure.

- **Folders:** Contain *both* network (Interfaces, Zones) and security (Policies, Objects) configurations. This reduces the need to switch contexts when building a policy that requires a new object.[22]
- **Snippets:** Replace "Template Stacks" for better modularity. You can insert policy snippets into specific folders without complex stack inheritance.[22]
- **Workflow:** Navigate to **Manage > Configuration > NGFW > Security Services**. You will see the familiar rule base but with integrated AIOps recommendations (e.g., "Unused Rules" are highlighted natively).[23]

Panorama / Local Firewall

- **Device Groups:** You must create Security/NAT policies here.
- **Templates:** You must create Zones/Interfaces/VLANs here.
- **Context Switching:** You often have to create the Zone in the Template, push/commit or ensure the context is correct, and then reference it in the Device Group policy. SCM eliminates this friction.[22]

4. Best Practices for 2026

- **Use Tags:** Mandatory for automation. Tags allow dynamic grouping of rules which tools like Cortex XSIAM can leverage for incident response.
- **Log at Session End:** Always enable "Log at Session End" in the **Actions** tab. Logging at "Start" generates excessive noise and lacks flow data (bytes/app-id).
- **Rule Shadowing:** Both SCM and Panorama will warn if a broad rule (e.g., "Allow-All") is placed above a specific rule.
- **Prisma Access Nuance:** If managing Prisma Access, remember that for "Mobile Users," Source NAT is often handled automatically by the service (Cloud egress), reducing the need

for manual SNAT rules compared to on-premise firewalls.[24]

⁂

cloud-delivered security services (CDSS) configuration (security profiles)

To leverage Palo Alto Networks **Cloud-Delivered Security Services (CDSS)** in 2026, you must configure **Security Profiles** and attach them to your Security Policy rules. The configuration workflow has minor differences between **Strata Cloud Manager (SCM)** and **Panorama/Local**, but the core profile types remain consistent.

1. CDSS Profile Types & Configuration

These profiles are the "brain" of the firewall, performing deep packet inspection (Layer 7) beyond simple port/protocol matching.

Advanced Threat Prevention (ATP)

- **Purpose:** Blocks exploits, vulnerability attacks, and C2 (Command & Control) traffic in real-time.
- **Key Configuration:**
    - **Vulnerability Protection Profile:** Use the default "strict" profile or clone it. Ensure highly critical severities are set to `reset-both` (TCP) or `drop` (UDP/ICMP).
    - **Anti-Spyware Profile:** Critical for C2 detection. You *must* enable "DNS Security" sinkholing within this profile (see below).
    - **Inline Cloud Analysis:** In 2026, ATP can perform inline deep learning analysis for zero-day C2 without sending files to the cloud, reducing latency.[33]

Advanced WildFire (Malware Analysis)

- **Purpose:** Sandboxes unknown files to detect zero-day malware.
- **Key Configuration:**
    - **WildFire Analysis Profile:** Define which file types (e.g., PE, PDF, MS Office, script, archive) are forwarded to the WildFire cloud.
    - **Best Practice:** Forward *all* file types and *all* applications ("Any/Any").
    - **Real-time:** Ensure the "Real-time WildFire" action is set to `block` in your Antivirus profile so that signatures generated by WildFire are enforced immediately.[34]

DNS Security

- **Purpose:** Prevents C2 communication via DNS tunneling and blocks malicious domains.
- **Key Configuration:**
  - **Integration:** Unlike other services, DNS Security is configured *inside* the **Anti-Spyware Profile** under the "DNS Policies" tab.[35] [36]
  - **Action:** Set the action to **Sinkhole**. This intercepts the DNS response and returns a dummy IP (the sinkhole IP), allowing you to identify the infected internal host by analyzing traffic destined for that dummy IP.
  - **New in 2025/2026:** Support for inspecting **DNS over HTTPS (DoH)** and **DNS over TLS (DoT)** is now native, provided SSL Decryption is enabled.[37]

SaaS Security Inline (formerly CASB)

- **Purpose:** Discovers and controls Shadow IT and sanctioned SaaS usage.
- **Key Configuration:**
  - **Activation:** Requires linking the firewall to the SaaS Security cloud tenant.
  - **Policy:** Instead of manually creating HTTP header insertion rules, you now use the **SaaS Policy Recommendation** engine (or snippets in SCM) to automatically generate rules that enforce tenant restrictions (e.g., "Allow Corporate Gmail, Block Personal Gmail").[38] [39]

2. Workflow: Attaching Profiles to Rules

A Security Policy rule allows traffic (e.g., "Allow Web Browsing"), but the *Profile* scans it.

Step	SCM (Strata Cloud Manager)	Panorama / Local PAN-OS
1. Create	Go to **Objects > Security Profiles**. Create distinct profiles for AV, Spyware, Vuln, etc.	Same path: **Objects > Security Profiles**.
2. Group (Optional)	**Profile Groups** are highly recommended (and sometimes mandatory in SCM wizards) to bundle profiles (e.g., "Standard-Internet-Access").	Profile Groups exist but are optional. You can attach individual profiles directly.
3. Attach	In **Security Services > Security Policy**, edit a rule. Go to the **Profile** tab and select the Group or individual profiles.	In **Policies > Security**, edit a rule. Go to the **Actions** tab and select the Profile Setting.
4. Log	Ensure "Log at Session End" is enabled to capture the threat log.	Same.

3. Best Practices for 2026

- **Profile Groups:** Use them to ensure consistency. If you update the "Standard_Web" group to include a new URL category, all rules using that group update automatically.[40]
- **SSL Decryption:** CDSS effectiveness is severely limited without SSL Decryption. Nearly 95% of web traffic is encrypted; without decryption, WildFire and ATP cannot inspect the

payload.[41]

- **Inline Deep Learning:** In ATP and WildFire profiles, explicitly enable "Inline Cloud Analysis" models if available in your PAN-OS version (11.x+) to catch highly evasive threats that traditional signatures miss.[33]

4. Cheat Sheet: Profile Actions

Profile	Recommended Action	Why?
Antivirus	**Reset-both** (TCP) / **Drop** (UDP)	Kills the connection immediately upon virus detection.
Vulnerability	**Reset-both** (Critical/High)	Blocks exploits. Use "Default" for Low/Info to avoid false positives unless tuning.
Anti-Spyware	**Reset-both** (C2) / **Sinkhole** (DNS)	Sinkholing is mandatory for identifying the infected source machine.
URL Filtering	**Block** (Malware, Phishing, C2)	Prevents access to known bad sites.

⁂

user-id and app-id

App-ID (Application Identification) and **User-ID** (User Identification) are the foundational pillars of the "Next-Generation" architecture. Instead of managing static IPs and Ports, you manage *Who* is accessing *What*.

1. App-ID: The "What"

App-ID identifies the underlying application irrespective of the port, protocol, or encryption (SSL/TLS). This eliminates the "port hopping" evasive techniques used by modern malware and shadow IT apps.[48] [49]

Core Concepts

- **Layer 7 Visibility:** App-ID scans the payload. A rule for `ssl` is not the same as a rule for `facebook-base` running *over* SSL.
- **Implicit vs. Explicit:**
  - **Implicit Usage:** When you allow `facebook-base`, App-ID automatically understands it runs on tcp/443. You do *not* need to hardcode "Service: tcp-443" unless you want to *restrict* it to non-standard ports (rare).[50]
  - **Best Practice:** Set the "Service" column to `application-default`. This ensures the application is only allowed on its standard ports (e.g., SSH on 22). If SSH traffic appears on port 80, the firewall blocks it, preventing evasion.[50]
- **Dependencies:** Some applications require others to function (e.g., `web-browsing` or `ssl`).
  - **Implicit Dependencies:** Modern PAN-OS versions often handle this silently.

  - **Explicit Dependencies:** If you add `facebook-posting`, the firewall may warn you to also allow `facebook-base` and `web-browsing`. SCM and Panorama often have a "Resolve Dependencies" button to fix this automatically.[51] [50]

2. User-ID: The "Who"

User-ID maps IP addresses to usernames, allowing you to write policies like "Allow **Marketing-Group** to access **LinkedIn**" instead of managing subnet lists.[48]

Mapping Methods (2026 Standards)

- **Cloud Identity Engine (CIE):** This is the modern standard, replacing many on-premise "User-ID Agents." CIE connects directly to cloud directories (Entra ID, Okta, Google Workspace) and on-prem AD to aggregate user data. It pushes mappings to all firewalls/Prisma Access nodes instantly, solving the "roaming user" visibility problem.[52] [53]
  - **Configuration:** You configure the **Cloud Identity Engine** profile under **Device > User Identification**.
- **Integrated User-ID Agent:** For strictly on-premise environments, the firewall can query Active Directory directly (WMI/WinRM) or monitor Exchange logs.
- **Captive Portal:** A fallback for unidentifiable users (e.g., Guest Wi-Fi). It forces a browser login page to capture identity.

Configuration Best Practices

1. **Zone Enablement:** You must explicitly enable "User-ID" on the **Zone** configuration (Network > Zones). If this box is unchecked, the firewall ignores user mappings for traffic entering that zone.[54]
2. **Ignore Lists:** Configure the "Ignore User List" to exclude service accounts or background daemons (e.g., "backup_svc") that might generate noise or incorrect mappings on multi-user servers.[55]
3. **Group Mapping:** Configure **Group Mapping Settings** to pull LDAP/AD group structures. This allows you to use group names directly in Security Policies.[53] [55]

3. Interaction & Order of Operations

Understanding how they interact is crucial for troubleshooting "Incomplete" or blocked traffic.

1. **Initial Handshake:** The firewall initially allows the TCP handshake based on Layer 4 (Port).
2. **App-ID Shift:** Once data flows, the App-ID engine inspects the signature.
   - *Scenario:* You have a rule allowing `ssh` (App) on `application-default` (Service).
   - *Traffic:* User tries SSH on port 80.
   - *Result:* Blocked. The application (`ssh`) matches, but the port (80) does not match the default (22).

3. **User-ID Evaluation:** User mappings are checked continuously. If a user's IP mapping expires (timeout), their session might suddenly hit the "Interzone-Default" deny rule.

4. Summary Table: What to Configure

Feature	Where to Configure	Key Setting	"Gotcha" to Avoid
App-ID	**Objects > Applications**	**Service: application-default**	Don't use "Service: Any" unless necessary; it breaks port security.
User-ID	**Network > Zones**	**Enable User Identification** (checkbox)	Forgetting to enable this on the *Source* zone results in "unknown" users.
Groups	**Device > User Identification**	**Group Mapping Profile**	Ensure you only import relevant groups to save management plane memory.
CIE	**Device > Cloud Identity Engine**	**Cloud Identity Engine Profile**	Requires a valid certificate and cloud pairing key [56].

⁂

Decryption

SSL/TLS Decryption is arguably the most complex but necessary feature in the Palo Alto Networks ecosystem. In 2026, with over 95% of web traffic encrypted, a firewall without decryption is effectively blind to modern threats.

1. Types of Decryption

There are two distinct modes, and mixing them up is a common error.

SSL Forward Proxy (Outbound)

- **Use Case:** Users inside your network accessing the Internet (e.g., browsing Google, downloading files).
- **Mechanism:** The firewall acts as a "Man-in-the-Middle" (MitM). It intercepts the user's connection, presents a *forward trust* certificate (signed by your internal CA), and then establishes a separate connection to the destination server.
- **Requirement:** Your internal PKI Root CA (or a Sub-CA) must be trusted by all client devices (PCs, phones) to avoid certificate browser errors. [63] [64]

SSL Inbound Inspection (Inbound)

- **Use Case:** External users accessing your internal servers (e.g., your public web server `www.company.com`).
- **Mechanism:** You upload the *actual* server certificate and private key to the firewall. The firewall passively decrypts the traffic or acts as a proxy to inspect threats directed at your server. [65] [66]

- **Requirement:** You must own the domain and have access to the private key. You cannot do this for servers you don't own (e.g., you can't inspect inbound traffic to Azure/AWS unless you control the keys).
- **TLS 1.3 Note:** For TLS 1.3 inbound inspection, the firewall cannot "passively" sniff traffic due to Perfect Forward Secrecy (PFS). It must act as a proxy. As of PAN-OS 11.2 (and into 2026), support for HSM-protected keys with TLS 1.3 is now available.[67]

2. Configuration Best Practices (2026)

Decryption Profiles

Never use the default profile. Create custom profiles to enforce security standards.[68]

- **Block Unsupported Modes:** In your "Forward Proxy" profile, strictly block expired certificates and untrusted issuers.
- **Protocol Versions:** Set **Min Version** to TLS 1.2 and **Max Version** to `Max` (TLS 1.3).
    - *Trap:* Do not block TLS 1.3 in the "No Decryption" profile. Since the certificate is encrypted in TLS 1.3, the firewall often cannot see the certificate details *unless* it decrypts first or relies on SNI.[68]
- **Cipher Suites:** Enforce PFS (ECDHE) ciphers. Avoid legacy RSA key exchange where possible.

Policy Rules: The "Do Not Decrypt" First Approach

Decryption is resource-intensive and legally sensitive. Build your policy top-down:

1. **Rule 1: Sensitive Categories (No Decrypt)**
    - **Action:** No Decrypt.
    - **Categories:** Financial Services, Health and Medicine, Government. (This ensures legal/privacy compliance).
2. **Rule 2: Technical Exclusions (No Decrypt)**
    - **Action:** No Decrypt.
    - **Source:** Specific device groups (e.g., IoT devices, printers) that don't support custom CAs.
    - **Categories:** Streaming Media (Netflix), Software Updates (Windows Update). Decrypting these breaks the apps or kills firewall CPU.[69]
3. **Rule 3: Decrypt All Else**
    - **Action:** Decrypt (Forward Proxy).
    - **Scope:** User traffic to "General Internet" categories.

