Infrastructure Management and CDSS

In the context of the Palo Alto Networks Network Security Professional (NSP) certification, **Infrastructure Management and CDSS** is a specific exam domain (weighted at 15%) that tests your ability to configure, maintain, and manage Cloud-Delivered Security Services and the platforms that control them.

This domain bridges the gap between *security features* (what the firewall does) and *operational health* (how the firewall stays connected and managed).

1. Cloud-Delivered Security Services (CDSS)

CDSS refers to the suite of subscription-based services that offload heavy analysis to the cloud, allowing the firewall to leverage real-time global threat intelligence (Unit 42) without impacting local performance.

The NSP exam focuses on the configuration and maintenance of these core services:

Service	Primary Function	Key Management Consideration
Advanced Threat Prevention	Blocks exploits, malware, and C2 traffic.	Requires regular dynamic updates (Threat-ID).
Advanced WildFire	Cloud-based sandboxing for unknown files.	Files are forwarded to the cloud; requires a valid service route.
Advanced URL Filtering	Real-time categorization of web traffic.	Relies on cloud lookups; latency-sensitive.
Advanced DNS Security	Detects malicious domains and C2 tunneling.	Often requires "sinkhole" configuration in Anti-Spyware profiles.
Enterprise DLP	Prevents data exfiltration.	Requires defining data patterns and cloud connectivity for analysis.
SaaS Security	Discovers and manages Shadow IT.	Integrated into SCM for visibility into SaaS usage.

2. Infrastructure Management Platforms

This part of the domain covers the *tools* used to manage the security infrastructure.

- **Strata Cloud Manager (SCM):** The modern, AI-powered management interface.
  - **Folder Hierarchy:** SCM uses a hierarchy (`Global` > `All Firewalls` > `Device Groups`) to manage policy scope. You must understand **inheritance**—policies defined at the

"Global" level apply to all devices, while device-specific exceptions are made lower down.[1]

    - **Onboarding:** Requires associating the firewall with your Customer Support Portal (CSP) account, installing a **Device Certificate**, and applying **Device Onboarding Rules** (which can automatically push a "Snippet" or base configuration).[2]
- **Panorama:** The traditional centralized management platform.
    - **Templates & Device Groups:** You must know how Templates (network/device settings) and Device Groups (policy/objects) interact to push configurations to managed firewalls.

3. Critical Infrastructure Components

To support CDSS, the underlying infrastructure (the firewall itself) must be configured correctly. The exam tests these specific "plumbing" tasks:

Service Routes

By default, the firewall uses its Management (MGT) interface for all communication with Palo Alto Networks cloud services (updates, DNS lookups, WildFire uploads).[3]

- **The Problem:** In many high-security networks, the MGT port is on an isolated OOB network with no internet access.
- **The Solution:** You must configure **Service Routes** (`Device > Setup > Services > Service Route Configuration`) to force the firewall to use a dataplane interface (e.g., `ethernet1/1`) to reach the update servers and CDSS clouds.[4]

Updates and Licensing

- **Dynamic Updates:** You must schedule regular updates for Applications and Threats. "Real-time" services like WildFire updates should be set to check as frequently as possible (e.g., every minute).
- **Licensing:** CDSS features will not function without valid licenses. "Infrastructure Management" involves monitoring license expiration and ensuring the firewall can "phone home" to validate its subscriptions.

Decryption (SSL/TLS)

While often its own topic, decryption is an infrastructure prerequisite for CDSS. If you cannot decrypt the traffic, services like DLP and Threat Prevention cannot inspect the payload, rendering them ineffective against encrypted threats.

Recommendation for NSP Study

For your NSP preparation, focus heavily on **Strata Cloud Manager (SCM)** workflows, as this is the newer standard emphasized in current certifications. Specifically, practice the **onboarding flow**:

1. Register device in CSP.

2. Install Device Certificate.
3. Configure SCM connection settings.
4. Verify status in SCM under "Cloud Managed Devices".[5]

⁂

Palo Alto Infrastructure Management and CDSS

This domain accounts for **15%** of the Network Security Professional (NSP) exam. In the NSP context, "Infrastructure Management" moves beyond basic firewall configuration into the *architecture* that keeps the security services (CDSS) running and updated.[28]

The core challenge tested here is: **"How do you ensure the firewall can successfully talk to the cloud to offload security processing?"**

1. Management Platforms: SCM vs. Panorama

The exam emphasizes the transition to Strata Cloud Manager (SCM). You must understand how configuration objects are inherited differently in SCM compared to Panorama.

Feature	Panorama (Traditional)	Strata Cloud Manager (Modern/NSP Focus)
Hierarchy	Device Groups (Policies) & Templates (Network)	**Folders** (Container for all config types)
Inheritance	Shared > Device Group > Firewall	Global > Folder > Sub-folder > Device
Modularity	Template Stacks	**Snippets** [29]
Variables	Template Variables	**Snippet Variables** [30]

- **Snippets:** These are modular configuration blocks (e.g., a "Best Practice Office 365" rule set) that you explicitly associate with a Folder or Device. Unlike parent folders, snippets are *not* automatically inherited; they must be attached.[29] [31]
- **Variables:** Used within snippets to standardize policy while allowing unique local values (e.g., defining a variable `$BRANCH_IP` that resolves to `10.1.1.0/24` in New York and `10.2.1.0/24` in London).[30]

2. CDSS "Plumbing" & Prerequisites

Cloud-Delivered Security Services (CDSS) will fail if the underlying infrastructure is not "plumbed" correctly. The exam tests these dependencies:

- **Service Routes:** By default, all cloud communication (WildFire uploads, DNS queries, URL lookups) leaves via the **MGT interface**. If MGT is air-gapped or restricted, you *must* configure a Service Route (`Device > Setup > Services > Service Routes`) to force traffic out a dataplane interface (e.g., `ethernet1/1`).[32]
- **DNS Resolution:** The firewall itself acts as a client. If the firewall cannot resolve `updates.paloaltonetworks.com` or `wildfire.paloaltonetworks.com`, all CDSS services fail. This is the #1 cause of "Failed to fetch license" errors.[32]

- **Device Certificate:** Required for SCM onboarding and secure logging. If this certificate expires, the device disconnects from management.

3. Troubleshooting Toolkit (CLI)

For a technical professional, knowing the CLI verification commands is critical for the "Maintenance" portion of this domain.

Service	CLI Command to Verify	Key Success Indicator
WildFire	`show wildfire status`	Look for `Cloud connection: connected` [33].
DNS Security	`show dns-proxy dns-signature info`	Verifies download of the "DNS Security" signatures [34].
URL Filtering	`show url-cloud status`	Checks connection to the PAN-DB cloud [35].
Licensing	`request license fetch`	Forces a manual check; useful if auto-renewal fails [36].
Updates	`ping host updates.paloaltonetworks.com`	Simple connectivity check from the *management plane* [32].

4. AIOps & Capacity Planning

The "Infrastructure Management" domain also includes AIOps for monitoring health.

- **Capacity Analyzer:** This specific AIOps feature is used to monitor hardware resource consumption (CPU, memory, session limits) over time to predict when you will outgrow a firewall.[28]
- **Adoption Insights:** SCM provides "Adoption" dashboards to show you which CDSS features (like DNS Security or BPDU protection) you are *licensed* for but *not using*.[37]

Exam Tip: If a question asks about "standardizing configuration across disparate locations with different IP schemes," the answer is likely **Snippets with Variables** in SCM, not just "Device Groups" in Panorama.

⁂

BPDU protection

BPDU (Bridge Protocol Data Unit) protection is a mechanism used in Layer 2 networks to maintain the integrity of the Spanning Tree Protocol (STP) topology. While primarily a switching concept (Cisco, Juniper, etc.), it is highly relevant to Palo Alto Networks firewalls when deployed in **Layer 2** or **Virtual Wire** interfaces, or when configured with zone protection profiles.

1. The Concept: Protecting the Topology

In a stable network, edge ports (connected to PCs, servers, or printers) should never generate STP packets (BPDUs). If an edge port receives a BPDU, it usually means someone has plugged in an unauthorized switch (Shadow IT) or created a loop.

BPDU Guard is the feature that monitors these ports.

- **Action:** If a BPDU is received on a protected port, the port is immediately shut down (placed in an `err-disabled` state) to prevent potential loops or root bridge manipulation.[44] [45]

2. BPDU Handling on Palo Alto Firewalls

Palo Alto Networks firewalls are not switches, but they process BPDUs differently depending on the interface mode.

A. Zone Protection Profiles (Security Focus)

You can configure **Zone Protection Profiles** to drop non-IP protocol traffic, which can include layer 2 protocols if not explicitly allowed. While not a direct "BPDU Guard" toggle like a switch, this profile defends the zone from layer 2 based attacks.[46]

- **Navigation:** `Network > Network Profiles > Zone Protection`.

B. Layer 2 Interfaces (Switching Focus)

When the firewall interfaces are configured in **Layer 2 mode**, the firewall acts as a bridge.

- **Default Behavior:** The firewall typically forwards BPDUs between interfaces in the same VLAN or Virtual Wire (VWire) to allow upstream/downstream switches to maintain STP.
- **Rewriting:** In complex VLAN scenarios, you may need to configure **BPDU Rewrite** to ensure BPDUs are tagged correctly for the receiving switch, preventing it from discarding legitimate STP traffic.[47]

3. Related "Guard" Technologies

In the context of network security infrastructure (NSP domain), you should differentiate these related protections:

Feature	Purpose	Typical Location
BPDU Guard	Shuts down port if BPDU received.	Edge ports (facing users).
Root Guard	Prevents a port from becoming a Root Port.	Downlink ports (facing downstream switches).
Loop Guard	Prevents loops caused by unidirectional link failures.	Fiber uplinks/trunks.
BPDU Filter	Ignores BPDUs entirely (risky).	Specific special-case ports.

Summary for NSP

For the Palo Alto NSP exam, understand that while the firewall itself doesn't typically run STP (unless in very specific L2 setups), it sits in the middle of these domains.

- **Key Takeaway:** If you deploy a firewall in **Virtual Wire** mode between two switches, you must ensure it **passes** BPDUs so the switches don't think the link is down and create a loop. Conversely, if you want to isolate two STP domains, you configure it to **drop** BPDUs.

⁂

Maintain and configure CDSS

In the context of the **Palo Alto Networks Network Security Professional (NSP)** exam, the "Maintain and Configure CDSS" domain tests your ability to operationalize the cloud-delivered services. You are expected to know not just how to turn them on, but how to ensure they remain connected and effective.

Key changes in the NSP curriculum include a heavy emphasis on **Strata Cloud Manager (SCM)** workflows and the "Advanced" versions of services (ATP, WildFire, etc.).

1. General CDSS Configuration & Maintenance

Before configuring specific services, the underlying "plumbing" must be maintained.

- **Service Routes:** By default, CDSS traffic uses the **MGT** interface. In production, you typically must configure a Service Route (`Device > Setup > Services > Service Routes`) to force this traffic out a dataplane interface (e.g., ethernet1/1) to reach the internet.
- **Profile Groups (SCM Specific):** Unlike Panorama where you can attach individual profiles to a rule, **Strata Cloud Manager (SCM) mandates the use of "Profile Groups"**. You must bundle your Antivirus, Spyware, and URL profiles into a group before applying them to a Security Policy Rule.[53]

2. Service-Specific Configuration Guide

Advanced Threat Prevention (ATP)

ATP blocks known exploits, malware, and C2 traffic. The "Advanced" feature adds **Inline Cloud Analysis** to block unknown C2 threats in real-time.

- **Configuration:**
  - **Vulnerability Protection Profile:** Create a rule to block "critical" and "high" severity threats.
  - **Inline Cloud Analysis:** Must be explicitly enabled in the profile to allow real-time cloud lookups for command-and-control traffic.[54]
- **Maintenance:**

- **Dynamic Updates:** Ensure "Applications and Threats" are set to download and install automatically (recommended: Daily or Real-time).
- **AIOps:** Use the SCM "Threat Practices" dashboard to identify rules that are missing ATP profiles.

Advanced WildFire

Analyzes unknown files in a cloud sandbox.

- **Configuration:**
  - **WildFire Analysis Profile:** Create a profile and set the action to `Forward` for "Any" file type.
  - **Best Practice:** Do not limit forwarding to specific file types (like PE or PDF); use "Any" to catch novel threats. Ensure the profile is attached to a Security Policy Rule allowing file transfer (e.g., web-browsing).[55] [56]
- **Maintenance:**
  - **CLI Check:** Run `show wildfire status` to verify the cloud connection.
  - **Forwarding Check:** Use `test wildfire registration` to ensure the firewall can upload samples.

Advanced URL Filtering

Controls web access and prevents credential phishing.

- **Configuration:**
  - **Profile Actions:**
    - `Block`: User sees a block page.
    - `Continue`: User sees a warning but can proceed (good for "Questionable" categories).
    - `Override`: Requires a password to proceed (often used for Helpdesk bypass).
  - **Credential Phishing:** In the profile's "User Credential Submission" tab, set "Block" for high-risk categories to prevent users from typing corporate passwords into bad sites.[57]
- **Maintenance:**
  - **Cloud Status:** Run `show url-cloud status` to verify connectivity to PAN-DB.

DNS Security

Protects against DNS tunneling and C2 domains.

- **Configuration:**
  - **Anti-Spyware Profile:** DNS Security is configured *within* the Anti-Spyware profile under the "DNS Policies" tab.

    - **Sinkhole:** You must configure a "Sinkhole" action (default IP: `sinkhole.paloaltonetworks.com`) for malicious domains. This forges a response to the client, redirecting them to a verifiable IP so you can identify the infected host.[58] [59]
- **Maintenance:**
    - **Connectivity:** Run `show dns-proxy dns-signature info` to verify signature downloads.

Enterprise DLP

Prevents sensitive data loss (PII, PCI, etc.).

- **Configuration:**
    - **Service Route:** Critical—you must typically create a specific service route for the DLP service to upload files to the cloud for inspection.[60]
    - **Policy:** DLP is invoked via a **Data Filtering Profile** attached to a security rule.
- **Maintenance:**
    - **Pre-Rules:** Ensure you have an SSL Decryption policy active; DLP cannot inspect encrypted traffic.

