NGFW and SASE Solution Maintenance and Configuration

For an advanced network security professional managing Palo Alto Networks environments, maintenance and configuration differ significantly between **Strata NGFW** (customer-managed hardware/VMs) and **Prisma SASE** (cloud-delivered, shared responsibility).

The following guide breaks down the maintenance lifecycles, configuration best practices, and essential tools for both platforms.

1. Maintenance Lifecycles: NGFW vs. Prisma SASE

Strata NGFW (Physical/VM)

You own the entire stack. Maintenance is critical for hardware health and software stability.

Frequency	Task	Description
Daily	**Log Review**	Check System logs for critical hardware/software errors and Config logs for unauthorized changes [1] [2].
	Dynamic Updates	Verify successful download/install of Antivirus, Applications, and Threat updates. Ensure WildFire updates are set to "Every Minute" [3].
	Interface Health	Monitor interface errors (CRC, drops) which often indicate cabling or duplex issues.
Weekly	**Config Backup**	Export "device state" or XML configs to an external server. Do not rely solely on local snapshots [4].
	Threat Analysis	Review the ACC (Application Command Center) for spikes in threat activity or blocked applications.
Monthly	**Unused Rule Audit**	Identify and disable rules with zero hit counts over 30 days.
	Software Upgrades	Check for new preferred PAN-OS releases. Plan upgrades if your current version is approaching EoL or has critical vulnerabilities [5].

Prisma SASE (Prisma Access)

Palo Alto Networks manages the infrastructure (gateways, cloud nodes). Your maintenance focus shifts to client-side components and connectivity.

- **Infrastructure Upgrades:** PANW manages backend upgrades (e.g., dataplane OS) during scheduled maintenance windows. You will receive notifications but typically cannot defer these indefinitely.[5] [6]

- **GlobalProtect App Versions:** *You* must actively manage the GlobalProtect client version hosted on the portal.
  - **Best Practice:** Keep the hosted version N-1 or N-2 from the latest release to ensure stability while getting bug fixes.[7]
  - **Action:** In **GlobalProtect > Portals > Agent**, configure upgrade behavior (e.g., "Allow with Prompt" or "Transparently").[8]
- **Public IP Allow-Listing:** Prisma Access Public IP addresses can change or expand. You must regularly retrieve the current list of Prisma Access IPs and update your third-party SaaS allow-lists (e.g., Office 365, Salesforce) to prevent access issues.[6]
- **Service Connection Monitoring:** Monitor bandwidth utilization on Service Connections (SC) back to your datacenter. If SCs are saturated, they become a bottleneck for all mobile users accessing internal apps.

2. Configuration Best Practices

Management Plane Hardening (Critical for NGFW)

- **Dedicated Management Network:** Never expose the management interface to the internet. Use a strictly isolated Out-of-Band (OOB) network.[9]
- **Permitted IP Lists:** Configure the "Permitted IP Addresses" list on the Management Interface to restrict access to only your admin subnets or jump hosts.[9]
- **Service Restrictions:** Disable Telnet and HTTP. Allow only SSH (v2) and HTTPS (TLS 1.2/1.3).[10]

Policy Management

- **Tagging & Description:** Enforce a strict tagging policy (e.g., `[Project_Name] [Requester]`). This is vital for SASE environments where rules can sprawl quickly across regions.
- **Zone Protection:** Apply Zone Protection Profiles to *all* zones (especially untrust) to mitigate flood attacks (SYN, UDP, ICMP) before they hit the policy engine.[11]
- **Decryption:** Use "No Decrypt" rules for sensitive categories (Health, Finance) and pinned-certificate applications. For SASE, ensure your decryption policy accounts for high-latency or country-specific privacy laws.

Prisma SASE Specifics

- **Service Connections (SC):** Configure at least one SC even if you don't need internal access immediately; it is often required for specific routing or DNS resolution scenarios.[6]
- **Gateway Naming:** If you undergo a corporate rebranding, gateway name changes require a support ticket (SRE) and a maintenance window; you cannot change them dynamically in the GUI.[6]

3. Essential Tools for Maintenance

Best Practice Assessment (BPA) Tool

This is the premier tool for auditing your configuration against PANW standards.