3. Troubleshooting & "Broken" Apps

When an application breaks (e.g., Dropbox, banking apps), it's usually due to **Certificate Pinning** or **Client Certificate Authentication**.[70] [69]

- **Predefined Exclusion List:** Palo Alto Networks maintains a list of sites known to break with decryption. Ensure this is enabled in **Device > Certificate Management > SSL Decryption Exclusion**.
- **Custom Exclusions:** If a new app breaks, add its SNI (domain) to a custom exclusion list.
- **Logs:** Check the **Decryption Log** (a separate log subtype in Monitor > Logs). Look for "error" in the error column to identify handshake failures.

4. Hardware Security Modules (HSM)

For high-security environments (finance/gov), storing private keys on the firewall disk is forbidden. You can integrate a Network HSM (e.g., Thales Luna, Entrust nShield) to handle the signing operations remotely.

- **New in 2025/2026:** Full support for TLS 1.3 Inbound Inspection even when keys are locked in an HSM.[67]

5. Summary Checklist

Task	Configuration Location	Critical Setting
Certificates	**Device > Certificate Management**	Mark your CA as "Forward Trust Certificate".
Profile	**Objects > Decryption Profile**	Block "Expired" and "Untrusted" issuers.
Policy	**Policies > Decryption**	Place "Sensitive/Health/Finance" **No Decrypt** rules at the top.
Inbound Keys	**Device > Certificates**	Import the Private Key for your internal web servers.

⁂

PKI Root CA

Integrating your Palo Alto Networks firewall with your **PKI Root CA** is the standard for avoiding certificate errors during SSL Decryption. Instead of manually installing a firewall-generated "Self-Signed" certificate on every endpoint (which is unmanageable), you issue a **Subordinate CA (Sub-CA)** certificate to the firewall from your existing Enterprise Root CA.

1. The Trust Hierarchy

To make decryption seamless, the firewall must be a valid issuer in your existing "Chain of Trust."

- **Enterprise Root CA:** The top-level authority (e.g., your Microsoft AD CS Root) already trusted by all domain computers.
- **Intermediate/Sub-CA (The Firewall):** You generate a key pair on the firewall, send the public key (CSR) to your Root CA, and the Root CA signs it. This gives the firewall the authority to "mint" certificates for Google, Facebook, etc., on the fly.
- **The Client:** Since the client trusts the Root CA, it automatically trusts any certificate signed by the firewall (the Sub-CA).[78] [79]

2. Configuration Workflow (The "CSR Method")

Do not generate a self-signed cert on the firewall for production. Use this workflow:[80] [81]

1. **Generate CSR (Firewall):**
    - Go to **Device > Certificate Management > Certificates**.
    - Click **Generate**.
    - **Name:** `PAN-Decryption-SubCA` (Use a clear name).
    - **Common Name:** `PAN-Decryption-SubCA` (Must match).
    - **Certificate Authority: Check this box**. (Critical! If unchecked, the signed cert won't be able to sign other certs).
    - **Signed By:** `External Authority (CSR)`.
2. **Sign CSR (PKI Server):**
    - Export the CSR and submit it to your CA (e.g., `certreq` on Windows).
    - **Template:** You must use a "Subordinate CA" template. Do not use a "Web Server" template; it lacks the `Key Cert Sign` usage capability.
3. **Import & Activate (Firewall):**
    - Import the signed certificate. It must have the *exact same name* as the CSR you generated.
    - Click the certificate name and check the box **Forward Trust Certificate**.[78]

3. Forward Trust vs. Forward Untrust

You need two certificates for the decryption engine to work logically.[82] [83]

Certificate Role	Purpose	How it works
Forward Trust	**The Norm.** Used when the destination site is valid.	When a user visits `google.com` (valid), the firewall mints a fake `google.com` cert signed by this "Trust" CA. The browser sees it chains to your Enterprise Root and accepts it silently.

Certificate Role	Purpose	How it works
Forward Untrust	**The Warning.** Used when the destination site is *invalid* (expired/hacked).	When a user visits `bad-site.com` (expired), the firewall mints a fake cert signed by this "Untrust" CA. You *intentionally* do NOT push this CA to clients. The browser sees an untrusted issuer and throws a scary red warning, alerting the user.

- **Best Practice:** The **Forward Untrust** certificate can be self-signed on the firewall. You do not need to sign it with your Enterprise PKI (in fact, you shouldn't, or the browser won't warn the user).[84]

4. Important Considerations for 2026

- **Validity Period:** Microsoft and other CA vendors are shortening validity periods. A standard Sub-CA might be valid for 5-10 years, but ensure it doesn't exceed the remaining life of your Root CA.[85]
- **HSM Usage:** In high-security environments, you cannot store the Sub-CA private key on the firewall disk. You generate the CSR on an HSM (Hardware Security Module) and link the firewall to it. The firewall sends "signing requests" to the HSM for every new session.[78]
- **Subject Alternative Name (SAN):** Modern browsers (Chrome/Edge) strictly require SAN fields. When creating your CSR, ensure the CN is also repeated in the SAN field to avoid "Common Name Invalid" errors on stricter clients.[86]

⁂

mean of PKI and CSR

You asked about the meaning of **PKI** (Public Key Infrastructure) and **CSR** (Certificate Signing Request). These concepts are the bedrock of trust for everything from SSL Decryption to VPN authentication.

1. PKI (Public Key Infrastructure)

The "Passport System" of the Digital World
Think of PKI as a government system for issuing passports. You trust a passport because it was issued by a trusted government authority.

- **Definition:** A framework of policies, hardware, and software used to create, manage, and revoke digital certificates.[93] [94]
- **Core Purpose:** To bind an identity (e.g., `google.com` or `User John`) to a cryptographic key.
- **Key Components:**
  - **CA (Certificate Authority):** The "Government Office" that issues the passports (Certificates).
  - **Digital Certificate:** The "Passport" itself. It says "This public key belongs to Google."

  - **CRL/OCSP:** The "Revocation List." A way to check if a passport has been stolen or cancelled.

2. CSR (Certificate Signing Request)

The "Application Form"
When you want a digital certificate (passport), you don't just print one yourself; you fill out a form and send it to the authority.

- **Definition:** A block of encrypted text that you generate on your server (or firewall) and send to a CA to apply for a certificate.[95]
- **What's Inside a CSR?**
  - **Public Key:** The lock you want people to use to send you secret messages.
  - **Subject Info:** Your details (Common Name `vpn.company.com`, Organization `Acme Corp`, Country `US`).
  - **Signature:** A digital signature proving *you* generated the request.
- **Why use it?** It allows you to get a signed certificate *without* ever revealing your **Private Key** to the CA. Your Private Key remains safely on your firewall/server and never travels across the network.

3. How They Work Together (The Workflow)

1. **Generation:** You (the Firewall) generate a **Key Pair** (Private Key + Public Key).
2. **Application:** You create a **CSR** containing your Public Key + ID info.
3. **Submission:** You send the **CSR** to the **PKI** (CA).
4. **Issuance:** The CA verifies your ID, signs your CSR with *its* Private Key, and returns a **Certificate**.
5. **Installation:** You import the Certificate. Now, anyone who trusts the PKI (CA) automatically trusts you.

Summary Table

Acronym	Metaphor	Technical Role
PKI	The **Government**	The entire system of trust (CAs, policies, revocation lists).
CA	The **Passport Office**	The entity that signs and issues certificates.
CSR	The **Application Form**	A file sent to the CA to ask for a certificate. Contains your Public Key.
Certificate	The **Passport**	The signed document proving your identity.

⁂

monitoring and logging

Monitoring and Logging in the Palo Alto Networks ecosystem has evolved into a "Cloud-First" model in 2026. While the local firewall logs remain fundamental, the architecture for *storage and analysis* has shifted from on-box retention to the **Strata Logging Service (SLS)** and unified dashboards in **Strata Cloud Manager (SCM)**.

1. The Core Architecture: Where do logs go?

The destination for your logs depends on your management architecture:

- **Local Logging (On-Box):** The firewall stores logs on its local SSD. This is still the default for standalone units but is discouraged for retention due to limited space (logs roll over quickly).
- **Panorama (Legacy Centralized):** Firewalls forward logs to Panorama or a "Log Collector Group" (M-Series appliances). This is the traditional on-premise method.
- **Strata Logging Service (SLS):** (Formerly *Cortex Data Lake*) This is the cloud-native standard for 2026. All firewalls (hardware, VM, Prisma Access) forward logs to this cloud repository. It acts as the "single source of truth" for SCM, Cortex XDR, and Cortex XSIAM. [104] [105]

2. Log Types & Critical Fields

Understanding the specific log types is crucial for passing exams and troubleshooting.

Log Type	What it tells you	Critical Fields to Check
Traffic	**Flow Data.** (Bytes, Packets, Allow/Deny). It does *not* show payload details.	`Session End Reason` (e.g., `tcp-rst-from-client` vs `policy-deny`), `Bytes Sent/Received` (Zero bytes often means a routing/NAT issue).
Threat	**Security Events.** (Virus, Spyware, Vuln). Generated only when a Security Profile triggers.	`Threat Name` (e.g., "Generic.Malware"), `Action` (alert vs reset-both), `Pcap_ID` (click to download the packet capture).
Unified	**Consolidated View.** Merges Traffic, Threat, URL, and Data logs into one timeline.	Useful for seeing the "whole picture" of a user's session without switching tabs [106].
System	**Hardware/OS Health.** (Link down, HA failover, User-ID connection loss).	`Severity` (Critical/High), `Description` (e.g., "HA Group 1: Moved to Active").
Config	**Audit Trail.** Who changed what and when.	`Admin`, `Path`, `Before Change / After Change` (diff view).

3. Monitoring Tools (GUI)

ACC (Application Command Center)

- **What it is:** The "Manager's View." A graphical dashboard providing a high-level overview of network traffic (e.g., "Top 10 High-Risk Applications," "Top Threats").
- **Usage:** Use this to identify trends (e.g., a sudden spike in `bittorrent` traffic) before drilling down into raw logs.
- **Change in 2026:** In SCM, ACC is evolved into the **"Command Center,"** which adds predictive analytics (e.g., "Your capacity will be exceeded in 3 days").[107]

Monitor Tab (The Engineer's View)

- **What it is:** The raw log viewer. This is where you spend 90% of your troubleshooting time.
- **Power Feature: Query Builder.** You can build complex boolean queries (e.g., `(addr.src in 10.0.0.0/8) and (port.dst eq 443) and (action neq allow)`).

4. Best Practices for 2026

- **Log at Session End: Always** enable "Log at Session End" in your Security Policy. Disabling this leaves you blind.
    - *Warning:* Do **not** enable "Log at Session Start" unless diagnosing a specific TCP handshake issue. It doubles your log volume and fills storage instantly.
- **Log Forwarding Profiles:** Never rely solely on local logs. Create a **Log Forwarding Profile** to send critical logs to:
    - **SLS:** For long-term retention and SCM visibility.
    - **Syslog/SIEM:** For correlation with other vendors (Splunk, QRadar).
    - **Email:** Only for "Critical" System events (e.g., HA Failover). *Never* email Traffic logs.[108]
- **Decryption Logging:** If troubleshooting SSL, enable the separate **Decryption Log** to see handshake failures (e.g., "Certificate Untrusted"). Note: In PAN-OS 11.x, HTTP/2 logs appear in "Tunnel Inspection" logs when decryption is enabled.[109]

5. Troubleshooting with "Flow Basic"

When logs aren't enough (e.g., the traffic log never appears because the packet was dropped *before* the session started), use the CLI.

- **Packet Capture (PCAP):** The "Filters" feature in the GUI is good, but the CLI is better for dropping stages.
- **Flow Basic:** The command `show counter global filter packet-filter yes delta yes` allows you to see *why* the box dropped a packet (e.g., `flow_policy_deny`, `tcp_drop_out_of_wnd`).

⁂

Application of CDSS

In the Palo Alto Networks ecosystem, **Cloud-Delivered Security Services (CDSS)** are applied by attaching **Security Profiles** to your **Security Policy** rules. They act as the "content inspection" layer, enforcing security *inside* the allowed application traffic.

Think of the **Security Policy** as the "Bouncer" (checks ID/Port) and **CDSS** as the "X-Ray Machine" (scans the bag).

1. Mapping Problems to CDSS Solutions

Each CDSS service is a specialized engine designed to stop a specific category of threat that a simple firewall rule cannot see.

Business Problem / Threat	CDSS Solution to Apply	Profile Type
"I want to block known viruses and malware."	**Advanced Threat Prevention (ATP)**	Antivirus Profile
"I need to stop hackers from exploiting a vulnerability (e.g., Log4j) in my servers."	**Advanced Threat Prevention (ATP)**	Vulnerability Protection Profile
"I need to prevent infected laptops from talking to Command & Control (C2) servers."	**Advanced Threat Prevention (ATP)** & **DNS Security**	Anti-Spyware Profile (with DNS Sinkhole)
"I want to block users from downloading a brand-new, zero-day virus."	**Advanced WildFire**	WildFire Analysis Profile
"I need to stop users from visiting gambling, porn, or phishing sites."	**Advanced URL Filtering**	URL Filtering Profile
"I want to block 'Shadow IT' (e.g., personal Gmail) but allow corporate Box/Dropbox."	**SaaS Security Inline**	*No Profile* (Applied via Policy Recommendations or HTTP Header Insertion)
"I need to protect my OT/IoT devices (MRI machines, robotic arms) that I can't patch."	**IoT Security**	*No Profile* (Passive learning + Policy Import)

2. How to Apply CDSS in Policy (The "Profile Group" Method)

In 2026, the best practice is to bundle these services into **Security Profile Groups** rather than attaching them one by one. This ensures consistency.