3. SaaS Security Inline

Visibility into "Shadow IT" and SaaS application usage.

- **Configuration:**
    - **Activation:** Requires linking the firewall to the SaaS Security tenant via the Hub/CSP.
    - **ACE (App-ID Cloud Engine):** Must be enabled to allow the firewall to download new App-IDs for SaaS apps dynamically without waiting for a content update.[61]
- **Maintenance:**
    - **Log Forwarding:** SaaS Security relies entirely on logs. You must configure **Log Forwarding** to the Cortex Data Lake (CDL) for the service to function. If logs stop flowing, the dashboard goes blank.

Summary Checklist for NSP Exam

Task	Key Requirement / Command
Verify Cloud Connection	`show wildfire status`, `show url-cloud status`
Force License Check	`request license fetch`
Handle DNS C2	Configure **Sinkhole** in Anti-Spyware Profile
SCM Policy	Must use **Profile Groups** (not individual profiles)
SaaS Visibility	Requires **Log Forwarding** to Data Lake

⁂

Security Policies: SCM vs. Panorama & Best Practices

In the Network Security Professional (NSP) exam, "Security Policies" is a foundational topic but with a twist: you are now tested on the **Strata Cloud Manager (SCM)** approach, which differs structurally from the traditional Panorama method.

1. Policy Hierarchy: SCM vs. Panorama

The way rules are inherited and prioritized is key to answering scenario-based questions.

Feature	Panorama (Traditional)	Strata Cloud Manager (NSP Focus)
Container	**Device Groups** (Hierarchy)	**Folders** (Hierarchy)
Rule Inheritance	`Pre-Rules` (Top) → `Local Rules` (Firewall) → `Post-Rules` (Bottom)	`Global Folder` (Top) → `Parent Folder` → `Child Folder` → `Device`
Visibility	Rules are split into "Pre", "Post", and "Default" sections.	**Unified Rulebase**: All inherited rules are visible in a single list, sorted by priority.
Overrides	You "override" specific objects in child groups.	You cannot delete inherited rules in child folders, only add new ones *around* them.

Key SCM Concept: "Configuration Scope."

- Policies defined in the **Global** folder apply to *every* firewall in your fleet.
- Policies in a **Data Center** folder apply only to firewalls in that folder.
- **Conflict Resolution:** If a Global rule allows traffic, a local rule cannot "block" it if the Global rule sits higher in the evaluation order. SCM encourages a "Shared Policy" model where common rules (e.g., "Block Bad IPs") are at the top (Global), and specific allowances (e.g., "Allow SQL to HR Server") are at the bottom (Device level).

2. Rule Types & Default Behavior

Palo Alto Networks firewalls use a "Zero Trust" model, but the default behavior depends on the *zones*.

- **Universal:** The default rule type. Applies to *both* inter-zone and intra-zone traffic.
- **Inter-zone (Default: BLOCK):** Traffic moving between *different* zones (e.g., Trust to Untrust) is implicitly **blocked** at the end of the rulebase.
- **Intra-zone (Default: ALLOW):** Traffic staying *within* the same zone (e.g., Trust to Trust) is implicitly **allowed**.
    - **NSP Best Practice:** You should create an explicit "Deny All" or "Cleanup" intra-zone rule at the bottom of your policy to override this unsafe default and gain visibility (logging) into lateral movement.

3. Anatomy of a "Best Practice" Rule

An exam-passing security policy rule must include more than just IPs. It must be **App-ID** centric.

- **Application:** Never use "Any". Always specify the App-ID (e.g., `ssl`, `web-browsing`, `ssh`).
- **Service:** Set to **"application-default"**.
  - *Why?* This forces the application to run on its standard port (e.g., SSH on 22). If malware tries to tunnel SSH over port 80, the firewall blocks it because it mismatches the "application-default" expectation.
- **Profile Groups (SCM Mandatory):** In Strata Cloud Manager, you cannot attach individual security profiles (like just "Antivirus") to a rule. You **must** create a **Security Profile Group** (bundling AV, Spyware, URL, etc.) and attach that group to the rule.
- **Log Forwarding:** A rule without a Log Forwarding Profile is invisible. You must attach a profile to send logs to Cortex Data Lake (CDL).

4. Shadowing & Order

Rules are evaluated **top-down, first-match-wins**.

- **Shadowing:** If Rule #1 says "Block All Traffic to France" and Rule #2 says "Allow Traffic to Paris Server", Rule #2 is "shadowed" (never hit) if the Paris IP is geolocated to France.
- **NSP Tip:** SCM includes "Policy Optimizer" and "Rule Usage" tools to highlight unused or shadowed rules, which you should regularly prune.

5. User-ID in Policy

- **Source User:** Instead of IP addresses (which change), use **User-ID** (e.g., `domain\marketing-group`).
- **Dependency:** This requires the firewall to have a mapping source (User-ID Agent, Terminal Server Agent, or GlobalProtect) to resolve the IP to a user *before* the packet hits the policy. If the mapping is missing, the rule is skipped.

Summary Checklist for NSP Exam

Feature	Best Practice / Exam Answer
Service Setting	Always use **application-default** (avoids non-standard port evasion).
Rule Type	**Universal** (covers both zone scenarios).
Intra-zone Default	**Allow** (must be overridden for Zero Trust).
SCM Requirement	Must use **Profile Groups**, not individual profiles.
Policy Scope	**Global** folder for org-wide blocks; **Device** folder for specific apps.

CDSS Security Policies: Configuration & Strategy

For the NSP certification, "CDSS Security Policies" refers to how you apply cloud-delivered protections to your traffic. There is no single "CDSS Policy" object; rather, you configure specific **Security Profiles** (ATP, WildFire, etc.) and attach them to **Security Policy Rules**.

In **Strata Cloud Manager (SCM)**, this workflow is stricter than in Panorama: you generally *must* use **Profile Groups** to bundle these services.

1. CDSS Policy Structure in SCM

To enable CDSS protections, you must build your Security Policy rules with these three layers:

Layer	Configuration	Best Practice
1. The Rule	`Policies > Security > [Rule Name]`	Use **App-ID** (not ports) and set Service to `application-default` [98].
2. The Profile Group	`Objects > Profile Groups`	Create a "Best Practice" group containing: - **Antivirus** (Blocking) - **Anti-Spyware** (DNS Sinkhole enabled) - **Vulnerability Protection** (Strict) - **URL Filtering** (Advanced) - **File Blocking** (Block risky types) [99].
3. The Attachment	`Rule > Profile Setting`	Attach the Profile Group to *every* Allow rule. **Note:** CDSS cannot inspect traffic in "Deny" rules.

2. Service-Specific Policy Nuances

Each CDSS service has unique "policy-like" configuration steps that the exam tests:

A. DNS Security (Anti-Spyware Profile)

- **Where it lives:** Inside the **Anti-Spyware Profile** > **DNS Policies** tab.[100]
- **Key Policy Action: Sinkhole**. You should rarely use "Block" for DNS.
  - *Why?* "Block" just kills the UDP packet, leaving the client confused (and retrying). "Sinkhole" returns a fake IP (`sinkhole.paloaltonetworks.com`), forcing the client to try to connect to it. This allows the firewall to log the *source IP* of the infected host in the Threat Log, making remediation possible.

B. Enterprise DLP (Data Filtering Profile)

- **Where it lives: Data Filtering Profile**.[99]
- **Policy Logic:** You define **Data Patterns** (e.g., Credit Card Regex) and **Confidence Levels**.
- **Placement:** DLP is resource-intensive.
  - *Best Practice:* Place DLP-enabled rules *higher* in the rulebase but scoped *narrowly* (e.g., "HR Subnet to Internet" or "Uploads to Box"). Do not apply "Block all Credit Cards" to your global "Allow All" rule unless you want to crash performance.

C. SaaS Security (Inline)

- **Where it lives: App-ID** & **URL Filtering**.
- **Policy Logic:** SaaS Security helps you discover "Shadow IT".
    - *Enforcement:* Once discovered, you don't just "block SaaS." You use **HTTP Header Insertion** (in URL Filtering) to enforce "Tenant Restrictions" (e.g., "Allow logging into *Corporate* Google Workspace, but block *Personal* Gmail").[101]

D. Advanced Threat Prevention (Inline Cloud Analysis)

- **Where it lives: Vulnerability Protection Profile**.
- **Policy Logic:** You must explicitly enable **"Inline Cloud Analysis"** within the profile to block *unknown* C2 traffic in real-time. Standard profiles only block *known* signatures.[102]

3. SCM Policy Hierarchy (The "Folder" Trap)

In the exam, you will be asked where to apply these CDSS policies.

- **Global Folder:** Apply "Base" CDSS rules here (e.g., "Block Known Malware Global"). These are inherited by *all* firewalls.
- **Device Folder:** Apply specific CDSS exceptions here (e.g., "Allow this specific Threat ID for the Legacy App Server").
- **Conflict:** If a Global rule says "Block Threat ID 12345 (Critical)" and a local rule says "Allow", the traffic is **blocked** if the Global rule is higher in the sequence. To override, you often need to place the specific allow rule *above* the global block in the hierarchy or use specific "Pre-Rule" logic.[103]

Summary Checklist

Feature	Exam Key
Profile Groups	**Mandatory** in SCM for attaching CDSS to rules.
Sinkhole	The required action for **DNS Security** to enable attribution.
Inline Cloud Analysis	Must be enabled inside **Vulnerability Protection** to catch zero-day C2.
Decryption	**Prerequisite.** CDSS cannot inspect SSL/TLS traffic without a Decryption Policy.

⁂

CDSS Profiles: Configuration for NSP

The "CDSS Profiles" domain tests the specific settings within each Security Profile that maximize protection. In **Strata Cloud Manager (SCM)**, you rarely apply these profiles individually; they are almost always bundled into **Profile Groups**.[113]

1. Advanced Threat Prevention (ATP)

- **Key Feature: Inline Cloud Analysis**.
- **Configuration:**
  - Navigate to the **Vulnerability Protection Profile**.
  - **Action:** Set rules to `block` (or `reset-both`) for severities `critical`, `high`, and `medium`.
  - **Inline Analysis:** You *must* check the box to enable **Inline Cloud Analysis** within the profile. This allows the firewall to query the cloud in real-time for *unknown* C2 traffic that doesn't yet have a signature.[114]
  - **Best Practice:** Do not just rely on the default profile; clone it and set the "Action" to `reset-both` to ensure the connection is actively killed.

2. Advanced WildFire

- **Key Feature:** Cloud Sandboxing for unknown files.
- **Configuration:**
  - Navigate to the **WildFire Analysis Profile**.
  - **Rule:** Create a rule for **Any** application and **Any** file type.
  - **Direction:** Set direction to **Both** (upload and download).
  - **Action:** Set to **Forward**.
  - **Best Practice:** The exam often tricks you with "limit to PE files" or "limit to PDF." The correct answer is **Any** file type to catch novel threats.[115]
  - **Note:** WildFire *only* analyzes; it doesn't block in real-time unless combined with "Hold Mode" (rare) or until a signature is generated (approx. 10-15 seconds later).

3. Advanced URL Filtering

- **Key Feature:** Web categorization and Phishing Prevention.
- **Configuration:**
  - **Site Access:** Set `block` for obvious bad categories (malware, command-and-control, phishing). Set `continue` for "questionable" categories to warn users.
  - **Credential Phishing:** This is a separate tab in the profile. You must enable "User Credential Detection" (requires User-ID).
    - **Action:** Set to `block` for "High Risk" and "Medium Risk" categories to stop users from entering corporate passwords into shady sites.[116]
  - **Safe Search:** Enable "Safe Search Enforcement" to force Google/Bing into strict mode.

4. Enterprise DLP

- **Key Feature:** Data Pattern Matching (Credit Cards, SSN, etc.).
- **Configuration:**
  - Navigate to **Data Filtering Profile**.
  - **Patterns:** Select a predefined pattern (e.g., `Credit Card Number`) or create a custom Regex.
  - **Confidence:** Set the confidence level (e.g., "High") to reduce false positives.
  - **Masking:** You can configure the profile to **mask** the sensitive data (e.g., `X-X-X-1234`) in the logs so admins don't see the PII.[117]
  - **File Types:** DLP can inspect both "File" and "Non-File" (web form) traffic.

5. DNS Security

- **Key Feature:** C2 Domain Blocking.
- **Location: Anti-Spyware Profile** (not its own profile type).
- **Configuration:**
  - Go to **DNS Policies** tab.
  - **Action:** Set to **Sinkhole** for known malicious domains (C2, malware).
  - **Packet Capture:** Enable "Single Packet Capture" on the sinkhole action to capture the DNS query for forensic analysis.[118]

Exam Summary Table

Profile Type	Critical Configuration Setting	NSP Exam Trap
Vulnerability	Enable **Inline Cloud Analysis**	Forgetting to enable the cloud lookup checkbox.
WildFire	File Type = **Any**	Limiting analysis to only ".exe" files.
URL Filtering	**Credential Phishing** tab	Confusing "Site Access" block with "Credential Submission" block.
Anti-Spyware	**DNS Sinkhole**	Setting action to "Block" (which hides the infected client IP).
DLP	**Masking**	Forgetting to mask PII in logs for compliance.

⁂

"Action" to reset-both

When configuring the **Action** in a Vulnerability Protection or Antivirus Profile, the setting `reset-both` is the preferred "Kill" switch for TCP-based threats.

What `reset-both` Does

- **Mechanism:** The firewall sends a TCP RST (Reset) packet to **both** the client (the attacker or victim) and the server (the destination).
- **Result:** This immediately tears down the TCP connection on both ends.
  - The **Client** receives a RST and stops sending data immediately (avoids retransmission timeouts).
  - The **Server** receives a RST and releases the socket resource immediately (protects against resource exhaustion).

Why use `reset-both` instead of `drop`?