- **What it does:** Analyzes your `tech-support` file and generates a heatmap showing feature adoption (App-ID, User-ID, etc.) and security gaps.[12] [13]
- **How to use:**
  1. Generate a Tech Support file from your Firewall or Panorama.
  2. Upload it to the Customer Support Portal (CSP) under **Tools > Best Practice Assessment**.
  3. Review the "Failed" checks. Focus first on "Management" and "Zone Protection" failures.[14]

Strata Cloud Manager (AIOps)

For newer deployments, **Strata Cloud Manager (SCM)** utilizes AIOps to predict health issues.

- **Free Capability:** Even without a premium license, AIOps provides basic best practice checks and health forecasting for NGFWs.[15]
- **Use Case:** Use it to predict disk usage exhaustion or certificate expiries before they cause an outage.

Summary Checklist for This Week

1. **[NGFW]** Run a BPA report on your primary perimeter firewall.
2. **[SASE]** Verify your hosted GlobalProtect agent version is not End-of-Life.
3. **[SASE]** Check if your Service Connections are nearing their bandwidth license limits.
4. **[Both]** Validate that your configuration backups are successfully saving to an external location.

⁂

Maintain and configure hardware firewalls, VM-Series firewalls, CN-Series firewalls, and Cloud NGFWs

The maintenance and configuration models for Palo Alto Networks firewalls vary significantly by form factor. While the **Policy** layer (App-ID, User-ID) remains consistent, the **Infrastructure** layer shifts from physical hardware management to code-based deployments (IaC).

Quick Reference: Maintenance & Configuration Matrix

Form Factor	Primary Maintenance Focus	Configuration "Source of Truth"	Critical Tooling
Hardware	Physical Health, Environment, RMA	Panorama / Local CLI	`request system software check`
VM-Series	Hypervisor Tuning, Driver Updates	Panorama / Bootstrap XML	SR-IOV, DPDK, vNIC tuning
CN-Series	Container Image Lifecycles, Helm Charts	Kubernetes Manifests / YAML	`kubectl`, Helm, K8s Plugin
Cloud NGFW	Rulestack Management, Cloud Connectivity	AWS/Azure Console / API	Cloud Provider Console, Terraform

1. Hardware Firewalls (PA-Series)

Traditional appliances where you own the full stack, from power cables to the management plane.

Maintenance

- **Environment & Physical:** Monitor fan speeds, temperature, and power supply redundancy. Vacuum air intakes annually if in dusty environments.
- **Management Plane:** Because the management plane is local, resource exhaustion is a risk.
  - **Action:** Regularly clear old logs/reports to prevent disk fill-up (`delete log...`).
- **Upgrades:** Follow the classic "download → install → reboot" path. Ensure you upgrade the **Data Plane** (PAN-OS) and **Content** (App+Threat) separately.

Configuration

- **Interface Hardening:** You must manually configure speed/duplex and negotiate settings.
- **High Availability (HA):** Requires dedicated physical cabling (HSCI/HA1/HA2). You are responsible for layer 1-2 troubleshooting.

2. VM-Series Firewalls

Virtual appliances running on hypervisors (ESXi, KVM, Nutanix, AWS/Azure). Maintenance focuses on the "Guest-to-Host" relationship.

Maintenance (Performance Tuning)

Unlike hardware, VM-Series performance depends heavily on the underlying host drivers.

- **Drivers:** You must maintain compatibility between the PAN-OS version and the Hypervisor's drivers (e.g., i40e vs i40evf).[30]
- **Packet Acceleration:**

- **SR-IOV:** Bypass the hypervisor switch to give the VM direct NIC access. Requires host-level BIOS/OS configuration.[31]
- **DPDK:** Enable Data Plane Development Kit to boost packet processing. You can enable this via the CLI: `set system setting dpdk-pkt-io on`.[32] [30]

Configuration

- **Bootstrapping:** Use `bootstrap.xml` and an `init-cfg.txt` file mounted via virtual CD-ROM or S3 bucket to configure the firewall at first boot automatically. This is essential for auto-scaling groups.
- **vCPU Pinning:** On KVM/ESXi, ensure firewall vCPUs are pinned to physical cores to prevent "noisy neighbor" latency.