Scenario A: User Internet Access (Outbound)

- **Goal:** Protect employees browsing the web.
- **Apply Profile Group:** `Standard-Internet-Access`
  - **Antivirus:** `default` (Block known viruses)
  - **Anti-Spyware:** `strict-dns-sinkhole` (Block C2 + DNS Sinkhole enabled)

    - **URL Filtering:** `block-bad-cats` (Block Gambling, Adult, Malware, Phishing)
    - **WildFire:** `default` (Forward all unknown files for sandbox analysis)
    - **File Blocking:** `block-risky-files` (Block .exe, .bat, .vbs downloads)

Scenario B: Public Web Server (Inbound)

- **Goal:** Protect your web server (DMZ) from hackers.
- **Apply Profile Group:** `Inbound-Server-Protection`
    - **Vulnerability Protection:** `Strict-Server` (Critical: Blocks SQL Injection, XSS, Buffer Overflows)
    - **Antivirus:** `default` (Prevents users from uploading malware to your server)
    - **Anti-Spyware:** `strict` (Prevents the server from beaconing out if it gets compromised)
    - **URL Filtering:** *Not typically needed for inbound, unless the server acts as a proxy.*

3. The "Gotcha": Decryption is Mandatory

You cannot apply CDSS to traffic you cannot see.

- **Fact:** Over 95% of malware is delivered via encrypted channels (HTTPS).
- **Rule:** If you apply an Antivirus profile to an HTTPS stream *without* a Decryption Policy, the firewall can only inspect the TCP handshake. The virus inside the SSL tunnel passes right through.
- **Application: Decryption Policy** + **Security Policy (with CDSS)** = Effective Protection.

4. Special Application: DNS Security

Unlike other profiles, DNS Security is applied *inside* the **Anti-Spyware Profile**.

- **Why?** DNS is a primary channel for "Command and Control" (C2). Malware uses random domains (DGA) to phone home.
- **Application:** You must open your Anti-Spyware profile, go to the **DNS Policies** tab, and set the action to **Sinkhole**. This allows the firewall to "lie" to the infected client, resolving the bad domain to a local IP so you can identify the victim.

ingternet of things security

IoT Security (Internet of Things) for Palo Alto Networks is an add-on subscription that solves the core problem of "unmanaged devices" (MRI machines, IP cameras, Smart TVs) that cannot run agents like GlobalProtect or Cortex XDR.

1. The Core Problem: "You Can't Secure What You Can't See"

IoT devices are black boxes. They often run outdated Linux kernels, have hardcoded passwords, and are prime targets for lateral movement. The IoT Security subscription uses **Machine Learning (ML)** to passively identify devices and recommend policies.[119]

2. Implementation Architecture: Sensors

The firewall acts as a **sensor**. It collects metadata (DHCP, DNS, Headers) and sends it to the IoT Security Cloud for analysis. It does *not* send the full payload, just the metadata.[120]

Deployment Modes

1. **Inline (Layer 3 Interface):** The firewall is the gateway for the IoT VLAN.
    - *Pros:* Can block attacks immediately (IPS).
    - *Cons:* Risk of disrupting sensitive OT gear if misconfigured.
2. **TAP / Span (Passive):** The firewall connects to a switch mirror port.
    - *Pros:* Zero risk of disruption. Perfect for "Audit Mode."
    - *Cons:* Cannot block attacks; can only alert.[121]

3. Critical Configuration: DHCP Visibility

This is the most common failure point.
For IoT Security to work, the firewall *must* see the DHCP exchange (DORA process). This is how it learns the **MAC Address**, which is the unique identifier for IoT devices.[122]

- **Best Practice:** Configure the firewall as a **DHCP Relay** for your IoT VLANs. If the DHCP server is on a different subnet and traffic doesn't pass through the firewall, the solution will fail to fingerprint devices accurately.

4. The "Policy Recommendation" Workflow

Instead of writing manual rules (e.g., "Allow Camera A to IP X"), you use the ML engine to write them for you.[123]

1. **Discovery (Wait Time):** Let the system run for ~7 days to learn "normal" behavior.
2. **Confidence Score:** Wait for the device profile to hit **90% Confidence.**[123]
3. **Review Recommendations:** The cloud will suggest a policy: *"This is a Hikvision Camera. It should only talk to the NVR (10.1.1.50) and the NTP server. Block everything else."*
4. **Import:** Click **"Import"** to push this policy to Panorama or the Firewall. It creates a rule using **Device-ID** objects (e.g., `Src Device: Hikvision-Cam`).

5. Summary Checklist

Component	Requirement	Why?
DHCP	**DHCP Relay** or **Broadcast Visibility**	Required to map IP-to-MAC and fingerprint the vendor/model.
Log Forwarding	**Cortex Data Lake**	The firewall must upload metadata to the cloud for ML analysis.
Policy	**Device-ID Objects**	Allows you to write rules based on "What it is" (Camera) rather than "Where it is" (IP).
Tap vs Inline	**TAP** for initial audit; **Inline** for enforcement	Start with TAP in critical OT/Hospital environments to avoid accidental outages [121].

⁂

mean of TAP for initial audit

The term **TAP (Test Access Point)** in the context of a Palo Alto Networks audit or IoT deployment refers to a **passive interface mode**. It allows the firewall to "see" traffic without being "in" the traffic path.

1. What is TAP Mode?

In TAP mode, the firewall acts like a sophisticated recording device. It receives a copy of network traffic (usually from a Switch SPAN/Mirror port) but **cannot stop or alter it**.

- **The Metaphor:** It's like a security camera recording a hallway. It can see a thief (malware) and alert the guards (you), but it cannot lock the door to stop them.
- **Technical Detail:** The interface does not have an IP address and does not route traffic. It simply ingests packets for inspection by the App-ID, User-ID, and Threat engines.[134] [135]

2. Why use it for an "Initial Audit"?

When deploying IoT Security or proof-of-concept (POV) firewalls, TAP is the gold standard for the "Discovery Phase."

- **Zero Risk of Outage:** Because the firewall is not inline, a misconfiguration (e.g., a "Block All" rule) cannot disconnect your critical MRI machines or SCADA controllers. The firewall is effectively invisible to the network.[135]
- **Baseline Discovery:** It allows you to let the system run for weeks to learn "normal" behavior. You can answer questions like: *"What exactly is that 10-year-old printer talking to?"* without fear of breaking its connection.[136]
- **IoT Fingerprinting:** The IoT Security subscription needs to see DHCP and HTTP headers to identify devices (e.g., "This is a Samsung Smart TV"). TAP mode allows you to feed this data to the cloud safely.

3. Limitations (The "Gotchas")

- **No Enforcement:** You cannot block threats. If the firewall sees a virus, it can only generate an **Alert** log. It cannot send a TCP Reset (RST) packet because it isn't part of the conversation.[134]
- **Asymmetric Traffic:** If you configure your Switch SPAN port incorrectly (e.g., only mirroring TX and not RX), the firewall will see "half" conversations. App-ID will fail to identify applications correctly, leading to "Incomplete" or "Unknown" results.[136]

4. Configuration Steps

1. **Switch Side:** Configure a SPAN/Mirror session on your core switch. Destination = The port connected to the firewall.
2. **Firewall Side:**
    - **Interface Type:** Set to **Tap**.
    - **Zone:** Create a special zone (e.g., `Tap_Zone`).
    - **Policy:** Create a rule: `Source: Tap_Zone` → `Dest: Tap_Zone` → `Action: Allow`. (You must "allow" the traffic for the logging engine to process and record it).[134]

⁂

Enterprise data loss prevention (DLP)

Enterprise Data Loss Prevention (DLP) in the Palo Alto Networks ecosystem is a cloud-delivered service that integrates across NGFWs, Prisma Access, and Prisma Cloud (CASB). Its primary goal is to prevent sensitive data (PII, credit cards, intellectual property) from leaving your organization, whether via email, web uploads, or SaaS applications.

1. Core DLP Matching Methods

Understanding the difference between **Exact Data Matching (EDM)** and **Indexed Document Matching (IDM)** is critical for configuration and exam scenarios.

Feature	Best For...	How it Works
Exact Data Matching (EDM)	**Structured Data** (Spreadsheets, Databases). E.g., a list of 10,000 valid Credit Card numbers or Customer IDs.	You upload a "hashed" CSV of your database to the DLP cloud. The firewall inspects traffic for *exact matches* of these values (e.g., "This specific SSN matches row 504 in the database"). This drastically reduces false positives compared to generic Regex patterns [144].
Indexed Document Matching (IDM)	**Unstructured Data** (Word docs, PDFs, Design specs). E.g., A blank "Standard Employment Contract" or "Top Secret Schematics."	You upload a sample document. The system creates a "fingerprint" (hash) of the text. It then detects if users try to upload that document (or one that is 80% similar) to a public site [145] [146].

Feature	Best For...	How it Works
Predefined Patterns	**Generic Compliance** (GDPR, HIPAA). E.g., "Any string that looks like a Visa card."	Uses regular expressions and machine learning to detect patterns like `\d{3}-\d{2}-\d{4}` (SSN) [147].

2. Architecture: Single Engine, Everywhere

The key advantage of Palo Alto's approach is the "Single Pass" architecture.

- **Unified Policy:** You define a Data Pattern *once* (e.g., "Confidential-Project-X") in **Strata Cloud Manager** or **Panorama**.
- **Universal Enforcement:** This same pattern is pushed to:
    - **NGFWs** (Physical firewalls at the perimeter).
    - **Prisma Access** (Securing remote users).
    - **Prisma Cloud / CASB-X** (Scanning "Data at Rest" stored in OneDrive/Box).[148] [149]

3. Integration with CASB (SaaS Security)

DLP is the "content engine" for CASB.

- **Inline CASB:** Uses DLP to block a user from *uploading* a sensitive file to Personal Dropbox in real-time.
- **API CASB (Out-of-Band):** Uses DLP to scan files *already stored* in Corporate Box. If it finds a file with Credit Card numbers shared publicly, it can automatically revoke the share link or quarantine the file.[150] [148]

4. Configuration Steps (High Level)

1. **Define Patterns:**
    - Go to **Objects > DLP > Data Patterns**.
    - Create a pattern (e.g., "Regex for Project Codename").
    - *Optional:* Upload your EDM/IDM datasets to the DLP Cloud service.
2. **Create Profile:**
    - Go to **Objects > DLP > Data Filtering Profiles**.
    - Add your patterns and define actions (Alert, Block).
    - *Tip:* Start with **Alert** mode to baseline "normal" business workflows before blocking.
3. **Attach to Policy:**
    - In your **Security Policy**, add the **Data Filtering Profile** to rules allowing outbound traffic (e.g., "Allow Web Browsing").
    - *Requirement:* **SSL Decryption** must be enabled. You cannot inspect encrypted files for sensitive data.[151]

5. Troubleshooting "False Positives"

- **Confidence Levels:** Most patterns have "Low," "Medium," and "High" confidence settings. If you get too many alerts, increase the required confidence level (e.g., "Only block if it looks like a Credit Card AND passes the Luhn checksum").
- **Context:** Use **Proximity Keywords**. Configure the rule to match an SSN only if the words "Social Security" or "SSN" appear within 20 characters of the number.[144]

⁂

CASB

Cloud Access Security Broker (CASB) is the "middleman" that secures the interaction between your users and cloud applications (SaaS). In the Palo Alto Networks ecosystem, this is rebranded as **"Next-Generation CASB"** (or SaaS Security) because it integrates directly into the SASE platform rather than requiring a separate proxy appliance.

1. Two Primary Modes of Operation

To secure the cloud effectively, you need both "Inline" and "API" modes. They solve different problems.

Mode	Deployment	Use Case	The "Metaphor"
SaaS Security Inline	**The Firewall.** Traffic passes *through* the NGFW or Prisma Access on its way to the cloud.	**Shadow IT Discovery & Access Control.** "Stop users from uploading to Personal Dropbox." "Block known bad SaaS apps."	The **Gatekeeper**. Stops bad things from entering or leaving the building.
SaaS Security API	**The Cloud Scanner.** Connects directly to the SaaS provider (e.g., Box, Slack, Office 365) via API.	**Data at Rest & Collaboration.** "Find a Credit Card file stored in OneDrive last year." "Stop a user from sharing a folder with `gmail.com` users."	The **Auditor**. Walks around the building at night checking if file cabinets are locked.

2. Core Features (Next-Gen CASB)

Legacy CASBs were complex proxies. The "Next-Gen" approach leverages the existing firewall footprint.

- **Shadow IT Discovery:**
  - **Problem:** Employees use unsanctioned apps (e.g., "PDF Converter Online") that steal data.
  - **Solution:** The firewall analyzes traffic logs to generate a **SaaS Risk Report**. It assigns a risk score (1-5) to thousands of apps based on their certifications (SOC2, encryption usage).[159] [160]
- **Data Loss Prevention (DLP):**
  - **Integration:** Uses the **Enterprise DLP** engine (discussed previously) to scan files.