In the NSP exam and real-world "Infrastructure Management," understanding *why* you choose this action is critical:

1. **Resource Efficiency:** If you just `drop` the packet, the client (attacker) doesn't know the packet was lost. It will keep retransmitting, and the server will keep the socket open waiting for data. `reset-both` forces both sides to "clean up" instantly.[129] [130]
2. **User Experience (Internal):** For internal users who accidentally download malware, `reset-both` results in an immediate browser error ("Connection Reset"), whereas `drop` causes the browser to hang/spin until it times out.
3. **The "Drop" Use Case:** You typically use `drop` only for **Denial of Service (DoS)** attacks or reconnaissance (scanning) on the internet edge, where you *want* to waste the attacker's time and hide your presence.[130]

Exam Nuance: The "Reset-Server" Trap

Sometimes, even if you configure `reset-both`, the Threat Log might show `reset-server`.

- **Scenario:** This happens if the threat is detected *very early* (e.g., in the HTTP GET request).
- **Reason:** The firewall injects a "503 Block Page" to the client (to tell the user why they are blocked). Since the client got a valid HTTP response (the block page), the firewall doesn't need to "Reset" the client; it only needs to "Reset" the server to stop the bad download. The logs reflect this action as `reset-server` because that's the only side that needed a forceful kill.[131]

Best Practice: For **Critical**, **High**, and **Medium** severity threats in Vulnerability and Antivirus profiles, always set the action to `reset-both`.[132] [133]

⁂

CDSS Updates

In the "Infrastructure Management and CDSS" domain, configuring **Dynamic Updates** correctly is a major exam topic because it represents the balance between *security* (getting updates fast) and *stability* (not breaking the network).

1. Types of Updates

You must know the difference between the core update types and their schedules:

Update Type	Contents	Frequency	Best Practice (Security-First)
Applications & Threats	New App-IDs and Threat signatures (IPS/Spyware).	Weekly (Apps) / Daily (Threats)	**Daily** (or Hourly) check. Action: **Download and Install**.
WildFire	Signatures for newly discovered malware.	**Real-time** (every 5 mins).	**Every Minute**. Action: **Download and Install**.
Antivirus	Daily malware signatures.	Daily.	**Hourly**. Action: **Download and Install**.

2. The "Threshold" Concept

This is a critical exam concept. You can configure a **Threshold** (in hours) to tell the firewall: *"Even if a new update is available, do not install it unless it has been released for X hours."*

- **Purpose:** To avoid "buggy" updates that might be pulled immediately after release.
- **Best Practice (Security-First):** Set threshold to **0** or very low (e.g., < 6 hours). You accept the risk of a bad update to ensure you are protected against zero-day threats immediately. [144]
- **Best Practice (Mission-Critical/Availability):** Set threshold to **24-48 hours**. This lets other customers "test" the update first. If Palo Alto pulls a bad update, your firewall won't have installed it yet. [145]

3. Strata Cloud Manager (SCM) Configuration

In SCM, update schedules are managed via **Snippets** or **Folders**.

- **Inheritance:** A schedule defined at the "Global" folder applies to all firewalls.
- **Action:** In SCM, navigate to `Configuration > NGFW > Device Setup > Software Update > Schedules`.
- **Recurrence:**
  - **WildFire:** Set to "Real-time" (preferred) or "Every Minute". [146]
  - **App/Threat:** Set to "Daily" or "Hourly" depending on risk appetite. [147]

4. Dependencies & Troubleshooting

- **The "Chicken and Egg" Problem:** Antivirus updates often fail if **Applications and Threats** are not installed first. The AV engine relies on the core Threat engine.[148]
- **License Check:** If updates fail with "Failed to fetch," check your **Service Route** (DNS/Internet access) and verify the license is active (`request license fetch`).[149]

Exam Tip: If a question asks how to protect a "High Security" environment from a new 0-day exploit released 2 hours ago, the answer involves setting the **Application and Threat Update Schedule** to "Recurrence: Hourly" and **Threshold: 0**. If you had a 24-hour threshold, you would still be vulnerable.

⁂

Maintain and configure IOT security

In the Palo Alto Networks NSP curriculum, **IoT Security** is not just an add-on; it is a full lifecycle domain that transforms the firewall into a sensor. The exam focuses on the *operational* aspect: how to set it up, how it gathers data, and how to turn that data into policy.

1. The IoT Security Lifecycle

The NSP exam tests your understanding of the five-step lifecycle:[159]

1. **Understand (Identify):** Discover all devices (IT, OT, IoT).
2. **Assess:** Determine risk scores based on vulnerabilities and behavior.
3. **Recommend:** Use ML to generate "least privilege" policies.
4. **Enforce:** Apply those policies to the firewall.
5. **Prevent:** Block known threats and anomalies in real-time.

2. Onboarding & Visibility (The "Sensor" Concept)

IoT Security does not work if the firewall cannot *see* the traffic.

- **The Problem:** Firewalls are often at the perimeter (Layer 3), but IoT devices use **DHCP** (Layer 2 broadcast) to get IP addresses. If the firewall doesn't see the DHCP handshake, it can't identify the device model/vendor accurately.
- **The Solution:** You must often deploy a "Sensor" interface to capture this data.
  - **TAP Interface:** The exam often asks about gaining visibility without disrupting the network. The answer is to configure a **TAP interface** connected to a span port on your core switch. This allows the firewall to see DHCP unicast/broadcast traffic it wouldn't normally route.[160] [161]
  - **DHCP Logging:** Ensure the firewall is sending "Enhanced Application Logs" (EAL) to the Data Lake (Cortex). This is how the cloud engine learns about the devices.

3. Policy Recommendations (The "Easy Button")

You are not expected to write IoT policies manually. The exam tests the **Policy Recommendation** workflow.

1. **Wait for Confidence:** You cannot generate a policy immediately. You must wait for the ML engine to reach **90% confidence** in the device's behavior.[162]
2. **Import:** Once ready, you "Import" the recommended policy from the IoT portal to Panorama or the Firewall.
3. **Structure:** The recommendation creates a **Device Profile** (e.g., "All MRI Machines") and a set of rules allowing only their observed traffic (e.g., "DICOM to Server A").

4. Risk Assessment

- **Risk Score:** Each device gets a risk score (0-100).
- **Factors:** The score is calculated based on:
  - **Vulnerabilities:** Known CVEs in the device firmware.
  - **Behavior:** Is the thermostat talking to an unknown IP in Russia?
  - **Hygiene:** Default passwords, expired certificates, or end-of-life OS.[163]

Exam Tip: If asked how to secure a network of medical pumps without knowing their communication patterns, the answer is **"Deploy IoT Security, wait for the ML baseline (90% confidence), and then import the recommended Policy."** Do *not* answer "Manually create rules" or "Block all unknown traffic immediately."

⁂

TAP Interface

A **TAP (Test Access Point) Interface** is a specific interface mode on Palo Alto Networks firewalls used for **passive visibility**. In this mode, the firewall acts like a sensor—it ingests a copy of network traffic (typically from a switch SPAN port) to identify applications, users, and threats *without* sitting inline or affecting network performance.

In the context of the **Infrastructure Management** and **IoT Security** domains of the NSP exam, the TAP interface is the primary mechanism for "out-of-band" discovery.

1. Configuration & Mechanics

To configure a TAP interface, you must configure *both* the interface and a specific zone type.

- **Interface Type:** Set the physical interface type to **TAP** (`Network > Interfaces`).
- **Security Zone:** You must assign it to a zone that is also of type **TAP**.
  - *Constraint:* A TAP interface cannot belong to a Layer 3 or Layer 2 zone. It requires a dedicated TAP zone.

- **Policy:** Even though it is passive, **you must configure a Security Policy rule** to "Allow" traffic from the TAP zone to the TAP zone.
    - *Why?* Without this rule, the firewall drops the packets upon ingress and performs no inspection (App-ID, Content-ID).
    - *Rule Action:* The action is effectively "Alert" only. You cannot "Block" traffic on a TAP interface because the firewall is not inline.[174]

2. Primary Use Case: IoT & DHCP Visibility

As discussed in the IoT domain, the firewall often sits at the perimeter (Layer 3) and misses the Layer 2 DHCP broadcasts that identify IoT devices.

- **The Solution:** Connect a TAP interface to a SPAN port on your internal switch.
- **DHCP Logging:** This allows the firewall to see the initial DHCP handshake (which contains the device's **MAC address**, **Hostname**, and **Vendor Class Identifier**).
- **Cloud Feed:** The firewall sends this metadata to the Cortex Data Lake via **Enhanced Application Logs (EAL)**, enabling the IoT Security service to profile the device correctly.[175]

3. Capabilities & Limitations (NSP Exam Critical)

You must know what a TAP interface *can* and *cannot* do compared to a Virtual Wire (VWire).

Feature	TAP Interface	Virtual Wire (VWire)
Topology	Out-of-band (Passive)	Inline (Active)
Blocking	**No**. Can only alert/log.	**Yes**. Can block/reset traffic.
Latency	Zero (does not touch live traffic).	Microseconds (inspects live traffic).
SSL Decryption	**Yes** (with limitations).	**Yes**.
NAT	No.	Yes.
Use Case	Proof of Concept (POC), IoT Discovery.	Transparent Inline Security, Segmentation.

- **Decryption Note:** A TAP interface *can* decrypt inbound SSL traffic (if you have the server certificate), but it cannot decrypt outbound SSL (Forward Proxy) effectively because it cannot "man-in-the-middle" the handshake to inject a certificate. It can only passively try to decrypt with a known key, which fails for ephemeral ciphers (DHE/ECDHE) commonly used today.[176] [177]

4. Hardware Resources

- **Oversubscription:** Be careful connecting a 10Gbps SPAN port to a 1Gbps TAP interface. If the traffic bursts exceed 1Gbps, the TAP interface will drop packets, causing "blind spots" in your visibility, though it won't impact production traffic.[178]
- **Dedicated Hardware:** For high-speed environments, it is recommended *not* to mix TAP traffic and Production traffic on the same firewall hardware, as the TAP inspection consumes CPU resources that could affect production throughput.[179]

Summary Checklist

- **Interface Type:** TAP.
- **Zone Type:** TAP.
- **Policy: Intrazone Allow** (Tap-to-Tap) is mandatory for inspection.
- **Decryption:** Possible for **Inbound Inspection** (static RSA keys) but generally not for Forward Proxy (DHE/ECDHE).
- **Key Function:** Feeds **Device-ID** and **App-ID** data to CDSS without risk of blocking.

⁂

IOT Security Security Policies

In the **Infrastructure Management and CDSS** domain of the NSP exam, "IoT Security Policies" test your ability to operationalize the telemetry collected from your network sensors. The key shift here is moving from "IP-based" rules to "**Device-ID** based" rules, leveraging the ML-driven recommendations from Strata Cloud Manager (SCM).

1. The Core Concept: Device-ID

Traditional firewalls use IP addresses. IoT Security introduces **Device-ID**, which tracks a device (e.g., "MRI Machine X-Ray 01") regardless of its IP changes.

- **Policy Structure:** Instead of `Source IP: 10.1.1.50`, your rule uses `Source Device: MRI-Scanner-Profile`.[189]
- **Prerequisite:** You must enable **Device Identification** on the *Source Zone* (`Network > Zones > [Zone] > Enable Device Identification`) for the firewall to map IPs to Device-IDs dynamically.[190]

2. The Policy Recommendation Workflow

The NSP exam emphasizes that you should *not* manually write IoT rules from scratch. You should use the automated workflow:

Step	Action	Key Detail
1. Baseline	Wait for ML Confidence.	The system observes traffic to build a baseline. Wait until confidence is high (e.g., 90%) [191].
2. Review	View Recommendations.	In SCM, go to the **IoT Security** dashboard. The system suggests a "Least Privilege" policy (e.g., "Allow MRI to DICOM Server, Block Internet").
3. Activate	"Activate" the Policy Set.	This stages the policy for export. Note: You can only activate *one* policy set per device profile at a time [192].
4. Import	Import to Rulebase.	In SCM/Panorama, select `Import Policy Rule(s)`. You choose whether to place them in **Pre-Rules** (Global) or **Post-Rules** (Local) [193].

3. SCM Specifics: "Integrated" Management

In previous versions, you had to jump between the IoT Portal and Panorama. In Strata Cloud Manager (SCM), this is **fully integrated**.

- **Unified Dashboard:** You view device risks, vulnerabilities, and policy recommendations directly inside SCM without a separate login.[194]
- **Push:** When you import a recommended policy, SCM automatically creates the necessary **Device Objects**, **Service Objects**, and **Address Objects** for you.
- **Log Forwarding:** Automated rules often *lack* a Log Forwarding Profile by default. You must manually attach one (or set a default) to ensure traffic is logged to Cortex Data Lake.[195]

4. Vulnerability Mitigation (Virtual Patching)

A critical "Manage and Configure" task is handling unpatchable IoT devices (e.g., an old Windows XP medical controller).

- **The Problem:** You cannot patch the device firmware.
- **The Solution:** Use the **IPS (Threat Prevention)** profile recommended by IoT Security. The system identifies the specific CVEs relevant to that device model and recommends a targeted IPS signature set to "virtually patch" it by blocking exploit attempts at the firewall level.[194]

Summary for NSP

- **Source:** Use **Device-ID** (not just Source IP).
- **Method:** Use **Import Policy** (don't write manually).
- **Enforcement:** Requires **Device-ID** enabled on the Zone.
- **Action:** Always **Allow** specific traffic and rely on the implicit "Deny All" (or a cleanup rule) to block anomalous behavior.

⁂

IOT Security Device-ID

The "IoT Security Device-ID" domain in the NSP exam focuses on how Palo Alto Networks firewalls move beyond IP addresses to identify and control devices based on their inherent characteristics (Model, Vendor, OS, Firmware).