3. CN-Series Firewalls

Containerized firewalls for Kubernetes (K8s). Maintenance is "Immutable Infrastructure" style—you rarely patch; you redeploy.

Maintenance (Image Lifecycle)

- **Upgrade Process:** You do not "install" PAN-OS. You update the container image reference in your orchestration files.
  - **Rolling Update (DaemonSet):** Update the image in your `pan-cn-mgmt.yaml` or use `kubectl set image`. K8s recycles pods sequentially.[33]
  - **Redeploy (Service Mode):** Often requires a complete teardown and redeploy, which may require a scheduled maintenance window for the application traffic.[33]
- **License Management:** CN-Series uses a credit-based licensing model (Software NGFW Credits). Ensure your credit pool in the CSP (Customer Support Portal) allows for auto-scaling spikes.

Configuration (Helm & YAML)

- **Helm Charts:** The recommended way to manage config. You define variables in a `values.yaml` file (e.g., PAN-OS version, CPU limits) and deploy via `helm install`.[34] [35]
- **Panorama Integration:** Requires the **Kubernetes Plugin** on Panorama. This plugin syncs tags (e.g., namespace, pod labels) to Dynamic Address Groups (DAGs), allowing you to write policies like "Allow App A to talk to App B" regardless of IP changes.[36]

4. Cloud NGFW (AWS/Azure)

Managed service where the infrastructure is hidden. You manage "Rulestacks".

Maintenance (Shared Responsibility)

- **Infrastructure:** Palo Alto Networks and the Cloud Provider patch the underlying OS and scale the infrastructure. You have **no CLI access** to the backend device.
- **Endpoints:** You must maintain the VPC Endpoints (AWS) or VNET injections (Azure). Ensure your routing tables (TGW, UDRs) correctly point traffic to these endpoints.

Configuration (Rulestacks)

- **Rulestack Model:** Instead of a "Device Group," you configure **Rulestacks**.
  - **Local Rulestack:** Applies to a specific firewall resource in one account.[37]
  - **Global Rulestack (AWS Only):** Managed via AWS Firewall Manager to enforce a baseline policy (Pre-rules) across *all* accounts in an AWS Organization.[38] [37]
- **Security Profiles:** You still configure Spyware/Vulnerability profiles, but you attach them to the Rulestack rather than a specific firewall interface.

Summary: Which Tool for Which Task?

Task	Hardware/VM	CN-Series	Cloud NGFW
Update OS	**GUI/CLI:** `request system software install`	**K8s:** `helm upgrade` / `kubectl set image`	**Automated:** Managed by Vendor
Config Rules	**Panorama:** Device Groups	**Panorama:** K8s Plugin + DAGs	**Cloud Console:** Rulestacks
Scale Up	**Manual:** Rack new unit / Clone VM	**Auto:** K8s HPA (Horizontal Pod Autoscaler)	**Auto:** Cloud Provider scaling
Debug	**CLI:** `tcpdump`, `debug dataplane`	**CLI:** `kubectl logs`, `micro-pcap`	**Logs:** CloudWatch / Azure Monitor

⁂

security policies

For an advanced practitioner, a **Security Policy** in the Palo Alto Networks ecosystem is not just an Access Control List (ACL); it is a context-aware enforcement object that integrates App-ID, User-ID, and Device-ID.

The following guide covers the architectural hierarchy, optimization strategies, and cloud-specific nuances for managing security policies effectively.

1. Architectural Hierarchy: Pre-Rules vs. Post-Rules

When managing policies via Panorama, the "single rulebase" view is actually a merged composite of three distinct layers. Understanding this evaluation order is critical for troubleshooting "shadowed" rules.