    - **Action:** If a user tries to upload a sensitive file to an unsanctioned app, the Inline CASB blocks the upload immediately.[161]
- **Misconfiguration Management (SSPM):**
    - **Feature:** SaaS Security Posture Management.
    - **Function:** Checks your SaaS apps for dangerous settings (e.g., "MFA is disabled for Admins in Salesforce" or "Zoom meetings allow anonymous guests").[162]

3. Implementation Workflow

1. **Activate:** Enable the SaaS Security subscription on your NGFW or Prisma Access.
2. **Discover:** Run the **Shadow IT Report** (Monitor > PDF Reports > SaaS Risk). You will likely find 100+ apps you didn't know about.
3. **Sanction:** Tag legitimate business apps (e.g., Office 365, Slack) as **Sanctioned**.
4. **Block:** Create a Policy Recommendation to block "High Risk" (Score 4-5) or "Unsanctioned" apps.
5. **Connect APIs:** For your Sanctioned apps (Office 365), authorize the **SaaS Security API** scanner to crawl your data for exposure risks (e.g., files shared with "Public Link").[160]

4. Summary Checklist

Function	CASB Component	Why you need it
Control Uploads	**Inline (NGFW)**	Prevents data exfiltration in real-time.
Clean up Old Data	**API (Cloud)**	Finds sensitive files uploaded *before* you bought the firewall.
Fix Settings	**SSPM**	Ensures your Salesforce/Slack isn't wide open to the internet.
Identify Apps	**Risk Report**	Shows you what "Shadow IT" apps your employees are actually using.

⁂

SaaS security

SaaS Security in the Palo Alto Networks portfolio is not just a reporting tool; it’s an active enforcement layer designed to close the "Shadow IT" gap. In 2026, the configuration is unified under **Strata Cloud Manager (SCM)**, allowing you to manage both "Inline" (Traffic) and "API" (Data) security from one dashboard.

1. The Two Pillars of SaaS Security

You must configure these separately, as they secure different vectors.

Feature	Vector	How it Works	Example Use Case
SaaS Security Inline	**Network Traffic**	Uses App-ID + ACE (App-ID Cloud Engine) to identify new apps instantly without waiting for a PAN-OS content update [169].	Blocking an employee from uploading a file to `mega.nz` (Unsanctioned App).
SaaS Security API	**Data at Rest**	Connects to the cloud provider (e.g., Slack, Box) via OAuth to scan files stored on their servers [170] [171].	Finding a spreadsheet labeled "Q4 Revenue" stored in a Public Google Drive folder and revoking the link.

2. Configuration: SaaS Security Inline (The "Gatekeeper")

This is now configured via **Policy Recommendations** rather than manually writing Regex.[172] [173]

1. **Discovery:**
    - Ensure your firewall is forwarding **Traffic Logs** to Strata Logging Service (Cortex Data Lake).
    - Navigate to **SaaS Security > Discovered Apps**. You will see a list of all apps used, rated by Risk Score (1-5).
2. **Authoring Recommendations:**
    - Select a high-risk app (e.g., "Personal Dropbox").
    - Click **"Create Policy Recommendation"**.
    - **Granularity:** Choose **Tenant-Level** if you want to block `personal@dropbox.com` but allow `corp@dropbox.com`. *Note: This requires SSL Decryption.*[173]
3. **Enforcement:**
    - Push the recommendation. It appears on the Firewall/Panorama as a **Security Policy Rule** (often tagged so you know it came from the SaaS engine).
    - **Action:** Block or Read-Only (allows downloading but prevents uploading).

3. Configuration: SaaS Security API (The "Auditor")

This setup is purely cloud-to-cloud and does not involve the physical firewall.[174] [170]

1. **Authentication:**
    - Log in to **Strata Cloud Manager > SaaS Security API**.
    - **Add Cloud App:** Select the provider (e.g., Microsoft 365, Salesforce).
    - **OAuth Grant:** You will be redirected to the Microsoft/Salesforce login page. Sign in with a **Global Admin** account to grant Palo Alto Networks permission to scan the tenant.
2. **Scan Configuration:**

    - **Asset Discovery:** Enable scanning for Files, Folders, and User Activities.
    - **DLP Integration:** Select the **Enterprise DLP** profile (e.g., "PII & Financial") you want to apply to this scan.
3. **Remediation:**
    - Define what happens when a violation is found.
    - *Auto-Remediation:* "Remove Public Link" or "Quarantine File."

4. Key 2026 Feature: App-ID Cloud Engine (ACE)

In the past, if a new SaaS app appeared, you had to wait for Palo Alto to release a content update (App-ID) to block it.

- **Now: ACE** performs real-time traffic analysis. If it sees traffic to a new "AI Chatbot" app, it can classify it and enforce policy *immediately* without a content update download.[169] [175]

5. Summary Checklist

Goal	Tool to Configure	Prerequisite
Block "Shadow IT" Apps	**SaaS Security Inline**	Log Forwarding to Cloud + SSL Decryption.
Separate Corporate vs. Personal Gmail	**SaaS Security Inline (Tenant Control)**	HTTP Header Insertion (or Tenant Policy) + SSL Decryption.
Find Sensitive Data in OneDrive	**SaaS Security API**	Global Admin credentials for the SaaS Tenant.
Fix "Open" Permissions in Salesforce	**SSPM (Posture Management)**	SaaS Security API connection [176].

⁂

PAN-OS SD-WAN

PAN-OS SD-WAN is a feature set built directly into the firewall's operating system, allowing you to use the firewall itself as an SD-WAN edge device. This differs from "Prisma SD-WAN" (formerly CloudGenix), which is a separate, dedicated appliance line.

1. Core Architecture: "Everything is an Interface"

The PAN-OS implementation abstracts multiple physical links (cable, fiber, LTE) into a single logical **SD-WAN Interface**.

- **The Virtual Interface:** Traffic routes to this single interface (e.g., `sdwan.1`).
- **The Physical Member:** The firewall decides which underlying physical link (e.g., `eth1/1` vs `eth1/2`) to use for each packet based on real-time performance metrics.[184] [185]

2. Path Quality Profiles (The "Health Check")

You don't just "fail over" when a cable is cut; you fail over when the application experience degrades.

- **Metrics:** The firewall measures **Latency, Jitter, and Packet Loss** continuously (every 200ms by default).[186]
- **Thresholds:** You create a profile (e.g., "Voice-Quality") with strict limits (e.g., Jitter < 30ms).
- **Action:** If the primary link exceeds 30ms jitter, the firewall seamlessly moves the VoIP call to the secondary link *without dropping the session*.[187]

3. Traffic Distribution Profiles (The "Decision Maker")

This determines *how* the firewall selects a link when multiple links are healthy.[188] [189]

- **Best Available Path:** Pick the link with the absolute best metrics (lowest latency) for every session. Used for sensitive apps.
- **Top-Down Priority:** "Always use Link A. Only use Link B if Link A is broken/degraded." Used for primary/backup scenarios (e.g., Fiber vs. expensive 5G).
- **Weighted Session Distribution:** "Send 70% of traffic to Fiber and 30% to Cable." Used for aggregate bandwidth.

4. PAN-OS SD-WAN vs. Prisma SD-WAN

This is a critical distinction for 2026 exams and architecture.

Feature	PAN-OS SD-WAN	Prisma SD-WAN (CloudGenix)
Hardware	Runs on **PA-Series** Firewalls.	Runs on **ION** Appliances.
Layer	**Layer 3 (Packet-Based).** Focuses on IP/Port and App-ID.	**Layer 7 (App-Defined).** Focuses purely on "App-SLA."
Security	**Native NGFW.** Full security (Threat, URL, WildFire) on-box.	**Lightweight.** Typically relies on Prisma Access (Cloud) for heavy security inspection [190] [191].
Best For...	Branches that need a **strong on-premise firewall** + basic SD-WAN.	Branches that are **Cloud-First** (SaaS heavy) and want the best possible app steering.

5. Implementation Workflow (PAN-OS)

1. **Interfaces:** Configure physical interfaces (e.g., `ethernet1/1` as "SD-WAN" type).
2. **Profile:** Create an **SD-WAN Interface Profile** to group these links (e.g., "Link Bundle").
3. **Monitor:** Attach a **Path Quality Profile** to define "What is a bad link?".
4. **Route:** In your Virtual Router, create a static route pointing to the logical `sdwan.1` interface.
5. **Policy:** Create an **SD-WAN Policy Rule** (separate from Security Policy) to map "Zoom Traffic" → "Voice-Distribution-Profile".[192]

Premium GlobalProtect

"Premium" GlobalProtect refers to the licensed GlobalProtect Gateway subscription (often abbreviated as the **GP License**). While a basic version of GlobalProtect comes free with every firewall, the "Premium" features unlock the advanced capabilities required for a Zero Trust or highly secure mobile workforce architecture.

1. Free vs. Licensed ("Premium") GlobalProtect

The distinction is critical for architecture and billing.

Feature	**Free (Standard)**	**Premium (Licensed)**
Supported OS	Windows, macOS.	**All OS** (iOS, Android, Linux, ChromeOS).
User Authentication	Basic (LDAP, RADIUS).	**Advanced** (SAML, MFA, Client Certificates).
Host Checking (HIP)	**No.** (Firewall cannot check if AV is running).	**Yes.** (Firewall scans the endpoint for Disk Encryption, Patch Level, AV status).
Connection Method	User-Initiated (Manual Connect).	**Always-On** (Connects automatically before login).
Split Tunneling	Basic (Route-based).	**Advanced** (App-Based, Domain-Based).
IPv6	No.	**Yes.**
Clientless VPN	No.	**Yes.** (Web-based portal for contractors).

2. Key Premium Feature: HIP (Host Information Profile)

This is the "Killer App" of the subscription. It turns the VPN into a Conditional Access system.

- **Concept:** The GlobalProtect agent scans the laptop and sends a "Report" (XML) to the firewall.
- **Policy Use:** You can write a Security Policy rule: *"Allow access to the HR Server ONLY IF the user is 'HR-Group' AND their laptop has BitLocker enabled AND Antivirus is updated."*
- **New in 2026 (Host Compliance Service - HCS):** HIP checks are now increasingly offloaded to the cloud (HCS) to reduce load on the firewall CPU and share compliance state across multiple gateways.[199]

3. Key Premium Feature: Mobile Support

Without the license, mobile devices (iPhones, Androids, iPads) **cannot** connect to the gateway.

- **Use Case:** MDM (Mobile Device Management) integrations. You can push a GlobalProtect profile via Intune/Jamf that forces an "Always-On" VPN for corporate iPads, ensuring traffic is always inspected.

4. Clientless VPN

This allows users to access internal web apps *without* installing the agent software.

- **How it works:** The user logs into a web portal (`https://vpn.company.com`). The firewall acts as a reverse proxy, rewriting internal links so they work through the browser.
- **Limitation:** It only works well for web applications (HTTP/HTTPS). It does not support thick clients (RDP, SSH) natively without HTML5 gateways.

5. Licensing Model

- **Per Device:** You buy a license for the *Firewall* (e.g., "GlobalProtect Subscription for PA-3410"). This covers *all* users connecting to that specific box.[200]
- **Prisma Access:** If you use Prisma Access (SASE), the GlobalProtect "Premium" features are inherently included in the user license, as the cloud service acts as the gateway.

Summary

You need the **Premium Subscription** if you answer "Yes" to any of these:

1. Do you need to support **iPhones/Androids**?
2. Do you need **Host Checking** (HIP) to block infected/unpatched laptops?
3. Do you need **Always-On** VPN (seamless connectivity)?
4. Do you need **Clientless** access for 3rd party contractors?

⁂

Advanced wildfire

Advanced WildFire is the evolution of the standard WildFire sandboxing service, designed specifically to stop "evasive" malware that knows it is being watched. It was introduced with PAN-OS 11.0 (Nova) and has become the standard premium offering in 2026.

1. Standard WildFire vs. Advanced WildFire

The core difference is *how* it analyzes files.

Feature	**Standard WildFire**	**Advanced WildFire**
Analysis Method	**Static + Dynamic Sandbox.** Runs the file in a VM (Windows/Android) and watches what it does (e.g., "Did it change a registry key?").	**Intelligent Run-Time Memory Analysis.** Looks directly into the RAM of the sandbox VM to see code execution that doesn't leave traces on the disk [209].
Evasion Resistance	Good against standard malware. Vulnerable to "Sandbox Aware" malware that goes to sleep if it detects a VM.	**Hypervisor-Level Stealth.** Uses a custom bare-metal hypervisor that is invisible to the malware.

Feature	**Standard WildFire**	**Advanced WildFire**
Inline Blocking	**Limited.** Relies on signatures generated *after* the first patient (patient zero) is infected (approx. 5-minute delay).	**Inline Cloud Analysis.** Uses Deep Learning models in the cloud to block unknown C2 and malware *in real-time* before the file transfer completes [210].
Dependencies	Analyzes the file "as is."	**Dependency Emulation.** If a malware file needs a specific DLL (e.g., `msvcr100.dll`) to run, Advanced WildFire automatically fetches it to force the malware to detonate [211].

2. Key Feature: Intelligent Run-Time Memory Analysis

This is the "secret sauce" of the Advanced license.

- **Problem:** Modern malware is "fileless" or uses "packing" to hide its code. It only unpacks the malicious payload in RAM for a split second before executing.
- **Solution:** Advanced WildFire takes snapshots of the RAM *during execution*. It sees the unpacked payload in memory, even if the file on disk looks encrypted and harmless.[212]
- **Configuration:** Zero-touch. If you have the license, this happens automatically in the cloud. You just see "Advanced WildFire" as a new category in your analysis reports.[213]

3. Key Feature: Inline Cloud Analysis (ICA)

This features moves "Verdict" capability from post-process to real-time.