1. What is Device-ID?

Device-ID is a feature (introduced in PAN-OS 10.0) that classifies devices based on metadata collected by the IoT Security service. It allows you to write policies like "Allow **MRI-Machines** to talk to **PACS-Server**" instead of managing a list of 500 changing IP addresses.[204]

2. Configuration Workflow (The Exam "Order of Operations")

To successfully enforce Device-ID policies, you must follow this exact sequence:

1. **License & Update:** Ensure the firewall has an IoT Security license and is running PAN-OS 10.0+.[205]
2. **Enable on Zone:** You must explicitly enable "Device Identification" on the **Source Zone** (e.g., your IoT VLAN zone).
   - *Path:* `Network > Zones > [Zone Name] > Enable Device Identification`.[206]
   - *Constraint:* Only enable this on internal zones (Trust, IoT), not the Internet/Untrust zone.
3. **Baseline Period:** The system needs time to learn. Best practice is to let it collect metadata for at least **14 days** before enforcing strict rules.[207] [205]
4. **Policy Creation:** Use the **Source Device** tab in your Security Policy.
   - You can select specific *Device Objects* (e.g., "Polycom Phone") or *Device Profiles* (groups of similar devices).

3. Device-ID vs. IP Precedence

The exam may test your understanding of how the firewall matches traffic when both Device-ID and IP are involved.

- **Device-ID is "Sticky":** Once a device is identified (e.g., IP 10.1.1.5 is a "Nest Thermostat"), that tag stays with the IP until the device goes offline or changes behavior.
- **Policy Match:** If you have a rule that says `Source Device: Nest-Thermostat` and another rule that says `Source IP: 10.1.1.0/24`, the firewall evaluates rules **top-down**.
- **The "Unknown" Gap:** If a device is new and not yet classified (Device-ID = "Unknown"), it will *skip* any rule requiring a specific Device-ID. You must have a "catch-all" rule below your Device-ID rules to handle (or block) unclassified devices.

4. Limitations & Troubleshooting

- **Visibility:** Device-ID relies on the firewall seeing the traffic. If the device is behind a NAT router *before* it hits the firewall, the firewall only sees the router's MAC/IP, breaking Device-ID accuracy. **Solution:** Use a TAP interface or DHCP Relay to forward original headers.[205]
- **Unsupported OS:** Device-ID works on *network behavior*, so it is OS-agnostic (works on Linux, Windows, RTOS, etc.) unlike User-ID which requires AD integration.

Summary Checklist

- **Enablement:** Per-Zone (Source only).
- **Policy Object:** Source Device (Device-ID).
- **Baseline:** 14-day learning period recommended.
- **Dependency:** Requires IoT Security License + Cloud Connection (Data Lake).

⁂

IOT Security Monitoring and logging

IoT Security relies entirely on the **telemetry** the firewall sends to the cloud. If you do not configure logging correctly, the IoT dashboard remains empty. The "Monitoring and Logging" domain for NSP tests your ability to set up this data pipeline and interpret the results.

1. Enhanced Application Logs (EAL)

Standard firewall logs (Traffic, Threat) are not enough for IoT profiling. You must enable **Enhanced Application Logs (EAL)**.

- **What is it?** EAL captures layer 7 payloads and protocol metadata (DHCP options, HTTP User-Agents, mDNS, SSDP) that uniquely identify a device.[219]
- **Configuration:**
  - **NSP "One-Click" Method:** In modern PAN-OS (10.0+), simply attach the **"IoT Security Default Profile"** to your Allow rules. This profile comes pre-configured with EAL enabled.[220] [221]
  - **Manual Method:** In a Log Forwarding Profile, you can manually check the box "Enable enhanced application logs in cloud logging".[219]

2. Log Forwarding to Cortex Data Lake (CDL)

All IoT analysis happens in the cloud. The firewall *must* forward logs to the **Cortex Data Lake**.

- **Requirement:** Your Log Forwarding Profile must target the CDL (Logging Service). If you only log locally or to a Syslog server, IoT Security will see nothing.[222]
- **Troubleshooting:**
  - **Command:** `request logging-service-forwarding status` verifies the connection to the cloud.[223]
  - **Counters:** `show counter global filter delta yes | match log` shows if logs are actually leaving the box [223].

3. Monitoring Dashboards (Strata Cloud Manager)

Once data is flowing, you use SCM to monitor three key areas:

- **Asset Distribution:** Shows the count of devices by Type (Camera, Pump, Sensor) and Profile (Hikvision, Siemens).
- **Risk Score:** A 0-100 score for each device.
  - *High Risk factors:* Default passwords, cleartext protocols (Telnet/HTTP), communication with Internet.[224]
- **Vulnerabilities:**
  - **CVE Matching:** The dashboard lists known CVEs affecting your specific device firmware.

- **Virtual Patching:** It shows which CVEs can be blocked by enabling specific Threat Prevention signatures.[224]

4. Third-Party Integrations

IoT Security can export data to other systems for broader visibility.

- **SIEM:** You can forward IoT alerts (e.g., "New Device Found", "Device Vulnerable") to a SIEM like Splunk or QRadar via Cortex Data Lake or XSOAR.
- **NAC:** Integration with ISE or ClearPass allows you to quarantine a device at the *switch port* level if IoT Security detects a high risk score.

Exam Tip: If the dashboard shows "Unknown" devices and no Model/Vendor info, the issue is almost always **missing EAL logs** (check Log Forwarding Profile) or **DHCP visibility** (need a TAP/Relay).

⁂

Configure Enterprise DLP and Enterprise SaaS Security

In the **NSP certification**, you are expected to know how to deploy **Enterprise DLP** and **SaaS Security Inline** (formerly CASB) as an integrated solution within **Strata Cloud Manager (SCM)**. These two services often work together: SaaS Security discovers the apps, and DLP inspects the data moving through them.

1. Enterprise DLP (E-DLP) Configuration

Enterprise DLP prevents sensitive data (PII, PCI, PHI) from leaving the network.

- **Key Concept:** E-DLP is a **cloud service**. The firewall extracts text from files/traffic, sends it to the DLP Cloud for analysis, and waits for a verdict (Block/Allow).[234]
- **Configuration Workflow in SCM:**
  1. **Data Profile:** Create a `Data Filtering Profile`.
     - **Classic vs. Granular:**
       - **Classic:** Applies one action (e.g., Block) to the entire profile.
       - **Granular:** Allows different actions for different data types within the same profile (e.g., *Alert* on "SSN" but *Block* on "Top Secret Project Name").[235]
  2. **DLP Rule:** Unlike other profiles, creating a Data Profile automatically creates a corresponding "DLP Rule" in the DLP tab. You must edit this rule to define the **Action** (Block/Alert).[236]
  3. **Security Policy:** You must attach this Data Profile to a **Security Profile Group**, and then attach that group to your **Security Policy Rule** (e.g., "Trust to Internet").
- **Prerequisite: SSL Decryption** is mandatory. If you cannot decrypt the HTTPS session, DLP cannot see the credit card numbers inside it.[237]

2. SaaS Security Inline (SSI)

SaaS Security Inline provides visibility into "Shadow IT" (unsanctioned apps) and enforces control over sanctioned apps.

- **Key Concept:** It uses the **App-ID Cloud Engine (ACE)** to instantly identify new SaaS apps without waiting for a monthly content update.[238]
- **Configuration in SCM:**
  1. **Activation:** Ensure the service is activated on your tenant.
  2. **ACE:** Enable "App-ID Cloud Engine" on the firewall.
     - *Warning:* Enabling ACE can change how traffic is classified. Traffic previously seen as generic `ssl` might suddenly be identified as `dropbox-upload`. You may need to update your security policies to avoid accidental blocks.[238]
  3. **HTTP Header Insertion:** To control "Tenant Restrictions" (e.g., Allow *Corporate* Office 365 but Block *Personal* Hotmail), configure **HTTP Header Insertion** in the **URL Filtering Profile**.
     - *Example:* Insert header `X-MS-Proxy` with value `Allowed-Domain=mycompany.com`.

3. Integrated Use Cases (NSP Scenarios)

The exam will present scenarios requiring both services:

Scenario	Solution
"Block Credit Card uploads to Personal Gmail"	1. **SaaS Security:** Use Header Insertion to block Personal Gmail login (best) OR use App-ID `gmail-upload`. 2. **DLP:** If Personal Gmail is allowed, attach a **DLP Profile** to the rule to block traffic matching the "Credit Card" pattern.
"Discover Shadow IT"	Enable **SaaS Security Inline** and ensure logs are forwarded to Cortex Data Lake. View the "SaaS Visibility" dashboard in SCM [239].
"Prevent Source Code Leak"	Create a custom **Data Pattern** (Regex) for your code headers in DLP. Attach to a policy allowing traffic to GitHub/GitLab [236].

Summary Checklist

- **DLP:** Requires Decryption + Data Filtering Profile + Security Policy.
- **SaaS Security:** Requires ACE (App-ID Cloud Engine) + Log Forwarding to CDL.
- **Management:** Both are fully managed in **Strata Cloud Manager** (SCM), often using shared objects.

⁂

Data Encription

In the context of the **Palo Alto Networks NSP** certification, "Data Encryption" typically refers to the **Decryption** (SSL/TLS) functionality. The exam views encryption as an "Infrastructure Prerequisite"—if you don't decrypt it, you can't inspect it with CDSS (DLP, Threat, etc.).

There are two primary modes of decryption you must master for the exam: **SSL Inbound Inspection** and **SSL Forward Proxy**.

1. SSL Inbound Inspection (Protecting Servers)

This mode decrypts traffic coming *from* the Internet *to* your internal servers (e.g., your DMZ web server).

- **Use Case:** Protecting your own web servers from inbound attacks (SQLi, XSS) hidden in HTTPS.
- **Infrastructure Requirement:** You must import the **Server's Private Key** and Certificate onto the firewall.
- **Mechanism:** Because the firewall holds the real private key, it can transparently decrypt the session without "Man-in-the-Middle" certificate warnings. It acts as the server to the client.
- **Exam Nuance:**
  - **HSM Support:** For high-security environments where the private key cannot leave a Hardware Security Module (HSM), the firewall acts as a client to the HSM to sign/decrypt without ever storing the key locally.[249]
  - **TLS 1.3:** Newer PAN-OS versions support TLS 1.3 for Inbound Inspection even with HSMs.[250]

2. SSL Forward Proxy (Protecting Users)

This mode decrypts traffic going *from* your internal users *to* the Internet.

- **Use Case:** Preventing users from downloading malware or uploading sensitive data (DLP) to external sites.
- **Infrastructure Requirement:**
  1. **Forward Trust Certificate (CA):** You must generate a CA certificate (either self-signed on the firewall or, better, a Sub-CA signed by your internal PKI).
  2. **Trust:** This CA certificate must be installed in the **Trusted Root Store** of every client machine (PC/Mac) in your organization.
- **Mechanism:** The firewall performs a "Man-in-the-Middle" (MitM). It intercepts the connection, presents a *fake* certificate signed by its Forward Trust CA to the client, and maintains a separate valid connection to the real server.[251]

3. Decryption Policy & Best Practices

For the NSP exam, you must know *what* to decrypt and *what not* to decrypt.

- **The "No Decrypt" List:**
  - **Legal/Compliance:** Do **not** decrypt sensitive categories like `Health-and-Medicine`, `Financial-Services`, or `Government` (unless explicitly authorized). Use a "No Decryption" rule for these URL categories.
  - **Technical Issues:** Some applications use **Certificate Pinning** (e.g., Dropbox client, Windows Update) and will break if decrypted. You must add these to the **SSL Decryption Exclusion List** (`Device > Certificate Management > SSL Decryption Exclusion`).[252]
- **Troubleshooting:**
  - **Exclude Cache:** If a site breaks, the firewall might automatically add it to the "Local Exclude Cache" for 12 hours. You can view this with `show system setting ssl-decrypt exclude-cache`.[252]
  - **Unsupported Ciphers:** If the firewall encounters a cipher it cannot handle (rare now), it will drop the connection unless your Decryption Profile is set to "Allow" for unsupported modes (not recommended).

4. Decryption Mirroring

- **Concept:** A feature often tested in "Infrastructure Management." It allows the firewall to send a copy of the *decrypted* traffic out a specific interface to a third-party tool (like a packet capture appliance or DLP solution) for forensic archiving. This is configured in the **Decryption Profile** under "Forwarding".

Summary Checklist

- **Inbound Inspection:** Needs Server Private Key.
- **Forward Proxy:** Needs Trusted CA on client.
- **Policy Order:** "No Decrypt" rules (Finance/Health) must be at the **top** of the policy.
- **DLP Dependency:** Enterprise DLP **requires** Forward Proxy decryption to function.

⁂

Enterprise DLP and Enterprise SaaS Security Access Control

In the Palo Alto Networks NSP curriculum, "Access Control" for **Enterprise DLP** and **SaaS Security** refers to the mechanisms used to allow, block, or limit user interactions with data and applications based on context (Tenant, Risk, Data Sensitivity).

These controls are often integrated directly into the **Strata Cloud Manager (SCM)** Security Policy workflow.

1. SaaS Security Inline Access Control

This service focuses on *which* applications users can access and *which instances* of those applications are permitted.

- **App-ID & Risk-Based Control:**
  - **Mechanism:** Uses the **App-ID Cloud Engine (ACE)** to dynamically identify thousands of SaaS apps.[264]
  - **Policy:** You can create rules that say "Block all apps with High Risk" or "Block apps that do not have SOC2 compliance" (using the SaaS Security filter in SCM).
- **Tenant Restrictions (The "Corporate Only" Rule):**
  - **Problem:** Users logging into *personal* Gmail or Dropbox accounts on corporate networks, bypassing DLP.
  - **Solution:** Configure **HTTP Header Insertion** in the URL Filtering Profile.
  - **How it works:** The firewall intercepts the HTTPS request (requires Decryption) and injects a header like `Restrict-Access-To-Tenants: mycompany.com`. The SaaS provider (e.g., Microsoft/Google) sees this header and blocks any login attempt to a non-corporate tenant.[265]
  - **NSP Exam Tip:** This is an "Inline" feature configured in URL Filtering, *not* an API feature.

2. Enterprise DLP Access Control

This service focuses on *what data* users can move.