Evaluation Order	Rule Type	Managed By	Best Use Case
1. Pre-Rules	Global/Shared	Panorama	**Corporate Mandates:** Block malicious IPs, Geoblocking (e.g., Block North Korea), and enterprise-wide "Allow DNS/NTP" rules. Local admins cannot override these.
2. Local Rules	Specific	Local Firewall / Stack	**Workload Specifics:** Rules specific to the application hosted behind that specific firewall (e.g., Allow SQL from App-Server to DB).
3. Post-Rules	Global/Shared	Panorama	**Cleanup & Safety Nets:** The "Clean-Up Rule" (Deny All + Log) belongs here. It ensures that if traffic doesn't match a specific local rule, it hits the corporate logging standard before being dropped [45] [46].
4. Default Rules	Implicit	System (Read-Only)	**Intrazone Allow / Interzone Deny:** These are invisible by default. *Best Practice:* Override these with an explicit "Deny All" Post-Rule to ensure visibility (logging) [47].

2. Best Practices for Hardening

- **Application-Default is Mandatory:** In the **Service** column, avoid `any`. Use `application-default`. This enforces that SSH traffic (App-ID: `ssh`) *must* occur on port 22. If an attacker tries to tunnel SSH over port 80, the firewall blocks it because the application does not match the standard port.[48]
- **Log at Session End:** Enable logging only at "Session End" for allow rules. "Session Start" generates excessive noise and should only be used temporarily for troubleshooting TCP connection issues.[49]
- **Tagging Schema:** Enforce a strict tagging schema (e.g., `Project:A`, `Exp:2026-12`). This allows you to filter the rulebase instantly and is required for some automation integrations.
- **UUID Persistence:** Remember that rule names are mutable; rule UUIDs are immutable. When automating rule audits via API, always reference the UUID, not the name.

3. Optimization: Moving from Ports to App-ID

Legacy "Port-Based" rules (allowing tcp/80, tcp/443) are opaque holes in your perimeter.

- **The Problem:** `tcp/443` is not just HTTPS; it's also tor-browser, bit-torrent, and external-proxy.
- **The Solution (Policy Optimizer):** Use the **Policy Optimizer** feature (found in the Policies tab).
  - **Workflow:** Sort by "Apps Seen." The firewall analyzes traffic hitting your legacy port-based rules and identifies the actual applications.
  - **Action:** You can "Clone Rule" based on "Apps Seen" to create a precise App-ID rule, then safe-delete the legacy port rule.[50] [48]

4. Cloud-Specific Policy Structures

The concept of "Device Groups" changes slightly in cloud-native deployments.

Cloud NGFW (AWS/Azure)

- **Rulestacks:** Instead of Device Groups, you manage **Rulestacks**.
  - **Global Rulestack (AWS Only):** Managed via AWS Firewall Manager to push baseline rules to *every* VPC in an AWS Organization.
  - **Local Rulestack:** Specific to a firewall endpoint.
- **Note:** You typically cannot reference "Zones" in Cloud NGFW rules in the same way as on-prem, as interfaces are abstracted. Policies are often tag-based or prefix-list based.[51] [52]

CN-Series (Kubernetes)

- **Dynamic Address Groups (DAGs):** In K8s, IP addresses are ephemeral. You cannot write static IP rules.
- **Method:** Use the **Panorama Kubernetes Plugin**. It scrapes K8s labels (e.g., `app=frontend`) and registers the IPs into a DAG.
- **Rule Logic:** "Allow Source: `DAG_Frontend` to Dest: `DAG_Backend` on App: `mysql`." This rule persists even as pods are destroyed and recreated with new IPs.[53]

⁂

Profiles

Security Profiles are the core "Threat Prevention" engine of the firewall. While Security Policies determine *who* can talk (Layer 3/4), Security Profiles determine *what* they can say (Layer 7 Content Inspection).