- **How it works:** When a user downloads a file (e.g., a PDF), the firewall holds the last few packets. It sends the file's metadata and snippets to the Advanced WildFire cloud. The cloud uses ML models to give a "Likely Benign" or "Likely Malicious" verdict in milliseconds.
- **Result:** You can block "Patient Zero" without waiting 5 minutes for a full sandbox run.
- **Configuration:** You must explicitly enable **"Inline Cloud Analysis"** in your **WildFire Analysis Profile**.[210]

4. Implementation Steps

1. **License:** Ensure the **Advanced WildFire** license is active.
2. **Profile:** Create a **WildFire Analysis Profile**.
    - **Rules:** Set "Any/Any" to Forward.
    - **Inline:** Go to the "Inline Cloud Analysis" tab and check "Enable."
    - **Action:** Set the action to **Block** (or Reset-both) for "Malware".[210]
3. **Policy:** Attach this profile to your Security Policy rules (e.g., "Internet-Access").
4. **Decryption:** As always, SSL Decryption is mandatory. You cannot analyze encrypted files.

⁂

"Verdict" capability

Advanced WildFire's "Verdict" capability is the final decision rendered by the cloud analysis engine after inspecting a file. It determines whether a file is safe or malicious and triggers the corresponding enforcement action.

1. Types of Verdicts (The "Tags")

When Advanced WildFire inspects a file, it assigns one of four primary verdicts:

1. **Benign:** The file is safe. No action is taken, and the file is allowed to pass.
2. **Malware:** The file is confirmed malicious (e.g., virus, worm, ransomware).
   - **Action:** The firewall blocks the file (if "Block" is set in the profile) and logs a Critical Threat event.[224]
3. **Grayware:** The file is technically not malware but is "unwanted" (e.g., adware, browser toolbars, intense tracking cookies).
   - **Action:** You can choose to "Block" or "Alert" separately from Malware.
4. **Phishing:** The file (or link) is designed to steal credentials.
   - **Action:** Blocked immediately.

2. Real-Time vs. Post-Analysis Verdicts

This distinction is crucial for understanding how "Advanced" WildFire improves security.

- **Standard WildFire (Post-Analysis):**
  - **Process:** The firewall allows the file to pass to the user (to avoid delaying business). *Simultaneously*, it uploads the file to the cloud.
  - **Delay:** 5 minutes later, the cloud says "Verdict: Malware."
  - **Result:** Patient Zero is infected. The firewall updates its signature list to block *future* downloads of that file.
- **Advanced WildFire (Real-Time / Inline):**
  - **Process:** The firewall holds the last few packets of the file transfer. It sends metadata to the **Inline Cloud Analysis** engine.
  - **Verdict:** The cloud returns a "Likely Malicious" verdict in milliseconds using Deep Learning (no sandbox wait time).
  - **Result:** The file transfer is terminated *before* the user receives the full file. Patient Zero is protected.[225] [226]

3. Verdict Changes & Updates

Verdicts are not static.

- **Re-Analysis:** WildFire frequently re-analyzes old files as detection logic improves.
- **Verdict Change:** A file previously marked "Benign" might be re-classified as "Malware" 2 days later.
- **Log Event:** The firewall generates a specific log entry: *"WildFire Verdict Changed for file X from Benign to Malware."* This is your trigger for Incident Response to hunt down the device that downloaded file X two days ago.[227]

4. Private Cloud Exception

If you use a **WF-500** (On-Premise WildFire Appliance) or Private Cloud:

- Your verdicts are generated locally.
- However, the appliance can now check the **Global Cloud** for known verdicts first (Hybrid mode). If the Global Cloud knows the file is malware, the local appliance accepts that verdict instantly instead of wasting resources sandboxing it locally.[227]

Summary: What does the Verdict do?

The verdict is the **trigger**.

- **Benign** → Allow & Log (Optional).
- **Malware** → Reset Connection + Generate Threat Log + Generate Signature (for future blocking).
- **Grayware** → Alert or Block (Policy dependent).

⁂

Advanced Threat Prevention

Advanced Threat Prevention (ATP) is the IPS (Intrusion Prevention System) component of the Palo Alto Networks firewall. Unlike "Advanced WildFire" (which focuses on file analysis), ATP focuses on the *traffic stream* itself, looking for exploits, command-and-control (C2) patterns, and known malicious packets.[236]

1. Standard Threat Prevention vs. Advanced

The "Advanced" modifier was added to signify the shift to **Inline Deep Learning**.

Feature	**Standard Threat Prevention**	**Advanced Threat Prevention (ATP)**
Mechanism	**Signature-Based.** Matches traffic against a static database of known bad patterns (Snort-style rules).	**Inline Cloud Analysis.** Uses Deep Learning models to inspect traffic in real-time for *unknown* C2 and zero-day exploits [237].

Feature	**Standard Threat Prevention**	**Advanced Threat Prevention (ATP)**
Update Interval	**Daily/Hourly.** You must download a "Content Update" package to get new signatures.	**Real-Time.** The firewall queries the ATP cloud instantly. No update download required for zero-day protection.
Scope	Known Exploits (CVEs), Spyware, Vulnerabilities.	**Unknown C2,** SQL Injection, Command Injection, and DNS Exfiltration [237].
Local Deep Learning	Not available.	**Yes.** (New in PAN-OS 11.2+) Performs fast, on-box deep learning analysis for evasive threats without needing to query the cloud for every packet [236].

2. Key Components

ATP bundles three distinct security profiles into one license:[236]

1. **Antivirus:** Detects malware downloads via stream signatures (distinct from WildFire).
2. **Anti-Spyware:** Detects infected hosts calling home to C2 servers. Includes **DNS Security** integration.
3. **Vulnerability Protection:** Detects attempts to exploit bugs in your servers (e.g., Log4j, SQLi) or clients (e.g., Browser exploits).

3. New Features in 2026 (Exfiltration Shield)

As of early 2026, ATP includes **Exfiltration Shield**, a feature designed to stop data theft via covert channels.[237]

- **DNS Relaying Attacks:** Detects attackers tunneling data out through legitimate web services by hiding payloads in HTTP headers (Host, X-Forwarded-For).
- **Mechanism:** Uses ML models to inspect the sequence and randomness of header fields in real-time.

4. Configuration Best Practice

- **Enable Inline Cloud Analysis:** In your **Anti-Spyware** and **Vulnerability Protection** profiles, ensure the "Inline Cloud Analysis" box is checked. This activates the connection to the deep learning engine.
- **Action:** Set the action to **Reset-both** (TCP) or **Drop** (UDP). "Alert" is useless for prevention because the packet has already reached the target by the time the log is written.

Summary: ATP vs. WildFire

- **ATP:** Stops the **hacker** (Exploits, C2, SQL Injection).
- **WildFire:** Stops the **file** (Malware, Ransomware exe).

⁂

Advanced URL Filetering

Advanced URL Filtering (AURL) is the "Next-Gen" replacement for the legacy PAN-DB URL Filtering subscription. While the legacy version relied on a static database download (updated every 5 minutes), AURL adds a **real-time Inline Cloud Analysis** engine to stop "Patient Zero" phishing and web attacks.

1. The Core Innovation: Inline Deep Learning

Legacy URL Filtering fails when a hacker spins up a *new* phishing site (e.g., `apple-support-login-x9z.com`).

- **Legacy Process:** User clicks → Firewall checks DB → DB says "Unknown" → User Allowed. (Patient Zero infected).
- **AURL Process:** User clicks → Firewall checks DB → DB says "Unknown" → **Firewall pauses traffic** → Sends URL + Content to AURL Cloud → Deep Learning Analysis → Verdict: "Phishing" → **Block.**[245] [246]
- **Speed:** This analysis happens in milliseconds, often stopping the page from loading "halfway through" as the firewall receives the block verdict.[247]

2. What it Detects (Beyond Categories)

AURL doesn't just look at the domain name; it inspects the **page content** in real-time.[248]

- **Phishing Kits:** Detects cloned login pages (e.g., a fake Microsoft 365 login page) even on a "clean" domain like `sharepoint-internal.com`.
- **Obfuscated JavaScript:** Detects malicious scripts hidden inside innocent-looking HTML to evade traditional scanners.
- **Cloaked URLs:** Identifies when a site shows innocent content to a crawler (Google Bot) but malicious content to a real user (User-Agent cloaking).
- **AI-Generated Threats:** New in 2025/2026, it uses Generative AI models to detect text and images created by AI for social engineering.[249]

3. Anti-Evasion Capabilities

AURL is designed to beat modern phishing tactics:

- **Phishing Redirection Chains:** It follows the "hop" from the email link → bit.ly → landing page → final payload, analyzing the *final* destination.[248]
- **Fake CAPTCHA:** Detects when a phishing site asks a user to "Verify you are human" to hide the login form from automated crawlers.

4. Configuration Best Practice

- **Real-Time Detection Category:** In your URL Filtering Profile, you will see a category called **"Real-time Detection"**.
    - **Action:** Set this to **Block**. If you leave it as "Alert," you are turning off the primary protection engine.[250]
- **Credential Phishing:** Enable **"User Credential Submission"** protection.
    - **Mode:** "Block" submission of corporate credentials to any category *except* "Sanctioned-IT." This stops users from typing their AD password into a fake Google Docs form, even if the URL isn't known to be bad yet.[245]

Summary: Legacy vs. Advanced

- **Legacy:** "Is this URL on the Blacklist?" (Good for known bad sites).
- **Advanced:** "Does this page *look* like a phishing site?" (Good for zero-day attacks).

⁂

advanced dns

Advanced DNS Security (ADNS) is a cloud-native evolution of the standard DNS Security service, designed to address threats that target the DNS infrastructure itself, such as DNS Hijacking and "Dangling DNS" (Subdomain Takeovers). It became widely prominent with PAN-OS 11.0+.

1. Standard vs. Advanced: The Core Difference

While standard DNS Security protects users from visiting bad *names* (e.g., `evil.com`), ADNS protects against manipulated *answers* and infrastructure attacks.

Feature	**DNS Security (Standard)**	**Advanced DNS Security (ADNS)**
Primary Goal	**Sinkhole Malware.** Stops users from resolving domains used for C2 or Malware distribution.	**Stop Hijacking.** Detects when a legitimate domain (e.g., `gmail.com`) returns a manipulated IP address due to a compromised upstream DNS server [260].
Analysis Scope	**Query Analysis.** Looks at the domain name requested (DGA detection).	**Response Analysis.** Looks at the IP/Record returned by the server. If `google.com` suddenly resolves to a known malicious IP in Russia, ADNS blocks it [261].
Threats Covered	DGA, DNS Tunneling, Malware Domains.	**DNS Hijacking, Misconfigured Domains, Subdomain Takeovers** [261].
Dangling DNS	No.	**Yes.** Detects "dangling" CNAME records pointing to abandoned cloud resources (e.g., an old AWS S3 bucket) that attackers can claim to hijack the subdomain [262] [263].

2. How "Response Analysis" Works

This is the key innovation.

- **Scenario:** An attacker poisons the cache of your ISP's DNS server. When your user asks for `bank.com`, the ISP returns the attacker's IP.
- **Standard Firewall:** Sees the user asked for `bank.com` (Good Domain) and allows it.
- **Advanced DNS Firewall:** Inspects the *Answer*. It sees the IP belongs to a known bulletproof hosting provider, not the bank's ASN. It calculates a "hijack probability" in real-time and blocks the response.[261]

3. New Features 2025/2026

- **Encrypted DNS Analysis:** ADNS now natively inspects **DNS over HTTPS (DoH)** traffic without needing complex SSL decryption rules, provided the firewall acts as the DoH proxy or is configured for DoH inspection.[264]
- **Custom FQDN Actions:** You can now create custom lists that support "Sinkhole" actions directly, rather than just Allow/Block.[264]

4. Configuration Steps

1. **License:** Verify "Advanced DNS Security" is active.
2. **Profile:** Open your **Anti-Spyware Profile**.
3. **DNS Policies:**
    - You will see new categories: **"DNS Misconfiguration Domains"** and **"Hijacked Domains."**
    - **Action:** Set these to **Block** (Sinkhole is often not necessary for hijacks; a simple block protects the user).
4. **Logging:** Ensure "Log at Session End" is enabled. You will see specific "DNS Security" logs detailing the hijack attempt.[264]

Summary Checklist

Use **Advanced DNS Security** if you are worried about:

- **Supply Chain Attacks** (Compromised Upstream DNS).
- **Subdomain Takeovers** (Orphaned cloud resources).
- **Nation-State Hijacking** (Man-in-the-Middle DNS redirection).

⁂

]aligning AIOps to Palo Alto Network Best Practices

AIOps for NGFW (and SCM) is the modern mechanism for enforcing "Best Practices." It replaces the manual "Best Practice Assessment (BPA)" spreadsheet process with an automated, closed-loop system that can fix issues for you.

1. The Core Shift: From "Reporting" to "Remediation"

Previously, you ran a BPA report, got a list of 500 failures, and manually fixed them.

- **AIOps Approach:** The system runs the BPA continuously (every 24 hours).
- **BPA+ (Plus):** AIOps not only identifies the failure but provides a **"Fix It" button**. Clicking this generates the exact CLI commands or XML snippet required to bring the configuration into compliance, which you can push directly to the device.[275] [276]

2. Implementation Workflow

1. **Activate AIOps:**
    - **Free Version:** Available to everyone. Upload a Tech Support File (TSF) manually to get a snapshot report.
    - **Premium:** Requires a license. Connects to the firewall/Panorama via telemetry for real-time, continuous monitoring.[277]
2. **Review the Dashboard:**
    - Navigate to **Strata Cloud Manager > AIOps**.
    - Check the **"Best Practice Assessment"** widget. It groups failures by "Security," "Decryption," "High Availability," etc.
3. **Remediate:**
    - Filter for **"Remediable"** failures (green checkmark).
    - Select a failure (e.g., "Anti-Spyware Profile is set to Alert").
    - Click **"Remediate"**. AIOps will propose the change (e.g., "Set Action to Reset-both").
    - **Commit:** Review the generated config and push it to the device.[278] [276]

3. Policy Analyzer & Optimization

AIOps goes beyond static settings; it analyzes *logic*.