- **Data Filtering Profiles:**
  - **Access Control Action:** The primary control is the **Action** within the Data Filtering Profile attached to your Security Rule.
  - **Actions:**
    - `Block`: Stops the file transfer immediately.
    - `Alert`: Allows transfer but logs the incident (for monitoring).
    - `Mask`: Allows transfer but replaces sensitive text (e.g., Credit Card #) with `X` characters in the logs (privacy control).[266]
- **Granular Context:**
  - **Upload vs. Download:** You can apply different profiles for different directions. For example, *Allow* downloading PII from the "HR-SaaS-App" but *Block* uploading PII to "Any-External-App".
  - **File Type Control:** DLP rules can be scoped to specific file types (e.g., "Block PDFs containing 'Confidential'").

3. Integrated Workflow in SCM

For the NSP exam, understand how these two work together in a single rule.

Policy Component	Access Control Function
Security Rule (App-ID)	"Allow only **Google-Drive** (Sanctioned App)."
URL Filtering (Profile)	"Enforce **Tenant Restriction** so users can only access the *Corporate* Google Drive instance."
Data Filtering (Profile)	"Block uploads of files containing **Credit Card Numbers** to this allowed instance."

4. API-Based Access Control (Out-of-Band)

While "Inline" controls traffic in real-time, **SaaS Security API** (CASB API) provides retroactive access control.

- **Use Case:** A user shared a sensitive file publicly *before* the DLP rule was created.
- **Action:** The API scans the SaaS cloud (e.g., Google Drive), finds the file with public permissions, and **revokes the sharing link** or quarantines the file automatically.[267]
- **Configuration:** This is configured under `SaaS Security API` settings, not in the firewall Security Policy.

Summary Checklist

- **Tenant Restrictions:** Uses **URL Filtering** (Header Insertion).
- **SaaS Blocking:** Uses **App-ID** (Risk categories).
- **Data Blocking:** Uses **Data Filtering Profile** (Enterprise DLP).
- **Prerequisite:** All these controls require **SSL Decryption** to function.

⁂

Enterprise DLP and Enterprise SaaS Security monitoring and logging

The "Monitoring and Logging" domain for Enterprise DLP and SaaS Security in the NSP exam focuses on verifying that the cloud services are receiving data and troubleshooting when they are not. Both services rely heavily on the **Strata Logging Service** (formerly Cortex Data Lake).

1. Enterprise DLP Logging

DLP incidents are not stored locally on the firewall in the same way as Traffic logs. They are generated by the DLP cloud service.

- **Log Type:** DLP events appear as **Data Filtering Logs**.
- **Key Fields:**

    - **Snippet:** A captured portion of the sensitive data (e.g., the specific Credit Card number that triggered the block).
    - **Masking:** By default, the snippet is *masked* (`XXXX-XXXX-XXXX-1234`) to protect privacy. You can configure "Unmasking" permissions for specific admin roles if forensic validation is needed.[279]
- **Troubleshooting Missing Logs:**
    - If you see "Allow" in Traffic logs but no DLP log:
        1. Verify **SSL Decryption** is working (DLP cannot see inside encrypted packets).
        2. Check the **Log Forwarding Profile** attached to the rule—it must forward "Data" logs to Cortex Data Lake.
        3. Verify the file size. DLP has file size limits (e.g., it may not scan files > 20MB depending on settings).

2. SaaS Security Inline Logging

SaaS Security uses firewall logs to discover applications.

- **Required Logs:** It primarily ingests **Traffic Logs** and **Enhanced Application Logs (EAL)**.
- **Identity Requirement:** SaaS Security relies on the `source_user_info` field. If your firewall is not correctly mapping User-IDs (seeing only IPs), the SaaS dashboard will show "Unknown User" or fail to attribute usage to departments.[280]
- **Admin Audit:** In Strata Cloud Manager, you can view **Admin Audit Logs** to see who changed a SaaS policy or overrode a risk score.[281]

3. Cortex Data Lake (CDL) Storage

- **Quota Management:** You must allocate storage quotas for different log types. If your "Data Filtering" quota is 0%, DLP logs will be dropped upon arrival at the cloud.[282]
- **Log Forwarding Status:**
    - Check connection: `request logging-service-forwarding status`.
    - If logs are queuing (buffered) on the firewall, it indicates a connectivity issue to CDL, which will cause a delay in SaaS visibility.

4. SIEM Integration

For the exam, remember that you generally do *not* forward logs directly from the firewall to Splunk for these services.

- **Path:** Firewall → Cortex Data Lake → **Log Forwarding App** (Cloud) → SIEM (Splunk/QRadar).
- **Format:** The preferred format for forwarding from CDL to SIEM is **LEEF** or **CEF**.[283]

Summary Checklist

- **DLP Log:** Look for **Data Filtering** logs (not Threat logs).
- **SaaS Visibility:** Requires **User-ID** to be working.
- **Masking:** DLP snippets are masked by default; requires admin privilege to view.
- **Storage:** Ensure CDL quota is allocated for "Data" logs.

⁂

Maintain and configure Strata Cloud Manager (SCM) and Panorama in network security environments

In the **Infrastructure Management** domain of the NSP exam, you are tested on managing the platform itself. The key theme is the transition from **Panorama** (legacy/on-prem) to **Strata Cloud Manager** (future/cloud-native).

1. Strata Cloud Manager (SCM) vs. Panorama

You must understand the architectural differences that affect day-to-day management.

Feature	Panorama (Traditional)	Strata Cloud Manager (SCM)
Hosting	On-prem VM or Hardware Appliance.	Cloud-Native Service (SaaS).
Config Structure	**Device Groups** (Policy) & **Templates** (Network).	**Folders** (Unified Network & Policy).
Inheritance	Template Stacks (Linear).	**Folder Hierarchy** (Tree-based: Global > Region > Site).
Variables	Template Variables (Network only).	**Snippet Variables** (Network *and* Security Policy) [294].
High Availability	Active/Passive (configured manually).	Built-in Cloud Redundancy (SLA-backed).

2. Migration: Panorama to SCM

The exam covers the migration workflow for customers moving to the cloud.

- **Tool:** You don't rebuild manually. You use the **Migration Tool** integrated into SCM.
- **Process:**
  1. **Export:** Save the Panorama running-config as XML.
  2. **Upload:** In SCM, navigate to `Manage > Configuration > NGFW` and upload the XML.
  3. **Validation:** The tool flags unsupported features (e.g., specific legacy VPN modes). You must resolve these "blockers" before proceeding.

4. **Cutover:** SCM pushes the converted config to the devices. The devices then disconnect from Panorama and connect to SCM.[295]

3. Onboarding Firewalls to SCM

To bring a new (or existing) firewall into SCM, you follow the "ZTP" (Zero Touch Provisioning) or manual onboarding flow.

- **Prerequisites:**
  - **License:** The firewall must have a valid SCM management license.
  - **Certificates:** The device needs a valid Device Certificate (OTP-based) to trust the cloud.
- **Connectivity:**
  - **Ports:** The firewall must be able to reach `*.paloaltonetworks.com` on TCP/443.
  - **Services:** You must configure **DNS** and **NTP** correctly; otherwise, the cloud handshake fails due to certificate time validation errors.[296]

4. Panorama High Availability (HA)

For on-prem scenarios, you still need to know Panorama HA.

- **Mode:** Typically **Active/Passive**. Only the Active peer pushes config.
- **Split-Brain Prevention:** Configuring the **Preemption** setting is critical.
  - *Best Practice:* If using NFS for logging, verify preemption settings carefully, as a failover might disrupt log writing if the mount isn't handled correctly.[297]
- **Path Monitoring:** You should configure Path Monitoring (ping upstream router) so Panorama can fail over if it loses network access, not just if the hardware dies.

Exam Tip: If asked about "Standardizing policy across 500 sites where the only difference is the internal subnet," the SCM answer is **"Use a Snippet with a Variable for the source subnet."** In Panorama, the answer would be "Template Variables," but SCM extends this power to security rules.

⁂

Strata Cloud Manager (SCM) and Panorama in network security environments supported products

In the **Infrastructure Management** domain, understanding *what* each management platform can control is critical for exam scenarios. As of 2026, the ecosystem is shifting heavily towards **Strata Cloud Manager (SCM)**, but **Panorama** remains vital for specific use cases.

1. Supported Products: SCM vs. Panorama

The NSP exam tests your ability to choose the right management plane based on the customer's fleet.

Product Category	Panorama (On-Prem/VM)	Strata Cloud Manager (Cloud-Native)
Hardware Firewalls (PA-Series)	**Yes.** Full support for all physical appliances (PA-400 to PA-7000).	**Yes.** Full support for modern PA-Series (requires PAN-OS 10.2+).
Virtual Firewalls (VM-Series)	**Yes.** Manages VMs in private/public clouds.	**Yes.** Manages VM-Series in AWS/Azure/GCP/Private.
Prisma Access (SASE)	**Yes.** (Via Cloud Services Plugin). *Legacy mode.*	**Yes. Primary platform.** Native integration with unified policy [309].
Prisma SD-WAN (CloudGenix)	**No.** Cannot manage SD-WAN appliances (ION).	**Yes.** Native management of Prisma SD-WAN (ION devices) [310].
Cloud-Delivered Security (CDSS)	**Yes.** Pushes profiles, but visibility is fragmented.	**Yes. Superior.** Integrated dashboards for AIOps, IoT, and SaaS Security [311].

2. Integration with Cortex & Operations

- **SCM:**
  - **AIOps:** Built-in. SCM natively includes "AIOps for NGFW" (Best Practice Assessment, Health Prediction) without extra appliances.[312]
  - **Unified Policy:** SCM allows you to write *one* security rule that applies to a physical firewall, a cloud VM, and a Prisma Access mobile user simultaneously. Panorama requires separate Device Groups for Prisma Access vs. NGFW in many legacy setups. [313]
- **Panorama:**
  - **Log Collection:** Requires **Cortex Data Lake** (cloud) OR **Dedicated Log Collectors** (on-prem M-Series/VM). SCM *only* supports Cortex Data Lake.
  - **Air-Gapped Networks:** Panorama is the *only* option for completely offline networks (government/defense) that cannot connect to the SCM cloud.

3. Exam Scenario: The "Hybrid" Trap

A common exam question involves a customer with **Prisma SD-WAN** and **PA-Series Firewalls**.

- **Question:** "Which platform provides a single pane of glass for both SD-WAN and Firewall security policies?"
- **Answer: Strata Cloud Manager**. Panorama cannot manage Prisma SD-WAN devices. SCM is the only unified answer.[310]

Summary Checklist

- **SD-WAN Management: SCM Only**.
- **Air-Gapped Management: Panorama Only**.
- **Prisma Access: SCM (Preferred)** / Panorama (Legacy Plugin).
- **Logs:** SCM requires **Cortex Data Lake**. Panorama supports local/NFS logging.

⁂

ION Devices

ION (Instant-On Network) devices are the dedicated hardware appliances for **Prisma SD-WAN**. In the NSP exam, you must distinguish them from PA-Series firewalls because they have different capabilities and management workflows.

1. Device Models & Roles

ION devices are specialized for "Application-Defined" routing, not just packet routing.

- **Branch Models:** ION 1200, 3200, 5200. These are deployed at remote sites to handle multiple WAN links (MPLS, LTE/5G, Broadband).[325]
- **Data Center Models:** ION 9000, 9200. These are high-throughput concentrators.
- **Virtual Models:** vION (available for AWS, Azure, GCP, ESXi).[325]
- **Key Distinction:** Unlike PA-Series firewalls which run PAN-OS, ION devices run specific **Prisma SD-WAN software**. However, newer integrated models (like ION 1200-S) and the "Prisma SASE" vision are converging these stacks.

2. Onboarding to Strata Cloud Manager (SCM)

Since ION devices are cloud-native, they *must* be managed by the cloud controller (SCM or the legacy Prisma SD-WAN portal).

- **Zero Touch Provisioning (ZTP):**
    1. **Claim:** You "claim" the device in the SCM portal using its Serial Number and Claim Key (found on the physical sticker).
    2. **Connect:** Plug the **Controller Port** (usually Port 1 or a dedicated mgmt port) into any internet-facing link (DHCP by default).
    3. **Phone Home:** The device calls home to `cloud-controller.paloaltonetworks.com`.
    4. **Assign:** You assign the device to a **Site** (e.g., "New York Branch") in SCM, which pushes the configuration.[326]

3. High Availability (HA)

ION HA differs from firewall HA.

- **Fail-to-Wire:** Many ION models (like ION 2000/3000) have physical "Bypass Pairs". If the device loses power, the relay closes and physically connects the WAN port to the LAN port, allowing traffic to flow (uninspected) to a backup router.
- **HA Groups:** In SCM, you configure two devices in an **HA Group**.
  - *Gen 1 Devices:* Use the **Control Port** for HA keepalives.
  - *Gen 2 Devices (NextGen):* Use a dedicated **HA Interface** (no longer need the control port).[327]

4. Comparison: ION vs. PA-Series (SD-WAN)

The exam often asks: "Which device should I position?"

Feature	Prisma SD-WAN (ION)	PA-Series (PAN-OS SD-WAN)
Routing Logic	**App-Defined.** Routes based on App Performance (SLA, jitter, packet loss).	**Packet-Based.** Routes based on L3/L4 headers + App-ID.
Security	**Lightweight.** Zone-based firewalling (ZBF). Needs Prisma Access for full security.	**Full NGFW.** Deep packet inspection, Threat Prevention, DLP on-box.
Management	**SCM Only.**	**Panorama or SCM.**
Use Case	Complex WANs (4+ links), heavy SaaS usage, "Thin Branch".	"Thick Branch" requiring on-prem security inspection.

NSP Tip: If a customer wants "Best-in-class application steering with automatic path correction for Zoom calls" but has a "Cloud-Heavy" security posture (SASE), position **ION Devices + Prisma Access**. If they need "On-prem inspection of East-West traffic" at the branch, position **PA-Series**.

⁂

Adding New Devices: Strata Cloud Manager vs. Panorama

The onboarding process differs significantly between the two platforms. **Panorama** relies on pre-staging serial numbers and auth keys, while **Strata Cloud Manager (SCM)** leverages cloud registration (ZTP) and OTPs.

1. Strata Cloud Manager (SCM) Onboarding

SCM creates a "Cloud-Native" relationship where the firewall reaches out to the cloud.