Golden Rule: Never create an "Allow" rule without attaching a Security Profile Group. An allow rule without profiles is just a stateful router, not a Next-Gen Firewall.[61] [62]

1. The "Big Three" Profiles (Must-Haves)

Antivirus (AV)

- **Goal:** Detects known malware signatures in file transfers.
- **Best Practice:**
  - **Action:** Set all decoders (HTTP, SMTP, SMB, etc.) to `reset-both` (or `drop` for UDP). Do not use `alert`—it allows the file through and just logs it.[62] [63]
  - **WildFire Action:** Within the AV profile, ensure the "WildFire Action" column is also set to `reset-both`. This ensures that if the firewall receives a "Malicious" verdict from WildFire for a hash it just saw, it blocks future downloads of that hash immediately.[64]

Vulnerability Protection (VP)

- **Goal:** Stops exploits (buffer overflows, SQL injection) and C2 (Command & Control) probes.
- **Best Practice:**
    - **Strict vs. Standard:** Start with the **Strict** profile for all internet-facing servers (Inbound). Use the **Standard** profile for internal user traffic (Outbound) to minimize false positives on legacy internal apps.[65] [63]
    - **Critical Setting:** Ensure the action for "Critical" and "High" severity threats is set to `reset-both`. Default profiles often leave "Medium" or "Low" as `alert`, which is acceptable for tuning, but critical threats must be blocked.

Anti-Spyware (AS)

- **Goal:** Detects infected hosts calling home to C2 servers.
- **Best Practice:**
    - **DNS Sinkholing:** This is the most critical feature. Enable **DNS Sinkhole** on the Anti-Spyware profile attached to your User/Outbound policies.
    - **Mechanism:** When a client queries a malicious domain (e.g., `malware.com`), the firewall intercepts the DNS response and replies with a "Sinkhole IP" (e.g., `72.5.65.111`). The infected client then tries to connect to that IP, which is easily blocked and logged, pinpointing the exact infected machine.[62]

2. Specialized Profiles (Context-Aware)

URL Filtering

- **Credential Phishing Prevention:** This is often overlooked.
    - **Configuration:** In the URL Filtering profile, under "User Credential Submission," set the action to **Block** for categories like `unknown`, `phishing`, and `parked`.
    - **Effect:** If a user tries to type their corporate AD username/password into a site categorized as "phishing," the firewall detects the hash of the password leaving the network and blocks the packet.[66] [67]

WildFire Analysis

- **Goal:** Sandboxing for "Unknown" files.
- **Best Practice:**
    - **Forwarding:** Configure a WildFire Analysis profile to forward *all* unknown file types (PE, APK, PDF, JAVA, Office) to the WildFire Public Cloud.
    - **Real-Time:** Ensure "Real-time Signature Lookup" is enabled. This allows the firewall to query the cloud cache for a verdict in milliseconds before the file transfer completes.[68] [69]

3. Implementation Strategy: Security Profile Groups

Managing 5 distinct profiles per rule is error-prone. Use **Security Profile Groups**.

- **Group 1:** `SPG-Internet-Outbound`
  - AV: `Strict`
  - AS: `Strict-Sinkhole`
  - VP: `Standard`
  - URL: `Block-Malicious-Categories`
  - WildFire: `Forward-All`
- **Group 2:** `SPG-Server-Inbound`
  - AV: `Strict`
  - AS: `Strict`
  - VP: `Strict` (Crucial for stopping exploit attempts against your web servers)
  - URL: `Alert-Only` (Servers generally don't browse the web, but logging is useful)

Note on Performance: Enabling profiles does incur a processing cost (Single Pass Architecture minimizes this), but disabling them defeats the purpose of an NGFW. "Strict" Vulnerability Protection on *all* internal traffic is the only scenario that might require hardware sizing review.[70]

⁂

updates

Keeping a Palo Alto Networks environment current involves managing two distinct streams: **Dynamic Updates** (Content) and **Software Upgrades** (System). In 2026, the strategy has shifted toward "Near-Real-Time" protection for content but "Conservative" stability for software.

1. Dynamic Updates (Content)

These updates contain the intelligence (signatures) for App-ID, Threat-ID, and WildFire. They do not require a reboot and are generally non-disruptive *if* configured correctly.

Update Type	Recommended Frequency	Action	Critical Nuance
WildFire	**Real-Time** (Streaming)	Download & Install	In PAN-OS 10.0+, switch to "Real-Time" updates to receive signatures via a persistent cloud connection rather than polling every minute [76] [77].
Antivirus	**Hourly**	Download & Install	Set a randomized delay (e.g., 10 mins) if managing thousands of firewalls to prevent bandwidth spikes on the management network [78].