- **Policy Analyzer:** Before you push a rule, AIOps checks if it shadows an existing rule or violates a best practice (e.g., "You are allowing 'Any' application on port 443"). It can block the commit if the rule is too dangerous.[278]
- **Policy Optimizer:** Identifies "Overly Permissive" rules.
    - *Scenario:* You have a rule allowing "Any" app to the Internet.

  - *Action:* AIOps watches the traffic for 30 days. It then says: "Actually, only `ssl` and `web-browsing` were used. Should I rewrite the rule to allow only these two?".[279]

4. Summary Checklist

Goal	Tool in AIOps	Action
Fix Config Settings	**BPA+**	Use the "Remediate" button to apply standard snippets.
Clean Up Rules	**Policy Analyzer**	Check for shadowed or redundant rules before committing.
Tighten Security	**Policy Optimizer**	Convert "Any/Any" rules into App-ID specific rules based on real traffic.
Prevent Mistakes	**Proactive Checks**	Configure Panorama to *reject* commits that fail critical BPA checks (e.g., "No unencrypted Management") [278].

Closing Summary

You have a comprehensive toolkit at your disposal.

1. **Architecture:** Use **Strata Cloud Manager** as your unified view.
2. **Traffic Control:** Use **App-ID** and **User-ID** to reduce the attack surface.
3. **Threat Prevention:** Layer **Advanced WildFire** (Files), **ATP** (Exploits), **Advanced URL** (Phishing), and **Advanced DNS** (Hijacking) for complete coverage.
4. **Encryption: SSL Decryption** is the prerequisite for *all* the above tools to work effectively.
5. **Validation:** Use **AIOps** to continuously check your work against the "Gold Standard" best practices.

⁂

Administration of AIOps

AIOps for NGFW administration is designed to be "set and forget" for data collection, while providing active "Push" notifications for issues. The system runs on the Palo Alto Networks cloud (Hub), meaning you don't install a local server—you just point your firewalls to it.

1. The Core Requirement: Telemetry

AIOps relies entirely on **Device Telemetry**.[290] [291]

- **What is it?** A background process on the firewall that bundles metrics (CPU, Session usage, Interface errors) and configuration snapshots.
- **Configuration:**
  - Go to **Device > Setup > Telemetry**.
  - **Enable Telemetry:** Check the box.

  - **Region:** Select your data residency region (e.g., "Americas").
  - **Certificate:** The firewall needs a valid Device Certificate (OTP) to authenticate to the cloud.[291]
- **New in 2026:** Telemetry is now "Auto-Enabled" on new devices upon onboarding to Strata Cloud Manager (SCM), removing the manual setup step.[290]

2. Alerts vs. Incidents

Understanding the difference is key to avoiding "Alert Fatigue."

Component	Definition	Example
Event	A single raw data point indicating a change.	"CPU spiked to 85% at 2:00 PM."
Alert	A specific problem detected by analyzing events.	"High CPU detected on Data Plane."
Incident	A **correlated** group of alerts that tell a story.	"Application Latency Incident: Caused by High CPU (Alert A) which started after Commit X (Event B)."

- **Admin Task:** You should configure notifications for **Incidents**, not raw Alerts. This reduces noise by 90%.[292] [293]

3. Predictive Analytics (The "Crystal Ball")

AIOps doesn't just report what happened; it predicts what *will* happen.

- **Capacity Planning:** The dashboard will show a "Days to Exhaustion" counter.
  - *Example:* "Based on current trends, your Session Table will be full in 14 days."
- **Admin Action:** Use this data to order hardware upgrades or enable aggressive session aging *before* the crash occurs.[294]

4. Role-Based Access (RBAC)

You don't want every junior admin clicking "Remediate."

- **App Administrator:** Full access to onboard devices and change settings.
- **Viewer:** Can see reports and health status but cannot trigger remediation or change thresholds.
- **Management:** Administered via the **Palo Alto Networks Hub** (apps.paloaltonetworks.com), not on the local firewall.[295]

Summary Checklist

1. **Onboard:** Register the firewall in the Cloud Hub.
2. **Telemetry:** Ensure the "Green Light" in **Device > Setup > Telemetry**.
3. **Notifications:** Configure email/webhook alerts for **"Critical Incidents"** only.

4. **Review:** Schedule a weekly review of the **"Predictive Health"** tab to catch hardware limits early.

⁂

dashboards

In the Palo Alto Networks ecosystem, **"Dashboards"** can refer to three distinct interfaces depending on whether you are looking at the local firewall, Panorama, or the modern **Strata Cloud Manager (SCM)**. Each serves a different operational role.

1. The Local Firewall / Panorama Dashboard

This is the "Landing Page" when you log in. It focuses on **System Health**.

- **Purpose:** "Is the box on fire?"
- **Key Widgets:**
  - **General Information:** Shows Hostname, Serial Number, PAN-OS Version, and *Application/Threat Content Versions* (Are signatures up to date?).[305]
  - **System Resources:** CPU (Data Plane vs. Management Plane) and Session Table usage.
  - **Interfaces:** Real-time Link State (Green/Red) for physical ports.
  - **High Availability:** Shows if the peer is Active/Passive or Suspended.
  - **Logged In Admins:** Shows who else is currently configuring the box.[305]

2. The ACC (Application Command Center)

This is the "Traffic Analysis" dashboard. It is distinct from the main system dashboard.

- **Purpose:** "Who is doing what?" and "Why is the internet slow?"
- **Key Tabs:**
  - **Network Activity:** Top Applications, Top Users, Top Source/Dest IPs.
  - **Threat Activity:** Top Threats, Top WildFire hits, Compromised Hosts.[306]
  - **Blocked Activity:** What is being denied and by which rule?
- **Interactivity:** The ACC is fully interactive. Clicking "Bittorrent" automatically filters all other widgets to show *only* users and threats related to Bittorrent.[306]

3. Strata Cloud Manager (SCM) Dashboards (2026)

SCM introduces a new layer of "Fleet Management" visualization that replaces the static Panorama views.

- **NetSec Health Dashboard:** A geographic map view of your entire deployment. It highlights "Unhealthy" sites (e.g., Device Down, Tunnel Down) in red, allowing global drill-down.[307]

- **Incident Dashboard:** Instead of raw logs, this shows correlated **Incidents** (e.g., "High CPU caused by Commit").
- **Threat Insights:** A holistic view of threats blocked across *all* vectors (DNS, URL, WildFire) in a single pane, rather than separate reports.[308]

4. Custom Dashboards

- **SCM:** Allows you to "Build My Dashboard" using a library of widgets (Bar charts, Line graphs) for specific KPIs (e.g., "SaaS Usage by Marketing Dept").[309] [310]
- **Local/Panorama:** You can add custom tabs to the ACC, but the main "Dashboard" tab is limited to a predefined set of system widgets.[311]

Summary: Which Dashboard When?

- **System Admin:** Uses **Local Dashboard** to check CPU/HA status.
- **Security Analyst:** Uses **ACC** or **SCM Threat Insights** to hunt threats and bandwidth hogs.
- **Manager/CISO:** Uses **SCM NetSec Health** or **Custom SCM Dashboards** for high-level fleet status.

⁂

Best Practice Assessment (BPA)

The **Best Practice Assessment (BPA)** is a critical auditing tool in the Palo Alto Networks ecosystem. As of 2026, the standalone BPA tool (Excel/HTML report) has been deprecated and fully integrated into **Strata Cloud Manager (SCM) / AIOps for NGFW**.

1. What is the BPA?

It is an automated "health check" that scans your configuration against 200+ industry-standard checks (NIST, CIS) and Palo Alto Networks vendor recommendations.[320]

- **Input:** Your firewall or Panorama configuration (Tech Support File - TSF).
- **Output:** A pass/fail score and a "Fix It" guide.

2. The "Heatmap": Visualizing Gaps

The most distinctive feature of the BPA is the **Adoption Heatmap**.[321] [322]

- **What it shows:** It's a color-coded matrix (Green/Red) mapping your **Security Zones** against **Security Profiles**.
- **Example Reading:**
  - **Row:** `Untrust-to-Trust` (Inbound Traffic).
  - **Column:** `Antivirus`.
  - **Cell Color: Red**.

    - **Meaning:** "You have a rule allowing traffic from the Internet to your Internal network, but you forgot to attach an Antivirus profile."
- **Goal:** Turn the matrix Green. It forces you to realize, "Oh, I have URL Filtering on my User traffic, but I forgot it on my Guest Wi-Fi."

3. How to Generate a Report (2026 Method)

Since the legacy portal is closed, you must use **AIOps**.[323] [324]

Method A: Continuous (Best Practice)

- **Prerequisite:** AIOps license + Telemetry enabled.
- **Process:** The BPA runs automatically every 24 hours. You log in to SCM and see the live status.

Method B: On-Demand (Free/Audit Mode)

- **Prerequisite:** AIOps Free Tier.
- **Process:**
    1. Go to **Strata Cloud Manager > AIOps**.
    2. Navigate to **Dashboards > On-Demand BPA**.
    3. Click **"Generate New BPA Report"**.
    4. Upload your **Tech Support File (TSF)** manually.
    5. Wait ~5 minutes for the report to generate.

4. Failed Checks: How to Fix?

The BPA doesn't just say "Failed"; it links to the remediation.

- **AIOps Premium:** Click the "Remediate" button to generate the CLI set commands automatically.
- **Manual:** The report provides a "Rationale" explaining *why* the setting is bad (e.g., "Disabling 'Require Client Certificate' on the Management Interface exposes you to brute force attacks").[325]

Summary Checklist

1. **Run BPA:** Before every major change window or audit.
2. **Check Heatmap:** Look for "Red Squares" in high-risk zones (Untrust).
3. **Prioritize:** Fix "Critical" failures first (e.g., Default Admin Password, Telnet enabled).
4. **Trend:** Use the "Trending" tab in AIOps to prove to management that your security posture is improving over time (e.g., "We went from 45% to 88% compliance in Q1").

⁂

1. https://www.linkedin.com/pulse/what-happened-palo-alto-networks-iron-skillet-config-best-joe-brunner-wmuqe
2. https://live.paloaltonetworks.com/t5/expedition-articles/important-update-end-of-life-announcement-for-palo-alto-networks/ta-p/589642
3. https://www.prnewswire.com/news-releases/palo-alto-networks-delivers-more-autonomous-cybersecurity-through-copilots-for-strata-prisma-and-cortex-platforms-302137998.html
4. https://www.reddit.com/r/paloaltonetworks/comments/1osdznp/please_help_me_decode_palo_altos_portfolio_strata/
5. https://www.paloaltonetworks.com/blog/2025/02/announcing-innovations-cortex-cloud/
6. https://datacipher.net/palo-alto-networks-certifications/
7. https://www.exam-labs.com/blog/navigating-the-palo-alto-networks-certification-path-a-strategic-guide
8. https://www.perplexity.ai/search/7015bedf-456c-41cf-995b-0534cc163018
9. https://cortex.marketplace.pan.dev/marketplace/details/PrismaAccess/
10. https://www.paloaltonetworks.com/blog/2025/12/partners-fueling-innovation-with-cortex-xsiam-and-prisma-sase/
11. https://live.paloaltonetworks.com/t5/expedition-articles/tkb-p/ExpeditionArticles/label-name/bpa
12. https://www.youtube.com/watch?v=gIERAMvGoWE
13. https://www.nwexam.com/blog/ultimate-guide-palo-alto-certification-path
14. https://metronlabs.com/palo-alto
15. https://live.paloaltonetworks.com/t5/expedition-articles/tkb-p/ExpeditionArticles
16. https://www.paloaltonetworks.com/resources/datasheets/palo-alto-networks-portfolio-platforms
17. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/nat/nat-policy-rules/nat-policy-overview
18. https://live.paloaltonetworks.com/t5/general-articles/nominated-discussion-precedence-of-routing-nat-policy/ta-p/526558
19. https://www.reddit.com/r/paloaltonetworks/comments/so38t8/policy_order/
20. https://kb.expedient.com/docs/creating-nat-policies
21. https://www.uninets.com/blog/palo-alto-static-nat-configuration
22. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/migrate-from-panorama-to-strata-cloud-manager
23. https://docs.paloaltonetworks.com/compatibility-matrix/reference/feature-parity
24. https://www.perplexity.ai/search/c650944e-d867-4c68-9119-63d10a155477
25. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-rules
26. https://www.reddit.com/r/networking/comments/2s65nf/assistance_with_palo_alto_interpretation_of_nat/
27. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/nat/nat-policy-rules
28. https://www.youtube.com/watch?v=8xKqHkKRn2w
29. https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/change-between-panorama-management-and-cloud-management
30. https://github.com/PaloAltoNetworks/panos-to-scm
31. https://docs.paloaltonetworks.com/network-security/security-policy/administration/all-policy-types/nat