- **Method A: Zero Touch Provisioning (ZTP)**
  - **Ideal For:** Shipping unconfigured devices directly to a branch.

- **Requirements:** A ZTP-ready device (ZTP Mode enabled) and a "Claim Key" (found on the physical sticker or email).
- **Workflow:**
  1. **Register:** Log in to SCM/Hub, enter the **Serial Number** and **Claim Key** to "Claim" the device.
  2. **Connect:** Plug the management port (or ZTP port) into an internet-facing link (DHCP).
  3. **Bootstrap:** The device phones home to the ZTP service, validates its claim, and automatically downloads its initial config (including SCM connectivity settings).[340]

- **Method B: Manual Onboarding (Existing Devices)**
  - **Ideal For:** Brownfield deployments or non-ZTP hardware.
  - **Workflow:**
    1. **Device Association:** In SCM, go to `System Settings > Device Management` and associate the device Serial Number with your tenant.
    2. **Certificate:** Generate a **Device Certificate (OTP)** in SCM.
    3. **Firewall CLI:** Run the command `request scm-registration` with the OTP to register the device.
    4. **Folder Assignment:** Once connected, you must move the device from "Unmanaged" to a specific **Folder** (e.g., "Branch Office") to apply policy.[341]

2. Panorama Onboarding (Traditional)

Panorama relies on a "Server-Client" relationship where you must authorize the connection on both ends.

- **The "Auth Key" Requirement (PAN-OS 10.1+):**
  - Older versions only required the Serial Number. Modern versions **require** a **Device Registration Auth Key** for mutual authentication.
- **Workflow:**
  1. **Generate Key:** In Panorama, go to `Panorama > Device Registration Auth Key`. Create a key (you can limit it by count or lifetime).[342]
  2. **Add Device:** Go to `Panorama > Managed Devices > Summary` and add the device Serial Number.
  3. **Configure Firewall:** On the firewall, configure the Panorama Server IP. You *must* input the Auth Key during this setup (`set deviceconfig system panorama-server ... auth-key ...`).
  4. **Commit:** You must commit on Panorama *before* the device can successfully connect.
  5. **Association:** Once connected, you manually add the device to a **Device Group** (Policy) and **Template Stack** (Network).

3. Key Differences for the Exam

Feature	Strata Cloud Manager (SCM)	Panorama
Trust Anchor	**Claim Key** (Hardware) or **OTP** (Manual).	**Device Registration Auth Key** (Generated on Panorama).
Initial Config	**ZTP Service** pushes config automatically.	**Bootstrap USB** or Manual CLI config required for IP/Connectivity.
Organization	Device is placed in a **Folder**.	Device is placed in a **Device Group** AND **Template Stack**.
Pre-Staging	"Device Onboarding Rules" can auto-assign folders based on SN/Model.	Manual assignment after connection (unless scripting API is used).

Exam Tip: If a question asks how to onboard a fleet of 50 firewalls shipped directly to sites *without* pre-configuring IPs, the answer is **ZTP with Strata Cloud Manager**. If the question asks about adding a firewall to a secure, air-gapped management network, the answer involves **Panorama with a Device Registration Auth Key**.

⁂

Reporting in Strata Cloud Manager vs. Panorama

For the NSP exam, the key distinction is that **Panorama** reports are *database-centric* (querying local or log collector logs), while **Strata Cloud Manager (SCM)** reports are *dashboard-centric* (querying the Cortex Data Lake).

1. Strata Cloud Manager (SCM) Reporting

SCM focuses on "Insights" and "Dashboards" rather than the traditional static reports of Panorama.

- **Dashboards as Reports:** In SCM, you don't typically "generate a PDF report" in the old sense. Instead, you build a **Custom Dashboard** with widgets (e.g., "Top High-Risk Applications").
- **Export & Schedule:**
  - **PDF/CSV:** You can download a dashboard or a specific widget view as a PDF or CSV for offline sharing.
  - **Scheduled Email:** SCM allows you to schedule the delivery of these dashboard snapshots to specific email addresses (e.g., weekly executive summary).[355] [356]
- **Data Source:** All SCM reports query the **Strata Logging Service (Cortex Data Lake)**. SCM cannot report on logs stored on local firewalls.

2. Panorama Reporting

Panorama reporting is more traditional and granular, often used for compliance artifacts.

- **Predefined vs. Custom Reports:**
  - **Predefined:** Over 40 built-in reports (e.g., "Top 50 Users by Bandwidth").
  - **Custom:** You can build reports based on specific log databases (Traffic, Threat, URL).
  - *Constraint:* A custom report can only query **one log type** at a time (e.g., you can't mix Traffic and Threat logs in a single query table).[357]
- **Scheduled Reports:**
  - **Mechanism:** You check the "Scheduled" box in the report configuration.
  - **Email Server:** You must configure an Email Server Profile and associate it with a **Report Group** to send the output.[358]
  - **Strata Logging Service Integration:** If your logs are in the cloud (CDL), you must explicitly enable "Scheduled Reports on Strata Logging Service" via the Panorama CLI (`request plugins cloud_services logging-service sched-report-enable`).[358]

3. Exam Nuances

- **"User Activity Report" (UAR):** This is a specific report type in Panorama used to audit a single user's behavior. In SCM, this is replaced by the "User Activity" dashboard.
- **Drill-Down:** SCM reports are interactive (click a bar in a chart to filter logs). Panorama PDF reports are static.

Exam Tip: If a question asks how to provide a "Live, interactive view of network threats" to a CISO, the answer is **SCM Dashboard**. If it asks for a "Daily CSV export of all blocked sessions for compliance archiving," the answer is **Panorama Scheduled Report** (or SCM Scheduled Report depending on context, but Panorama is the traditional answer for CSV compliance dumps).

⁂

Configuration Management: Strata Cloud Manager (SCM) vs. Panorama

In the NSP exam, this domain tests your ability to operationalize the "write once, deploy many" philosophy. SCM introduces a new paradigm with **Folders**, **Snippets**, and **Variables**, moving away from Panorama's "Device Group/Template" model.

1. Configuration Hierarchy (Scope)

The way settings are organized and inherited differs fundamentally.

Feature	Panorama (Legacy)	Strata Cloud Manager (Modern)
Structure	**Dual-Stack:** Security is in **Device Groups**; Network is in **Templates**. They are separate trees.	**Unified Tree: Folders** contain *both* Network and Security settings [370].

Feature	Panorama (Legacy)	Strata Cloud Manager (Modern)
Inheritance	Linear Stacks. Child Device Groups inherit from Parent.	Tree Hierarchy. **Global** > **Region** > **Site** > **Device**. Max depth of 4 folders [371].
Overrides	"Override" at the device level (often messy).	"Variable" based overrides (cleaner) or Folder-level overrides.

2. Snippets (The "Modular" Config)

Snippets are a unique SCM feature often tested.

- **What they are:** Small, reusable blocks of configuration (e.g., "Standard Office 365 Rules" or "Guest Wi-Fi Setup").
- **How they work:** Unlike folders (where inheritance is automatic), a Snippet must be **explicitly attached** to a Folder, Deployment, or Device.
- **Flexibility:** You can attach the same Snippet to multiple unrelated folders (e.g., "West Coast" and "East Coast" folders both use the "Global DNS" snippet).[372]
- **Variables in Snippets:** You can define a variable (e.g., `$DNS_SERVER`) inside a snippet. Each folder/device that uses the snippet can provide its own value for that variable.[373]

3. Variables (Standardization)

Variables allow you to standardize policy while localizing values.

- **Syntax:** Variable names must start with ** ∗ ∗ (e.g.,\INTERNAL_SUBNET`).
- **Use Case:** You write *one* Security Rule: `Source: $INTERNAL_SUBNET, Dest: Any, Action: Allow`.
  - In the "London" folder, you define `$INTERNAL_SUBNET = 10.1.0.0/16`.
  - In the "New York" folder, you define `$INTERNAL_SUBNET = 10.2.0.0/16`.
- **CSV Import:** You can bulk-import variable values via CSV to configure hundreds of sites quickly.[373]

4. Audit & Compliance

- **Config Audit:** SCM provides a **"Show Config Diff"** feature to detect "Drift." It compares the SCM-defined config against the firewall's local state. If a local admin made changes via CLI, SCM flags them as **Conflicts**.[374]
- **Audit Logs:** SCM tracks *who* changed *what* in the `Manage > Configuration > Audit Logs` view. This is critical for compliance (SOC2/PCI).[375]

Exam Tip: If a question asks, "How do you apply a standard set of security rules to five specific firewalls that are in different folders?" the answer is **"Create a Snippet containing the rules and attach it to each of the five firewalls (or their folders)."** You cannot do this with Folder inheritance alone if the folders are siblings.

⁂

1. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
2. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/onboard-to-strata-cloud-manager
3. https://docs.paloaltonetworks.com/ngfw/networking/networking/configure-service-routes
4. https://www.wiresandwi.fi/blog/palo-alto-firewalls-working-with-service-routes
5. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/validate-strata-cloud-manager-onboarding
6. https://www.globalknowledge.com/es-es/products/palo_alto_networks/pan-cnsp
7. https://www.mbtechtalker.com/unlocking-the-power-of-palo-alto-networks-cloud-delivered-security-services/
8. https://www.youtube.com/watch?v=2VES4GECQdc
9. https://datacipher.net/palo-alto-network-security-professional-certification-guide-2025/
10. https://slashdot.org/software/p/Palo-Alto-Networks-Cloud-Delivered-Security-Services/
11. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/getting-started/insights-scm/cdss-adoption
12. https://www.sunsetlearning.com/certification-tracks/palo-alto-certifications/
13. https://tei.forrester.com/go/paloalto/CDSS/
14. https://www.cbtnuggets.com/blog/training/certification-paths/a-complete-palo-alto-certification-guide
15. https://www.paloguard.com/products.asp
16. https://www.uninets.com/blog/network-security-generalist-certification-guide
17. https://www.youtube.com/watch?v=CnAXJ770yHs
18. https://www.youtube.com/watch?v=YnYDOAQgPpQ
19. https://www.pass4success.com/palo-alto-networks/exam/netsec-generalist
20. https://www.youtube.com/watch?v=KVEBpdGZxrc
21. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/service-routes/configure-service-routes
22. https://www.dumpspedia.com/palo-alto-networks-systems-engineer-professional-hardware-firewall-dumps.html
23. https://www.youtube.com/watch?v=o0_PE-YGaEE
24. https://www.paloaltonetworks.com/services/education/certification
25. https://www.paloaltonetworks.com/services/education/palo-alto-networks-netsec-professional
26. https://www.nwexam.com/palo-alto/palo-alto-netsec-pro-certification-exam-syllabus
27. https://www.paloaltonetworks.com.br/network-security/strengthen-your-network-security-foundation
28. https://www.passquestion.com/news/NetSec-Generalist-PaloAlto-Networks-Network-Security-Generalist-Exam-Questions.html
29. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
30. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/configuration-overview/variables

31. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/configuration-overview/snippets
32. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PP1RCAW
33. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oMCYCA2
34. https://docs.paloaltonetworks.com/content/techdocs/en_US/dns-security/administration/configure-dns-security/test-connectivity-to-the-dns-security-service
35. https://github.com/PacktPublishing/Mastering-Palo-Alto-Networks/blob/master/chapter 13 - CLI cheat sheet
36. https://docs.paloaltonetworks.com/vm-series/11-0/vm-series-deployment/license-the-vm-series-firewall/vm-series-models/activate-the-license/troubleshoot-license-activation-issues
37. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/getting-started/insights-scm/cdss-adoption
38. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking
39. https://orhanergun.net/top-10-palo-alto-cli-commands-you-need-to-know
40. https://bluecatnetworks.com/blog/palo-alto-networks-cli-tips/
41. https://aicybernetworx.co.uk/2018/05/30/palo-alto-useful-commands/
42. https://www.scribd.com/document/839154028/CLI-Command-Reference
43. https://media.paloaltonetworks.com/documents/4.1-cnse-study-guide.pdf
44. https://www.exam-labs.com/blog/understanding-bpdu-guard-a-vital-network-security-feature
45. https://www.thenetworkdna.com/2025/08/ccna-basics-what-is-bpdu-guard.html
46. https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/configure-packet-based-attack-protection
47. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/configure-interfaces/layer-2-interfaces/manage-per-vlan-spanning-tree-pvst-bpdu-rewrite
48. https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dos-protection
49. https://networkjourney.com/mastering-portfast-bpdu-guard-loop-guard-stp-protection-techniques-explained-with-lab-cli-ccnp-enterprise/
50. https://documentation.extremenetworks.com/exos_31.5/GUID-F3DB0AEB-9E38-480A-B316-169B1446208F.shtml
51. https://www.firewall.cx/cisco/cisco-switches/spanning-tree-protocol-bpdu-guard-deployment-configuration.html
52. https://www.youtube.com/watch?v=TNMCCSgwWL4
53. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-groups
54. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions
55. https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-deployment-best-practices/advanced-wildfire-best-practices
56. https://docs.paloaltonetworks.com/advanced-wildfire/administration/configure-advanced-wildfire-analysis/forward-files-for-advanced-wildfire-analysis
57. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-profiles