Update Type	Recommended Frequency	Action	Critical Nuance
Applications & Threats	**Daily / Weekly**	*Conditional*	**Daily:** For high-security zones (Edge). **Weekly:** For stable internal zones. **Crucial:** Always enable "**Disable new apps in content update**" [79] [80].

Why "Disable New Apps"?

When PANW releases a new App-ID (e.g., `chatgpt-upload`), traffic that previously matched a generic rule (e.g., `ssl` on port 443) might suddenly match this new, specific App-ID.

- **Risk:** If you don't have a rule allowing `chatgpt-upload`, that traffic gets blocked immediately after the update.
- **Best Practice:** By checking "Disable new apps," the firewall learns the App-ID but doesn't enforce it yet. You gain time to review the "New App-IDs" report and add them to your policy before enabling them globally.[79] [80]

2. Software Upgrades (PAN-OS)

Upgrading the operating system (Data Plane/Management Plane) is disruptive and requires a maintenance window.

The "Preferred Release" Rule

Never upgrade to the latest numeric version (e.g., 11.2.0) immediately. Always target the **Preferred Release** designation on the Palo Alto Support site.

- **General Rule:** Wait for the `x.x.4` or `x.x.5` release before deploying to production (e.g., 11.1.6-h3).

Upgrade Paths (Skip Level Upgrades)

Modern PAN-OS versions (10.1+) support "Skip Software Version" upgrades, significantly reducing downtime.

- **Old Way (Sequential):** 10.1 → 10.2 → 11.0 → 11.1
- **New Way (Skip):** You can often jump directly from 10.1 or 10.2 to 11.1, provided you are on the latest maintenance release of your *current* version.[81] [82]
  - *Step 1:* Upgrade current 10.2.x to latest 10.2.preferred.
  - *Step 2:* Download 11.1 Base Image (do not install).
  - *Step 3:* Download & Install target 11.1.preferred release.
  - *Step 4:* Reboot once.

3. Automation & Orchestration

- **GlobalProtect Data File:** Schedule this frequently (Daily) as it contains HIP (Host Information Profile) checks for patching endpoint OS versions.
- **External Dynamic Lists (EDLs):** These are not "updates" in the traditional sense but update frequently (every 5-15 mins). Ensure your management plane DNS is resilient, as EDLs failing to refresh can cause rules to drop legitimate traffic if the list empties (fail-safe options exist in 11.x).

4. Verification Checklist

Before any major upgrade:

1. **Check Disk Space:** `show system disk-space` (Ensure >20% free on root).
2. **Check Content:** Ensure App+Threat database is current.
3. **Review Release Notes:** specifically the "Changes to Default Behavior" section, which often contains "gotchas" like new strict TCP handling or certificate checks.

⁂

upgrades

Software upgrades in the Palo Alto Networks ecosystem (NGFW, Panorama, and SASE) require distinct procedures. While the end goal is the same—stability and new features—the execution path differs fundamentally between hardware you own and cloud services you lease.

1. Upgrade Hierarchy: The Golden Rule

Always upgrade from the top down. A management platform must be on a version equal to or higher than the devices it manages.[91] [92]

> **Hierarchy:** `Panorama` ≥ `Firewalls` ≥ `Log Collectors`

- **Risk:** If you upgrade a Firewall to 11.1 while Panorama is on 11.0, Panorama will lose the ability to push configurations to that device.
- **Best Practice:** Upgrade Panorama first. It is backward compatible and can manage firewalls running older versions (e.g., Panorama 11.1 can manage PAN-OS 10.1, 10.2, and 11.0).[91]

2. Hardware & VM-Series: The "HA Dance"

For Active/Passive High Availability (HA) pairs, you can perform upgrades with **zero packet loss** by following a strict sequence. Do not simply "reboot" the active unit.[93] [94]

Step	Unit	Action	Command/GUI	Why?
1	**Passive**	**Upgrade**	Install → Reboot	Upgrade the standby unit first while traffic flows through the Active unit.