32. https://www.youtube.com/watch?v=Ahrao6kBg8w
33. https://www.youtube.com/watch?v=HaZIF3H6xmc
34. https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-deployment-best-practices/advanced-wildfire-best-practices
35. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-dns-security
36. https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security
37. https://live.paloaltonetworks.com/t5/community-blogs/cloud-delivered-security-service-newsletter-november-2025/ba-p/1242603
38. https://docs.paloaltonetworks.com/saas-security/activation-and-onboarding/activate-saas-security-inline-ngfw
39. https://docs.paloaltonetworks.com/whats-new/new-features/february-2025/simplified-security-policy-recommendations-for-saas-security-inline
40. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles
41. https://datacipher.net/palo-alto-network-security-professional-certification-guide-2025/
42. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/security-services
43. https://www.youtube.com/watch?v=i_XDvTi-qsk
44. https://www.techtarget.com/searchsecurity/feature/How-to-set-up-Palo-Alto-security-profiles
45. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/cloud-delivered-security-services
46. https://docs.paloaltonetworks.com/saas-security/getting-started/whats-saas-security/whats-saas-security-inline
47. https://networkdevicesinc.com/community/blog/palo-alto-firewall-configuration-guide
48. https://www.linkedin.com/pulse/palo-alto-firewall3-app-id-user-id-acc-saeid-faraji
49. https://www.youtube.com/watch?v=d_F7jQqLdJQ
50. https://www.cbtnuggets.com/blog/technology/networking/how-to-configure-app-id-in-palo-alto-firewall
51. https://kb.wisc.edu/security/94783
52. https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/manage-the-cloud-identity-engine/cloud-identity-engine-user-context
53. https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/authenticate-users-with-the-cloud-identity-engine/configure-the-cloud-identity-engine-as-a-mapping-source-on-the-firewall
54. https://www.cbtnuggets.com/blog/technology/networking/configuring-user-id-in-palo-alto-firewall-a-guide
55. https://docs.paloaltonetworks.com/ngfw/administration/user-id
56. https://www.youtube.com/watch?v=QPD5z1rF9Hw
57. https://docs.paloaltonetworks.com/best-practices/10-1/user-id-best-practices
58. https://docs.paloaltonetworks.com/best-practices
59. https://studylib.net/doc/9983163/palo-alto-application-id-vs.-url-filtering-and-application

60. https://www.reddit.com/r/paloaltonetworks/comments/1ixsbsa/best_practices_for_managing_userid_on_palo_alto/
61. https://faatech.be/security-policies-best-practices-palo-alto-networks-next-gen-firewalls/
62. https://docs.paloaltonetworks.com/ngfw/administration/app-id/app-id-overview
63. https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices
64. https://www.cbtnuggets.com/blog/certifications/security/ssl-decryption-benefits-challenges-and-best-practices
65. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/configure-ssl-inbound-inspection
66. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/decryption-concepts/ssl-inbound-inspection
67. https://docs.paloaltonetworks.com/whats-new/new-features/may-2024/tlsv1-3-support-for-hsm-integration-inbound-inspection-decryption
68. https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices
69. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/decryption/decryption-exclusions
70. https://www.youtube.com/watch?v=tj-FJOBf2WE
71. https://www.reddit.com/r/paloaltonetworks/comments/1gev3bv/ssl_decryption_best_practice/
72. https://www.linkedin.com/pulse/palo-alto-tls-13-decryption-best-practice-block-traffic-joe-brunner-aurbe
73. https://docs.paloaltonetworks.com/network-security/decryption/administration/enabling-decryption/configure-ssl-inbound-inspection
74. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/troubleshoot-and-monitor-decryption
75. https://www.youtube.com/watch?v=tpQc5uAT3Mw
76. https://www.scribd.com/document/508145897/decryption-best-practices
77. https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment
78. https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices
79. https://docs.paloaltonetworks.com/ngfw/administration/certificate-management
80. https://www.wiresandwi.fi/blog/palo-alto-firewalls-basic-https-inspection-outbound-ca
81. https://www.youtube.com/watch?v=yUeP-6idTMM
82. https://www.reddit.com/r/paloaltonetworks/comments/gvy3jm/help_me_understand_trust_vs_untrust_certificates/
83. https://cordero.me/understanding-ssl-tls-decryption-with-palo-alto-firewalls-forward-trust-and-forward-untrust-certificates/
84. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/decryption/decryption-concepts/keys-and-certificates-for-decryption-policies
85. https://learn.microsoft.com/en-us/answers/questions/2236412/best-practices-for-pki-certification-authority-dur
86. https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/globalprotect-certificate-best-practices

87. https://www.scribd.com/document/772790193/Palo-Alto-Firewall-Certificate-Deployment
88. https://justus.ws/tech/paloalto-ca-cert/
89. https://www.encryptionconsulting.com/best-practice-ca-certificates-renewal/
90. https://www.reddit.com/r/paloaltonetworks/comments/lsx8a8/import_certificate_as_ca/
91. https://live.paloaltonetworks.com/t5/next-generation-firewall/best-practice-for-root-ca-self-signed-cert-on-ngfw/td-p/480538
92. https://www.wiresandwi.fi/blog/palo-alto-firewalls-basic-https-inspection-outbound-self
93. https://www.fortinet.com/resources/cyberglossary/public-key-infrastructure
94. https://en.wikipedia.org/wiki/Public_key_infrastructure
95. https://www.youtube.com/watch?v=yUeP-6idTMM
96. https://deadiversion.usdoj.gov/drugreg/csos/docs/CSOS-PublicKeyInfrastructureOverview.pdf
97. https://www.keyfactor.com/education-center/what-is-pki/
98. https://www.ibm.com/think/topics/public-key-infrastructure
99. https://www.okta.com/identity-101/public-key-infrastructure/
100. https://www.geeksforgeeks.org/computer-networks/public-key-infrastructure/
101. https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki
102. https://www.futurex.com/blog/what-is-a-pki
103. https://www.digicert.com/what-is-pki
104. https://docs.paloaltonetworks.com/strata-logging-service
105. https://live.paloaltonetworks.com/t5/community-blogs/cortex-data-lake-cdl-embraces-its-new-identity-as-strata-logging/ba-p/588991
106. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/monitor/monitor-logs/log-types
107. https://www.sdxcentral.com/news/palo-alto-networks-consolidates-network-security-and-sase-management/
108. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding
109. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/view-and-manage-logs/log-types-and-severity-levels
110. https://sourceforge.net/software/compare/Palo-Alto-Networks-Panorama-vs-Palo-Alto-Networks-Strata/
111. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/prisma-access-app-features
112. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/configure-log-forwarding
113. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/migrate-from-panorama-to-strata-cloud-manager
114. https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-release-notes/features-introduced-in-pan-os
115. https://cortex.marketplace.pan.dev/marketplace/details/CortexDataLake/
116. https://www.linkedin.com/pulse/when-strata-cloud-manager-scm-replace-panorama-complex-joe-brunner-bpyhe
117. https://docs.paloaltonetworks.com/compatibility-matrix/reference/feature-parity
118. https://www.reddit.com/r/paloaltonetworks/comments/1ntbnx8/panorama_vs_strata/

119. https://www.paloaltonetworks.lat/cyberpedia/what-is-iot-security
120. https://docs.paloaltonetworks.com/iot/getting-started/iot-security-solution/iot-security-solution-setup
121. https://www.micromindercs.com/blog/tap-vs-span-in-ot-environments
122. https://docs.paloaltonetworks.com/iot/iot-security-best-practices
123. https://docs.paloaltonetworks.com/content/techdocs/en_US/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/policy-recommendation-best-practices
124. https://pan.dev/splunk/docs/iot-security/
125. https://docs.paloaltonetworks.com/iot/iot-security-admin/recommend-security-policies/policy-rule-recommendations
126. https://klasresearch.com/report/healthcare-iot-security-2026-vendors-pushing-beyond-device-visibility-to-drive-measurable-outcomes/3313
127. https://industrialcyber.co/news/evaluating-network-taps-vs-span-in-ot-critical-infrastructure-environments/
128. https://aws.amazon.com/blogs/machine-learning/how-palo-alto-networks-enhanced-device-security-infra-log-analysis-with-amazon-bedrock/
129. https://www.youtube.com/watch?v=1wlbNbQMxkw
130. https://docs.paloaltonetworks.com/iot/administration/configure-iot-networks
131. https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security
132. https://www.paloaltonetworks.com/resources/videos/iot-security-by-palo-alto-networks
133. https://insights.profitap.com/tap-vs-span
134. https://docs.paloaltonetworks.com/ngfw/networking/configure-interfaces/tap-interfaces
135. https://www.paloaltonetworks.com/blog/2015/07/use-tap-mode-to-see-ics-scada-traffic-and-risks-more-clearly/
136. https://docs.paloaltonetworks.com/content/techdocs/en_US/iot/best-practices/deploy-iot-security-using-best-practices
137. https://go.ordr.net/rs/976-OJA-437/images/ordr_integration_guide_ordr_and_palo_alto_networks_integration_guide.pdf
138. https://docs.paloaltonetworks.com/ngfw/help/11-1/monitor/monitor-iot-devices
139. https://rdp21.org/wp-content/uploads/2020/11/ot-and-Iot-device-security-in-industrial-control-systems.pdf
140. https://www.reddit.com/r/networking/comments/4xfww6/palo_alto_vm_in_tap_mode_for_application/
141. https://www.youtube.com/watch?v=H5Ff-j31bEE
142. https://www.paloaltonetworks.com/resources/videos/iot-security-by-palo-alto-networks
143. https://xsoar.pan.dev/docs/reference/integrations/palo-alto-networks-io-t
144. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/configure-exact-data-matching
145. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/custom-document-types-for-enterprise-dlp/about-custom-document-types
146. https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/protect-home/about-dlp-indexes.html

147. https://docs.paloaltonetworks.com/content/techdocs/en_US/enterprise-dlp/administration/configure-enterprise-dlp
148. https://docs.paloaltonetworks.com/enterprise-dlp/activation-and-onboarding/enable-enterprise-dlp
149. https://docs.paloaltonetworks.com/prisma-access/activation-and-onboarding/your-prisma-access-license/all-available-apps-and-services/cheat-sheet-dlp-with-prisma-access
150. https://securitybrief.co.nz/story/palo-alto-networks-adds-sd-wan-and-dlp-capabilities-to-edge-networking-platform
151. https://www.nightfall.ai/blog/palo-alto-networks-dlp-comprehensive-analysis-and-top-alternatives
152. https://www.forcepoint.com/blog/insights/best-dlp-software
153. https://www.sdxcentral.com/news/palo-alto-networks-fights-data-breaches-with-dlp/
154. https://live.paloaltonetworks.com/t5/general-topics/does-palo-alto-plan-to-offer-on-prem-versions-of-the-dlp-ot/td-p/1244870
155. https://www.proofpoint.com/us/blog/information-protection/advanced-data-classification-dlp-edm-vs-idm
156. https://www.reddit.com/r/networking/comments/1qartz5/looking_for_solid_dlp_solutions_for_enterprise/
157. https://www.paloguard.com/Data-Loss-Prevention.asp
158. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-january-2026
159. https://www.paloaltonetworks.com/cyberpedia/what-is-a-casb-cloud-access-security-broker
160. https://www.netfriends.com/blog-posts/what-is-a-cloud-access-security-broker-casb
161. https://docs.paloaltonetworks.com/next-gen-casb
162. https://www.cyberhaven.com/guides/top-cloud-access-security-broker-casb-software-products-vendors-solutions
163. https://www.paloaltonetworks.com/cyberpedia/sase-vs-casb
164. https://secureitconsult.com/casb-explained/
165. https://www.paloaltonetworks.com/resources/videos/next-generation-casb-by-palo-alto-networks
166. https://www.miniorange.com/blog/top-cloud-access-security-broker-casb-tools/
167. https://www.prnewswire.com/news-releases/palo-alto-networks-expands-casb-offering-with-new-cloud-security-capabilities-300529575.html
168. https://www.csoonline.com/article/557365/cloud-access-security-broker-buyers-guide.html
169. https://docs.paloaltonetworks.com/saas-security/getting-started/get-started-with-saas-security-inline
170. https://www.youtube.com/watch?v=VWdnWxdMuxY
171. https://www.youtube.com/watch?v=J9Zu_bMekKU
172. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-saas-security
173. https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-inline/remediate-risks-saas-security-inline/manage-saas-security-inline-policy/create-saas-policy-rule-recommendations
174. https://docs.exabeam.com/en/cloud-connectors/all/configuration/129105-palo-alto-networks-saas-security-cloud-connector.html
175. https://docs.paloaltonetworks.com/content/techdocs/en_US/saas-security/release-notes/features-introduced-in-2026.html
176. https://docs.paloaltonetworks.com/saas-security/getting-started/get-started-with-sspm