58. https://xsoar.pan.dev/docs/reference/playbooks/pan-os---configure-dns-sinkhole
59. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/configure-dns-sinkholing
60. https://docs.paloaltonetworks.com/enterprise-dlp/activation-and-onboarding/enable-enterprise-dlp
61. https://docs.paloaltonetworks.com/saas-security/activation-and-onboarding/activate-saas-security-inline-ngfw
62. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/threat-prevention-resources
63. https://docs.paloaltonetworks.com/best-practices
64. https://docs.paloaltonetworks.com/advanced-threat-prevention
65. https://www.paloaltonetworks.com.br/resources/video/advanced-threat-prevention
66. https://docs.paloaltonetworks.com/ngfw/administration/monitoring
67. https://www.paloaltonetworks.com.br/network-security/advanced-threat-prevention
68. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/configuring-url-filtering/url-filtering-best-practices
69. https://docs.paloaltonetworks.com/saas-security/data-security/monitor-saas-security-api-issues/monitor-app-health-in-data-security
70. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/about-advanced-threat-prevention
71. https://docs.paloaltonetworks.com/content/techdocs/en_US/enterprise-dlp/administration/configure-enterprise-dlp
72. https://docs.paloaltonetworks.com/enterprise-dlp/activation-and-onboarding/setup-prerequisites-for-enterprise-dlp
73. https://www.nightfall.ai/blog/palo-alto-networks-dlp-comprehensive-analysis-and-top-alternatives
74. https://www.scribd.com/document/686002504/enterprise-dlp-admin
75. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/endpoint-dlp/troubleshoot-endpoint-dlp
76. https://www.reddit.com/r/paloaltonetworks/comments/wurwti/configuring_palo_alto_as_an_inline_transparent/
77. https://www.youtube.com/watch?v=6fcEollYzYw
78. https://docs.paloaltonetworks.com/saas-security/getting-started/get-started-with-saas-security-inline
79. https://www.youtube.com/watch?v=mdZ847In8Fc
80. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000g1Z5CAI&lang=en_US
81. https://www.youtube.com/watch?v=_PFoPk_lRo0
82. https://xsoar.pan.dev/docs/reference/integrations/palo-alto-networks-enterprise-dlp
83. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm
84. https://cciedump.spoto.net/palo-alto-certified-network-security-analyst-dumps.php
85. https://www.linkedin.com/posts/singhpriya11_palo-alto-security-policies-interzone-activity-7295293102410362880-mEsl
86. https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-device-groups/manage-precedence-of-inherited-objects
87. https://pan.dev/strata-cloud-manager/

88. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices
89. https://kb.wisc.edu/security/90963
90. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/security-posture/security-posture-settings
91. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/security-services
92. https://www.youtube.com/watch?v=J-58RtoTeAw
93. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
94. https://www.nwexam.com/palo-alto/palo-alto-netsec-pro-certification-exam-sample-questions-and-answers
95. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITHCA0
96. https://dependencyhell.net/2024/introduction-to-strata-cloud-manager-part-i
97. https://techdocs.broadcom.com/gr/el/vmware-sde/velocloud-sase/vmware-velocloud-sd-wan/5-3/palo-alto-networks-strata-cloud-manager-configuration.html
98. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-policy
99. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/recommendations-for-security-rules
100. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-anti-spyware
101. https://www.msp-channel.com/news/64067/palo-alto-networks-strengthens-saas-protection
102. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/cloud-delivered-security-services
103. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
104. https://docs.paloaltonetworks.com/cloud-ngfw/azure/cloud-ngfw-for-azure/strata-cloud-manager-policy-management
105. https://www.reddit.com/r/paloaltonetworks/comments/1g6iyr0/apply_dlp_rules_to_specific_saas_applications/
106. https://docs.paloaltonetworks.com/content/techdocs/en_US/cloud-ngfw-azure/administration/protect-traffic-with-cloud-ngfw-for-azure
107. https://www.reddit.com/r/paloaltonetworks/comments/1bc99b3/antispyware_profile_strict_vs_sinkhole_dns/
108. https://www.msspalert.com/news/palo-alto-networks-unveils-saas-security-posture-management
109. https://www.co-next.eu/protect-against-modern-threats-with-palo-alto-networks-cloud-delivered-security-services/
110. https://docs.paloaltonetworks.com/ngfw/help/10-2/policies/policies-security/security-policy-overview
111. https://www.optiv.com/insights/discover/blog/natively-integrated-security-palo-alto-networks-ecosystems-cloud-delivered
112. https://www.paloaltonetworks.fr/cyberpedia/nist
113. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/policy/security-profiles

114. https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Advanced-Threat-Prevention-Engine-Settings.htm?TocPath=Appliance+Configuration|Managing+Threat+Prevention|____5
115. https://docs.paloaltonetworks.com/advanced-wildfire/administration/advanced-wildfire-deployment-best-practices/advanced-wildfire-best-practices
116. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-profiles
117. https://docs.paloaltonetworks.com/content/techdocs/en_US/enterprise-dlp/administration/configure-enterprise-dlp/create-an-enterprise-dlp-data-profile/create-a-data-profile/create-a-data-profile-panorama
118. https://www.reddit.com/r/paloaltonetworks/comments/1bc99b3/antispyware_profile_strict_vs_sinkhole_dns/
119. https://www.youtube.com/watch?v=i_XDvTi-qsk
120. https://help.comodo.com/topic-451-1-939-12857-manage-advanced-threat-protection-profiles.html
121. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/configuring-url-filtering/configure-url-filtering
122. https://www.youtube.com/watch?v=odsrR-cCnM0
123. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-wildfire
124. https://www.scribd.com/document/686002504/enterprise-dlp-admin
125. https://www.optiv.com/insights/discover/blog/natively-integrated-security-palo-alto-networks-ecosystems-cloud-delivered
126. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/cloud-delivered-security-services
127. https://docs.paloaltonetworks.com/best-practices
128. https://live.paloaltonetworks.com/t5/community-blogs/zero-trust-based-cloud-applications-and-its-data-access-control/ba-p/587156
129. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTaCAK
130. https://www.linkedin.com/posts/rajeshkumar-d_the-choice-between-using-a-deny-reset-both-activity-7255271637506301952-COs0
131. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-vulnerability-protection
132. https://www.reddit.com/r/paloaltonetworks/comments/jsrjzd/security_action_drop_vs_reset_both/
133. https://kb.wisc.edu/security/90962
134. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/security-policy/security-policy-actions
135. https://www.examtopics.com/discussions/palo-alto-networks/view/109318-exam-pcnsa-topic-1-question-349-discussion/
136. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-rules
137. https://robertheaton.com/2020/04/27/how-does-a-tcp-reset-attack-work/
138. https://docs.oracle.com/cd/E56061_01/docs.101/E55884_rev_2.pdf
139. https://community.fortinet.com/t5/Fortinet-Forum/What-s-the-difference-between-reset-drop/m-p/42027

140. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HCCKCA4&lang=en_US
141. https://www.youtube.com/watch?v=WaZXOEqjvjY
142. https://www.examtopics.com/discussions/palo-alto-networks/view/97783-exam-pcnsa-topic-1-question-292-discussion/
143. https://en.wikipedia.org/wiki/TCP_reset_attack
144. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/best-practices-for-app-and-threat-content-updates/best-practices-security-first
145. https://community.indeni.com/t/content-update-schedule-is-not-following-best-practices-paloaltonetworks-panos/3477
146. https://www.packtpub.com/en-IN/product/mastering-palo-alto-networks-9781803241418/chapter/setting-up-a-new-device-2/section/adding-licenses-and-setting-up-dynamic-updates-ch02lvl1sec11
147. https://docs.paloaltonetworks.com/content/techdocs/en_US/ngfw/getting-started/manage-your-ngfws/upgrade-cloud-managed-ngfws
148. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClyDCAS
149. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000sYieCAE&lang=en_US
150. https://www.youtube.com/watch?v=QAvlGeDOjmM
151. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/software-and-content-updates/app-and-threat-content-updates/configure-app-threat-updates
152. https://community.indeni.com/t/wildfire-content-update-schedule-is-not-following-best-practices-paloaltonetworks-panos/3479
153. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/app-and-threat-content-updates
154. https://bluecatnetworks.com/blog/palo-alto-networks-best-practice-compliance-with-indeni/
155. https://docs.paloaltonetworks.com/content/techdocs/en_US/network-security/security-policy/administration/objects/schedules/add-a-schedule-cm
156. https://live.paloaltonetworks.com/t5/next-generation-firewall/best-practices-for-dynamic-updates/td-p/508360
157. https://www.paloaltonetworks.com/cyberpedia/firewall-best-practices
158. https://www.reddit.com/r/paloaltonetworks/comments/1d3d7v4/best_practice_for_dynamic_content_updates_between/
159. https://www.b-secure.co/hubfs/5-best-IoT-security-solutions.pdf
160. https://docs.paloaltonetworks.com/iot/getting-started/firewall-deployment-for-device-visibility/use-a-tap-interface-for-dhcp-visibility
161. https://docs.paloaltonetworks.com/content/techdocs/en_US/iot/getting-started/firewall-deployment-for-device-visibility/firewall-deployment-options-for-iot-security
162. 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
163. https://docs.paloaltonetworks.com/iot/administration/detect-iot-device-vulnerabilities/iot-risk-assessment
164. https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

165. https://docs.paloaltonetworks.com/content/techdocs/en_US/iot/enterprise-administration/onboard-enterprise-iot-security
166. https://www.youtube.com/watch?v=ZmvdCxxJ3S8
167. https://docs.paloaltonetworks.com/iot/iot-security-admin/recommend-security-policies/policy-rule-recommendations
168. https://www.firewalls.com/pub/media/wysiwyg/datasheets/PaloAlto/iot-security.pdf
169. https://www.paloaltonetworks.lat/cyberpedia/runtime-security
170. https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise
171. https://docs.paloaltonetworks.com/iot/administration/configure-iot-networks
172. https://docs.paloaltonetworks.com/content/techdocs/en_US/best-practices/security-lifecycle-review-getting-started/getting-started/updates
173. https://www.paloaltonetworks.de/cyberpedia/cloud-security-glossary-faqs
174. https://docs.paloaltonetworks.com/ngfw/networking/configure-interfaces/tap-interfaces
175. https://docs.paloaltonetworks.com/iot/getting-started/firewall-deployment-for-device-visibility/use-a-tap-interface-for-dhcp-visibility
176. https://www.youtube.com/watch?v=hyWIQYSJPYo
177. https://docs.paloaltonetworks.com/network-security/decryption/administration/enabling-decryption/configure-ssl-inbound-inspection
178. https://insights.profitap.com/tap-vs-span
179. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClMzCAK
180. https://www.reddit.com/r/paloaltonetworks/comments/1aem3mj/limitation_of_tap_interface/
181. https://docs.paloaltonetworks.com/content/techdocs/en_US/iot/getting-started/firewall-deployment-for-device-visibility/firewall-deployment-options-for-iot-security
182. https://cdn.studio.f5.com/files/k6fem79d/production/31509ed23540571d848ebef744698aa50ec3bab9.pdf
183. https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-security-zones-creation-and-configuration.html
184. https://www.networkcomputing.com/network-infrastructure/span-port-vs-tap-the-latency-impact
185. https://www.reddit.com/r/networking/comments/4xfww6/palo_alto_vm_in_tap_mode_for_application/
186. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/configure-interfaces/tap-interfaces
187. https://www.youtube.com/watch?v=jFGaVUBkIF0
188. https://www.youtube.com/watch?v=p68n6HZGqPY
189. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-id/device-id-overview
190. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-id/configure-device-id
191. https://docs.paloaltonetworks.com/iot/iot-security-admin/recommend-security-policies/policy-rule-recommendations
192. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/iot-security-features/iot-security-policy-rule-recommendation-enhancements
193. https://docs.paloaltonetworks.com/iot/administration/recommend-security-policies/import-a-policy-set-into-panorama

194. https://live.paloaltonetworks.com/t5/community-blogs/streamlined-security-fully-integrated-iot-security-in-strata/ba-p/1230760
195. https://docs.paloaltonetworks.com/iot/getting-started/prepare-your-firewall-for-iot-security
196. https://www.reddit.com/r/paloaltonetworks/comments/1m383wn/iot_security_policies_in_scm/
197. https://docs.paloaltonetworks.com/whats-new/new-features/november-2023/enhanced-iot-policy-recommendation-workflow-for-strata-cloud-manager
198. https://paloaltofirewalls.co.uk/subscriptions/internet-of-things-iot-security/
199. https://www.paloguard.com.au/datasheets/strata-cloud-manager.pdf
200. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rule-best-practices
201. https://pan.dev
202. https://www.paloaltonetworks.com/cyberpedia/how-to-secure-iot-devices-in-the-enterprise
203. https://www.youtube.com/watch?v=sEmdB6cZ6IY
204. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-id/configure-device-id
205. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/device-id/device-id-overview
206. https://docs.paloaltonetworks.com/network-security/device-id/administration/configure-device-id
207. https://docs.paloaltonetworks.com/network-security/device-id/administration/device-id-overview
208. https://www.cbtnuggets.com/blog/technology/networking/configuring-user-id-in-palo-alto-firewall-a-guide
209. https://help.ivanti.com/ps/help/en_US/IPS/22.x/ag/configuring_palo_alto_networks_firewall.htm
210. https://live.paloaltonetworks.com/t5/general-topics/order-of-preference-of-source-for-user-and-ip-mapping/td-p/220860
211. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000Cr9GCAS&lang=en_US
212. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CljLCAS
213. https://networkdevicesinc.com/community/blog/palo-alto-firewall-configuration-guide
214. https://docs.paloaltonetworks.com/network-security/device-id/administration/prepare-to-deploy-device-id
215. https://docs.paloaltonetworks.com/network-security/device-id/administration/manage-device-id
216. https://docs.paloaltonetworks.com/content/techdocs/en_US/cloud-identity/cloud-identity-engine-getting-started/manage-the-cloud-identity-engine/configure-third-party-device-id
217. https://www.reddit.com/r/paloaltonetworks/comments/tx557n/user_id_to_ip_mapping_stopped_or_intermittent/
218. https://www.paloaltonetworks.com.br/cyberpedia/how-to-secure-iot-devices-in-the-enterprise
219. https://docs.paloaltonetworks.com/iot/getting-started/prepare-your-firewall-for-iot-security
220. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/subscriptions/enhanced-application-logs
221. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-new-features/iot-security-features/simplified-iot-security-onboarding
222. https://docs.paloaltonetworks.com/iot/iot-security-admin/iot-security-overview/iot-security-integration-with-next-generation-firewalls
223. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CqrRCAS

224. https://www.youtube.com/watch?v=sEmdB6cZ6IY
225. https://live.paloaltonetworks.com/t5/community-blogs/streamlined-security-fully-integrated-iot-security-in-strata/ba-p/1230760
226. https://appairium.com/en/tools/palo-alto-networks-iot-ot-security
227. https://github.com/PaloAltoNetworks/panos-logging-skillets/blob/master/cortex_iot_config_helpers/dhcp_move_server_to_relay/README.md
228. https://www.youtube.com/watch?v=UlsYmgxRGoI
229. https://aws.amazon.com/blogs/machine-learning/how-palo-alto-networks-enhanced-device-security-infra-log-analysis-with-amazon-bedrock/
230. https://docs.rapid7.com/insightidr/palo-alto-cortex-data-lake/
231. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/subscriptions/enhanced-application-logs
232. https://docs.paloaltonetworks.com/content/techdocs/en_US/iot/getting-started/firewall-deployment-for-device-visibility
233. https://www.paloaltonetworks.com.br/cyberpedia/firewall-best-practices
234. https://www.paloguard.com/SaaS-Security.asp
235. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/create-an-enterprise-dlp-data-profile
236. https://www.scribd.com/document/856722268/Enterprise-Dlp-Administration-1
237. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-enterprise-dlp
238. https://docs.paloaltonetworks.com/saas-security/activation-and-onboarding/activate-saas-security-inline-on-prisma-access
239. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-saas-security
240. https://www.scribd.com/document/686002504/enterprise-dlp-admin
241. https://appomni.com/learn/saas-security-fundamentals/
242. https://www.youtube.com/watch?v=6fcEoIlYzYw
243. https://www.youtube.com/watch?v=oh4ck37yi14
244. https://www.docontrol.io/blog/how-is-saas-dlp-different-from-traditional-dlp
245. https://www.paloguard.com/strata-cloud-manager.asp
246. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/modify-a-dlp-rule-on-prisma-access-cloud-managed
247. https://www.reddit.com/r/paloaltonetworks/comments/1g6iyr0/apply_dlp_rules_to_specific_saas_applications/
248. https://www.youtube.com/watch?v=ClDQmabhEzc
249. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/certificate-management/secure-keys-with-a-hardware-security-module
250. https://docs.paloaltonetworks.com/whats-new/new-features/may-2024/tlsv1-3-support-for-hsm-integration-inbound-inspection-decryption
251. https://www.youtube.com/watch?v=Y8O_QyqZ1Oc
252. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/decryption-exclusions/local-ssl-decryption-exclusion-cache

253. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/decryption-concepts/ssl-inbound-inspection
254. https://docs.paloaltonetworks.com/network-security/decryption/administration/enabling-decryption/configure-ssl-inbound-inspection
255. https://www.youtube.com/watch?v=IA0YxpO4g9g
256. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/configure-ssl-inbound-inspection
257. https://www.reddit.com/r/paloaltonetworks/comments/1iwblc6/ssl_decryption_stopped_working/
258. https://www.examcollection.com/palo-alto-networks_exams.html
259. https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment
260. https://www.examtopics.com/discussions/palo-alto-networks/view/67495-exam-pcnse-topic-1-question-191-discussion/
261. https://www.paloaltonetworks.com/resources/webcasts/ssl-decryption-best-practices-deep-dive
262. https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices
263. https://www.reddit.com/r/paloaltonetworks/comments/1igtqi7/ssl_decryption_implementation_suggestions/
264. https://docs.paloaltonetworks.com/saas-security/getting-started/whats-saas-security/whats-saas-security-inline
265. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/tenant-restrictions
266. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-data-filtering
267. https://www.paloguard.com/SaaS-Security.asp
268. https://live.paloaltonetworks.com/t5/community-blogs/ocr-for-enterprise-dlp-and-saas-security-api/ba-p/515593
269. https://docs.azure.cn/en-us/entra/identity/enterprise-apps/tenant-restrictions
270. https://www.cyberhaven.com/guides/top-cloud-access-security-broker-casb-software-products-vendors-solutions
271. https://docs.paloaltonetworks.com/enterprise-dlp/administration/configure-enterprise-dlp/create-an-enterprise-dlp-data-profile
272. https://docs.paloaltonetworks.com/saas-security/getting-started
273. https://www.paloguard.com/Data-Loss-Prevention.asp
274. https://www.paloaltonetworks.com/sase/saas-security
275. https://www.nightfall.ai/blog/palo-alto-networks-dlp-comprehensive-analysis-and-top-alternatives
276. https://www.paloaltonetworks.com/sase/enterprise-data-loss-prevention
277. https://www.taloflow.ai/guides/comparisons/opensystemssase-vs-paloaltosse-sse
278. https://docs.paloaltonetworks.com/network-security/security-policy/administration/internet-access-rules/create-an-internet-access-policy-rule/create-an-internet-access-policy-rule-cloud-management
279. https://www.scribd.com/document/686002504/enterprise-dlp-admin
280. https://docs.paloaltonetworks.com/saas-security/getting-started/get-started-with-saas-security-inline/connect-saas-security-inline-and-strata-logging-service

281. https://docs.paloaltonetworks.com/saas-security/getting-started/get-started-with-saas-security-inline/manage-saas-security-inline-administrators
282. https://www.youtube.com/watch?v=htx9Gll4TAw
283. https://www.ibm.com/docs/en/dsm?topic=panps-forwarding-palo-alto-cortex-data-lake-next-generation-firewall-leef-events-qradar
284. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/monitoring/configure-log-forwarding
285. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000g1Z5CAI&lang=en_US
286. https://www.webspy.com/getting-started/paloalto/
287. https://learn.microsoft.com/en-us/troubleshoot/microsoft-365/purview/data-loss-prevention/analyze-endpoint-dlp-diagnostic-logs
288. https://docs.solo.io/gloo-edge/latest/guides/security/data_loss_prevention/
289. https://docs.rapid7.com/insightidr/palo-alto-cortex-data-lake/
290. https://docs.paloaltonetworks.com/cortex/cortex-data-lake/log-forwarding-schema-reference/network-logs/network-traffic-log/network-traffic-syslog-fields
291. https://live.paloaltonetworks.com/t5/community-blogs/new-cortex-data-lake-features-log-forwarding-amp-more/ba-p/361172
292. https://www.paloaltonetworks.com/network-security/strata-logging-service
293. https://www.paloguard.com.au/Cortex-Data-Lake.php
294. https://dependencyhell.net/2024/introduction-to-strata-cloud-manager-part-i
295. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/migrate-from-panorama-to-strata-cloud-manager
296. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/onboard-to-strata-cloud-manager
297. https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-high-availability/manage-a-panorama-ha-pair/set-up-ha-on-panorama
298. https://docs.defenseorchestrator.com/t-troubleshoot-device-connectivity-with-SDC.html
299. https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-high-availability
300. https://www.scribd.com/document/896583062/Strata-Cloud-Manager-AIOps
301. https://www.youtube.com/watch?v=KVEBpdGZxrc
302. https://www.coursehero.com/file/p7clmgm7e/Only-Ethernet-11-is-supported-to-successfully-onboard-a-ZTP-firewall-to/
303. https://support.controlant.com/en/20956-37768-scm-app---troubleshooting.html
304. https://docs.paloaltonetworks.com/compatibility-matrix/reference/feature-parity
305. https://www.reddit.com/r/paloaltonetworks/comments/1bnfo33/strata_cloud_manager_vs_panorama/
306. https://www.youtube.com/watch?v=nZsqKe4MqOY
307. https://www.reddit.com/r/paloaltonetworks/comments/1b8147l/strata_cloud_manager_vs_panorama/
308. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/migrate-prisma-access-from-panorama-to-strata-cloud-manager
309. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/migrate-prisma-access-from-panorama-to-strata-cloud-manager
310. https://www.youtube.com/watch?v=ClDQmabhEzc

311. https://dependencyhell.net/2024/introduction-to-strata-cloud-manager-part-i
312. https://www.scribd.com/document/896583062/Strata-Cloud-Manager-AIOps
313. https://docs.paloaltonetworks.com/prisma-access/administration/monitor/view-and-monitor-prisma-access-in-strata-cloud-manager
314. https://docs.paloaltonetworks.com/whats-new/new-features/november-2024/scm-config-apis-ngfw-platforms
315. https://securitybrief.asia/story/palo-alto-networks-launches-new-sd-wan-solutions-and-enhancements
316. https://www.netscout.com/technology-partners/palo-alto-networks/cortex-xsoar
317. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-january-2026
318. https://www.paloguard.com/CloudGenix-SD-WAN.asp
319. https://xmcyber.com/press-release/xm-cyber-announces-integration-with-palo-alto-networks-cortex-xsoar/
320. https://www.youtube.com/watch?v=5nxt7R9d-YI
321. https://www.reddit.com/r/paloaltonetworks/comments/1bnfo33/strata_cloud_manager_vs_panorama/
322. https://docs.paloaltonetworks.com/compatibility-matrix/reference/feature-parity
323. https://live.paloaltonetworks.com/t5/panorama-discussions/panorama-to-strata-cloud-manager-anyone-using-in-production/td-p/628007
324. https://studyx.ai/questions/4llo99y/the-security-engineer-asks-about-key-differences-between-strata-cloud-manager-and
325. https://docs.paloaltonetworks.com/compatibility-matrix/reference/prisma-sd-wan-compatibility-matrix
326. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-devices/connect-the-ion
327. https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-branch-high-availability/configure-control-interface-for-management-services-in-ha-setup
328. https://live.paloaltonetworks.com/t5/prisma-sd-wan-discussions/palo-alto-sd-wan-vs-prisma-sd-wan/td-p/426808
329. https://aws.amazon.com/marketplace/pp/prodview-bpvsouextldoy
330. https://www.mbtechtalker.com/scm-device-onboarding/
331. https://www.ibm.com/docs/en/sevone-npm/8.0.0?topic=troubleshooting-sd-wan-palo-alto-prisma-guide
332. https://docs.paloaltonetworks.com/ngfw/release-notes/12-1/features-introduced-in-pan-os/sd-wan-features
333. https://www.scribd.com/document/838235231/Prisma-SD
334. https://www.paloaltonetworks.com/resources/datasheets/prisma-sd-wan-instant-on-network-ion-device-specifications
335. https://www.paloguard.com/ION-1000.asp
336. https://docs.paloaltonetworks.com/prisma-sd-wan
337. https://www.boll.ch/de/datasheets/Prisma_SD-WAN_ION.pdf
338. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/getting-started/insights-scm/monitor-prisma-sd-wan-ion-devices

339. https://www.sonicwall.com/support/knowledge-base/how-to-setup-active-standby-high-availability-on-nssp-13700-appliances/kA1VN0000000IUq0AM
340. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/activation-and-onboarding/onboard-to-strata-cloud-manager/onboard-ztp-ngfws
341. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/onboard-to-strata-cloud-manager
342. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-new-features/panorama-features/authentication-key-for-secure-firewall-onboarding
343. https://www.reddit.com/r/paloaltonetworks/comments/1kf2f32/strata_cloud_manager_onboarding_firewall_with/
344. https://www.techclick.in/how-to-add-a-locally-managed-firewall-to-panorama-management
345. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/panorama-web-interface/panorama-device-registration-auth-key
346. https://www.youtube.com/watch?v=q5ZMWAZu1_w
347. https://docs.paloaltonetworks.com/whats-new/new-features/may-2025/enhanced-visibility-for-ztp-onboarding
348. https://www.mbtechtalker.com/scm-device-onboarding/
349. https://docs.paloaltonetworks.com/content/techdocs/en_US/ngfw/getting-started/initial-setup-configuration-ngfws/onboard-to-panorama-or-strata-cloud-manager
350. https://www.youtube.com/watch?v=KVEBpdGZxrc
351. https://docs.paloaltonetworks.com/ngfw/getting-started/onboard-your-ngfws/onboard-a-firewall
352. https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/add-a-firewall-as-a-managed-device
353. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/panorama-web-interface/panorama-device-registration-auth-key
354. https://docs.paloaltonetworks.com/ngfw/getting-started/onboard-your-ngfws/onboard-ztp-firewalls/ztp-configuration-elements
355. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/reports
356. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/insights-scm
357. https://www.youtube.com/watch?v=9RnO_vo0iLg
358. https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/monitor-network-activity/use-panorama-for-visibility/generate-schedule-and-email-reports
359. https://www.ibm.com/docs/en/powersc-standard/2.3.0?topic=reports-exporting-report-status-pdf-csv
360. https://www.youtube.com/watch?v=5nxt7R9d-YI
361. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding/configure-log-forwarding-scm
362. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/view-and-manage-reports/generate-custom-reports
363. https://www.crmsoftwareblog.com/2025/09/export-dynamics-365-report-to-pdf-word-csv-native-vs-click2export/
364. https://www.youtube.com/watch?v=ClDQmabhEzc
365. https://www.reddit.com/r/paloaltonetworks/comments/1bnfo33/strata_cloud_manager_vs_panorama/

366. https://live.paloaltonetworks.com/t5/panorama-discussions/panorama-to-strata-cloud-manager-anyone-using-in-production/td-p/628007
367. https://www.reddit.com/r/paloaltonetworks/comments/1pd6z68/anyone_tried_migrating_from_panorama_to_strata/
368. https://www.youtube.com/watch?v=2VES4GECQdc
369. https://docs.paloaltonetworks.com/whats-new/new-features/june-2023/custom-dashboard
370. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scope
371. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/folder-management
372. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/configuration-overview/snippets
373. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/configuration-overview/variables
374. https://live.paloaltonetworks.com/t5/strata-cloud-manager/ngfw-local-config-audits-with-scm/td-p/1223832
375. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/getting-started/system-settings/system-settings-audit-logs
376. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/migrate-from-panorama-to-strata-cloud-manager
377. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/configuration-overview
378. https://www.reddit.com/r/paloaltonetworks/comments/1hws13i/scm_folder_and_snippet_structure/
379. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/overview/get-started
380. https://www.reddit.com/r/paloaltonetworks/comments/19d281f/migration_from_panorama_to_strata_cloud_manager/
381. https://pan.dev/scm/docs/tenant-service-groups/
382. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
383. https://www.youtube.com/watch?v=yaLTccZSfgA
384. https://dependencyhell.net/2024/introduction-to-strata-cloud-manager-part-i