177. https://docs.paloaltonetworks.com/content/techdocs/en_US/saas-security/release-notes/features-introduced-in-2026/january-2026.html
178. https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-inline/remediate-risks-saas-security-inline/manage-saas-security-inline-policy/saas-policy-rule-recommendations
179. https://www.reddit.com/r/SeaPower_NCMA/comments/1qgptfy/is_sar_possible_with_the_mission_editor/
180. https://www.reddit.com/r/sysadmin/comments/17ugew8/email_security_inlinemx_vs_api_what_do_you_prefer/
181. https://pan.dev
182. https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-api/get-started-with-saas-security-api
183. https://docs.paloaltonetworks.com/saas-security
184. https://docs.paloaltonetworks.com/sd-wan/activation-and-onboarding/plan-sd-wan-configuration
185. https://pan.dev/panos/docs/tutorials/redundant-internet/
186. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-sd-wan-link-management/objects-sd-wan-link-management-path-quality-profile
187. https://www.scribd.com/document/892938630/Pan-Os-Sd-Wan-Path-Selection-Primer
188. https://docs.paloaltonetworks.com/sd-wan/administration/enable-sd-wan-without-auto-vpn/manage-sd-wan-link-failovers/sd-wan-traffic-distribution-profiles
189. https://docs.paloaltonetworks.com/content/techdocs/en_US/sd-wan/administration/enable-sd-wan-without-auto-vpn/manage-sd-wan-link-failovers/define-path-selection-for-sd-wan-traffic
190. https://live.paloaltonetworks.com/t5/general-topics/prisma-sd-wan-vs-pan-os-sd-wan-focused-on-sase/td-p/528285
191. https://zpesystems.com/sd-wan-leaders-zs/
192. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000saXJCAY&lang=en_US
193. https://docs.paloaltonetworks.com/sd-wan/getting-started/initial-set-up-for-sd-wan
194. https://www.youtube.com/watch?v=ocRINJhsZ6M
195. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-sites/add-panos-as-prisma-sdwan-dc/configure-panos-as-prisma-sdwan-dc
196. https://github.com/PaloAltoNetworks/sdwan
197. https://www.reddit.com/r/paloaltonetworks/comments/1k9cma8/anyone_with_exp_in_panos_sdwan_without_panorama/
198. https://docs.paloaltonetworks.com/sd-wan/administration/enable-sd-wan-without-auto-vpn/manage-sd-wan-link-failovers/define-your-custom-sd-wan-application-thresholds
199. https://docs.paloaltonetworks.com/ngfw/release-notes/12-1/features-introduced-in-pan-os/globalprotect-features
200. https://www.firewalls.com/palo-alto-networks-pa-1410-globalprotect-subscription-5-years-60-months-term.html
201. https://docs.paloaltonetworks.com/whats-new/new-features/january-2026
202. https://www.redpacketsecurity.com/palo_alto_networks_security_advisories_cve-2025-4227-globalprotect-app-interception-in-endpoint-traffic-policyenforcement/
203. https://docs.paloaltonetworks.com/globalprotect
204. https://www.reddit.com/r/paloaltonetworks/comments/1mqa1r2/end_of_sale_for_global_protect/

205. https://docs.paloaltonetworks.com/globalprotect/administration
206. https://www.actual4test.com/discussions/Palo-Alto-Networks/exam-pcnse-topic-2-question-31-discussion-p1152236.html
207. https://www.trustradius.com/compare-products/fortinet-fortigate-vs-palo-alto-networks-prisma-access
208. https://www.instagram.com/p/DMu-WX3NRNQ/?hl=en
209. https://utm-shop.de/media/40/b8/6b/1744884956/advanced-wildfire.pdf
210. https://docs.paloaltonetworks.com/advanced-wildfire/administration/configure-advanced-wildfire-analysis/enable-advanced-wildfire-inline-cloud-analysis
211. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-release-notes/features-introduced-in-pan-os/wildfire-features
212. https://www.youtube.com/watch?v=bwZMto6QhBQ
213. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/wildfire-features/intelligent-run-time-memory-analysis
214. https://www.optiv.com/insights/discover/blog/natively-integrated-security-palo-alto-networks-ecosystems-cloud-delivered
215. https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/advanced-wildfire-inline-cloud-analysis
216. https://www.youtube.com/watch?v=HaZIF3H6xmc
217. https://www.tenable.com/audits/items/CIS_Palo_Alto_Firewall_11_Benchmark_v1.2.0_L1.audit:99062f524c57c6745f4dc249cad23305
218. https://underdefense.com/industry-pricings/palo-alto-networks-pricing-ultimate-guide-for-security-products/
219. https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/latest-wildfire-cloud-features/intelligent-run-time-memory-analysis
220. https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-subscription
221. https://www.paloaltonetworks.com/network-security/advanced-wildfire
222. https://www.paloguard.com/WildFire.asp
223. https://www.reddit.com/r/paloaltonetworks/comments/1khqwdi/license_question_does_advanced_threat_prevention/
224. https://utm-shop.de/media/40/b8/6b/1744884956/advanced-wildfire.pdf
225. https://docs.paloaltonetworks.com/advanced-wildfire/administration/configure-advanced-wildfire-analysis/enable-advanced-wildfire-inline-cloud-analysis
226. https://www.youtube.com/watch?v=bwZMto6QhBQ
227. https://docs.paloaltonetworks.com/wildfire/u-v/wildfire-whats-new/wildfire-features-in-panos-80/verdict-checks-with-the-wildfire-global-cloud
228. https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-overview/advanced-wildfire-concepts/verdicts
229. https://www.youtube.com/watch?v=W9NKsbc4I5Q
230. https://docs.paloaltonetworks.com/advanced-wildfire
231. https://www.paloguard.com/WildFire.asp

232. https://www.boll.ch/datasheets/WF_WildFire.pdf
233. https://www.westconcomstor.com/content/dam/wcgcom/pan-vip/wildfire.pdf
234. https://www.reddit.com/r/networking/comments/kb7zh3/is_palo_altos_wildfire_product_actually_worth_it/
235. https://www.paloaltonetworks.com/resources/videos/preventing-attacks-using-wildfire
236. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/about-advanced-threat-prevention
237. https://docs.paloaltonetworks.com/advanced-threat-prevention
238. https://www.paloaltonetworks.com/resources/videos/advanced-threat-prevention
239. https://docs.paloaltonetworks.com/whats-new/new-features/june-2023/advanced-threat-prevention-dashboard
240. https://www.firewalls.com/catalog/product/view/id/48868/s/palo-alto-networks-advanced-threat-prevention-subscription-for-device-in-an-ha-pair-year-1-pa-3410/category/2/
241. https://slashdot.org/software/comparison/Palo-Alto-Networks-Advanced-Threat-Protection-vs-Palo-Alto-Networks-Threat-Prevention/
242. https://slashdot.org/software/comparison/Palo-Alto-Networks-Advanced-Threat-Protection-vs-WildFire/
243. https://www.peerspot.com/products/comparisons/palo-alto-networks-advanced-threat-prevention_vs_palo-alto-networks-url-filtering-with-pan-db
244. https://www.cdw.com/product/palo-alto-networks-advanced-threat-prevention-subscription-license-1-yea/7028246
245. https://docs.paloaltonetworks.com/advanced-url-filtering
246. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-overview
247. https://www.reddit.com/r/paloaltonetworks/comments/rua5p3/pandb_url_filtering_vs_advanced_url_filtering/
248. https://www.cc.com.pl/pl/prods/paloaltonetworks/pdf/advanced-url-filtering.pdf
249. https://www.paloaltonetworks.com/network-security/advanced-url-filtering
250. https://live.paloaltonetworks.com/t5/community-blogs/ignite-amp-activate-outsmart-the-next-phishing-attack-with/ba-p/1241991
251. https://www.enbitcon.com/shop/palo-alto-networks/palo-alto-firewalls/licenses/palo-alto-pa-415-advanced-url-filtering-lizenz-pan-pa-415-advurl
252. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/how-url-filtering-works
253. https://www.peerspot.com/products/comparisons/palo-alto-networks-advanced-threat-prevention_vs_palo-alto-networks-url-filtering-with-pan-db
254. https://www.peerspot.com/products/comparisons/advanced-url-filtering-by-palo-alto_vs_prisma-access-by-palo-alto-networks
255. https://www.trustradius.com/products/palo-alto-networks-advanced-url-filtering/reviews
256. https://www.youtube.com/watch?v=mkLLrreu7po
257. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features
258. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-january-2026

259. https://www.firewalls.com/catalog/product/view/id/48879/s/palo-alto-networks-pa-3410-advanced-url-filtering-subscription-1-year-12-months-term-renewal/category/2/
260. https://www.paloaltonetworks.com/network-security/advanced-dns-security
261. https://docs.paloaltonetworks.com/whats-new/may-2024/advanced-dns-security
262. https://www.wiz.io/blog/wiz-introduces-dangling-domain-detection-to-help-you-prevent-subdomain-takeovers
263. https://www.crowdstrike.com/en-us/blog/4-steps-to-prevent-subdomain-takeovers/
264. https://docs.paloaltonetworks.com/dns-security
265. https://www.paloguard.com/DNS.asp
266. https://www.youtube.com/watch?v=c4oY2EgPkb4
267. https://www.pass4success.com/palo-alto-networks/discussions/exam-netsec-pro-topic-2-question-7-discussion
268. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-dns-security
269. https://www.peerspot.com/products/comparisons/infoblox-advanced-dns-protection_vs_palo-alto-networks-dns-security
270. https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover
271. https://live.paloaltonetworks.com/t5/advanced-dns-security/advanced-dns-security-vs-dns-security/td-p/589027
272. https://www.reddit.com/r/paloaltonetworks/comments/1ht9iek/which_licenses_do_we_need_to_have_to_be_effected/
273. https://www.youtube.com/watch?v=QewzjlxpYzM
274. https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-advanced-dns-security
275. https://live.paloaltonetworks.com/t5/community-blogs/bpa-transition-to-aiops-for-ngfw/ba-p/548612
276. https://www.linkedin.com/pulse/what-happened-palo-alto-networks-iron-skillet-config-best-joe-brunner-wmuqe
277. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/best-practices-in-ngfw
278. https://www.scribd.com/document/896583062/Strata-Cloud-Manager-AIOps
279. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/security-posture/policy-optimizer
280. https://cortex.marketplace.pan.dev/marketplace/details/PaloAltoNetworksAIOps/
281. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/best-practices-in-ngfw/on-demand-bpa-report
282. https://live.paloaltonetworks.com/t5/community-blogs/auto-remediation-in-prisma-cloud/ba-p/445343
283. https://docs.paloaltonetworks.com/saas-security/saas-security-inline/manage-saas-security-inline-policy/manage-saas-policy-rule-recommendations-on-strata-cloud-manager
284. https://www.youtube.com/watch?v=CNs42av5a7E
285. https://www.paloaltonetworks.com/resources/videos/easily-fix-misconfigurations-at-any-stage-of-the-application-lifecycle
286. https://pan.dev/aiops-ngfw-bpa/api/
287. https://www.paloaltonetworks.com/services/bpa

288. https://www.optiv.com/insights/discover/blog/aiops-palo-alto-networks
289. https://docs.paloaltonetworks.com/saas-security/sspm/remediate-posture-security-risks/remediate-saas-app-misconfigurations
290. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/about-metrics
291. https://docs.paloaltonetworks.com/ngfw/administration/device-telemetry/device-telemetry-configure/device-telemetry-enable
292. https://secureitconsult.com/aiops-for-ngfw/
293. https://docs.paloaltonetworks.com/ngfw/incidents-and-alerts/alerts
294. https://docs.paloaltonetworks.com/ngfw/incidents-and-alerts/alerts-reference
295. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/about/activate-aiops-for-ngfw
296. https://www.youtube.com/watch?v=03ZiBLB_nEk
297. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/best-practices-in-ngfw
298. https://www.youtube.com/watch?v=l7g8hYe1GJA
299. https://www.reddit.com/r/paloaltonetworks/comments/16yr3dw/anyone_try_aiops_for_ngfw_free/
300. https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/the-difference-between-alerts-that-are-included-in-an-incident/td-p/516582
301. https://live.paloaltonetworks.com/t5/next-generation-firewall/ai-for-fw-management/td-p/1245095
302. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-new-features/management-features/aiops-for-ngfw
303. https://www.optiv.com/insights/discover/blog/aiops-palo-alto-networks
304. https://www.youtube.com/watch?v=AzUB6xH0UJQ
305. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-the-dashboard
306. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-the-application-command-center/acc-tabs
307. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-january-2026
308. https://www.scribd.com/document/935840767/Strata-Cloud-Manager-Administration
309. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/insights-scm
310. https://docs.paloaltonetworks.com/iot/administration/create-dashboards-and-reports/custom-dashboards-widgets
311. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/dashboard/dashboard-widgets
312. https://www.youtube.com/watch?v=c24nc0tFRp4
313. https://www.youtube.com/watch?v=ulKpfu6jEAM
314. https://events.fuelusergroup.org/events/details/fuel-user-group-melbourne-user-group-presents-strata-cloud-manager-overview/
315. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/getting-started/ai-canvas/manage-widgets
316. https://www.youtube.com/watch?v=xG6TNSqKZOY
317. https://docs.paloaltonetworks.com/ngfw/help/10-2/acc
318. https://pan.dev/scm/docs/home/

319. https://www.paloaltonetworks.com/network-security/strata-cloud-manager
320. https://www.orangecyberdefense.com/be/palo-alto/firewall-best-practice/full-best-practices-assessment
321. https://www.youtube.com/watch?v=zOliowL8-Xo
322. https://www.youtube.com/watch?v=2mrUcLkuidQ
323. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000Xgh6CAC
324. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards/on-demand-bpa-report
325. https://live.paloaltonetworks.com/t5/community-blogs/bpa-transition-to-aiops-for-ngfw/ba-p/548612
326. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/best-practices-in-ngfw/on-demand-bpa-report
327. https://bluecatnetworks.com/blog/indeni-vs-palo-alto-networks-aiops/
328. https://pan.dev/aiops-ngfw-bpa/api/post-bpa-v-1-requests/
329. https://www.youtube.com/watch?v=CNs42av5a7E
330. https://www.youtube.com/watch?v=G0sdX-rWUHE
331. https://www.optiv.com/insights/discover/blog/aiops-palo-alto-networks
332. https://www.reddit.com/r/paloaltonetworks/comments/17b146i/ondemand_bpa_i_wish_we_could_go_back_to_the_old/
333. https://pan.dev/aiops-ngfw-bpa/api/
334. https://docs.paloaltonetworks.com/best-practices/best-practices-getting-started/get-started-with-best-practices/identify-and-prioritize-best-practices