Step	Unit	Action	Command/GUI	Why?
2	**Passive**	**Verify**	`show high-availability state`	Ensure the upgraded unit comes back up as "Passive" and syncs sessions.
3	**Active**	**Suspend**	`request high-availability state suspend`	Force failover. The upgraded unit (now Active) takes traffic.
4	**New Passive**	**Upgrade**	Install → Reboot	Upgrade the former Active unit (now Passive).
5	**New Passive**	**Unsuspend**	`request high-availability state functional`	Bring the unit back into the HA cluster.
6	**Optional**	**Failback**	`request high-availability state suspend`	If you have a strict "Primary must be Active" policy, fail back now.

Pre-Check Tip: Before upgrading, run `request system software check`. If the base image is missing, the firewall cannot install the maintenance release.[95]

3. Prisma Access (SASE): Innovation vs. Preferred

You do not "upload" software to SASE; you manage the rollout schedule. Palo Alto Networks handles the backend infrastructure, but you control *when* it hits your dataplane.[96] [97]

- **Release Tracks:**
  - **Preferred:** Proven stability. Best for production environments requiring high uptime.
  - **Innovation:** Latest features. Use this for Lab/Test environments or if you need a specific new capability immediately.
- **The 7-Day Rule:** You typically receive a notification 21 days before a major upgrade. You *must* select your preferred upgrade window (e.g., "Saturday 2 AM"). If you do not select a window by **7 days** prior, PANW will auto-assign a slot, which might be during your business hours.[98] [96]
- **GlobalProtect:** Remember, SASE upgrades do *not* automatically upgrade the GlobalProtect app on end-user laptops. You must still manage that version in the Portal configuration.

4. Troubleshooting Common Failures

If an upgrade fails or the device boots into "Maintenance Mode," check these common culprits:

- **Autocommit Failed:**
  - *Symptom:* Device is accessible via CLI but traffic is not passing.
  - *Cause:* Configuration syntax became invalid in the new version (e.g., a "duplicate user" error that was ignored in 10.1 is now a hard stop in 11.0).[99] [100]
  - *Fix:* Use `tail follow yes mp-log autocommit.log` to see the specific error. You may need to revert (`debug swm revert`) to fix the config before trying again.

- **Disk Space:**
    - *Symptom:* Upgrade job fails instantly.
    - *Fix:* Delete old software versions (`delete software version x.x.x`) and old content updates. You generally need >10GB free on the root partition for 11.x upgrades.

5. Cloud NGFW & CN-Series (Immutable)

- **CN-Series:** Do not run upgrade commands inside the container. Update the image tag in your Helm chart (e.g., `image: pan-os:11.1.0`) and run `helm upgrade`. Kubernetes will spin up new pods and terminate the old ones.
- **Cloud NGFW (AWS):** You select the version in the AWS Console. The service spins up new endpoints behind the scenes and shifts traffic. **Note:** This can cause a momentary reset of TCP sessions, so perform during low-traffic windows.

⁂

add, configure, and maintain Prisma SD-WAN

Prisma SD-WAN (formerly CloudGenix) uses a fundamentally different model than PAN-OS. It is "Application-Defined" rather than packet-based, meaning you configure policies based on *business intent* (e.g., "Microsoft Teams must use the high-bandwidth path") rather than IPs and ports.

1. Adding & Configuring ION Devices (The Lifecycle)

Step 1: Claiming the Hardware

Unlike firewalls, ION devices (Instant-On Network) are claimed via serial number in the cloud controller before they are physically plugged in.

- **Workflow:** Go to **Configuration > ION Devices > Claim**.
- **Action:** Enter the Serial Number and Claim Key found on the box or email invoice.
- **Result:** The device appears in the "Unassigned" list.

Step 2: Site Configuration (The Logical Wrapper)

You must define the "Site" (logical container) before configuring the device.

- **Create Site: Configuration > Sites > Add Site**.
    - **Critical Fields:** Address (determines Geolocation for map), Site Type (Branch vs. DC), and **Tags** (e.g., `Region:SaoPaulo`, `Type:Retail`).
    - **Why Tags?** Policies apply to tags, not individual devices. You write one policy for `Type:Retail` and it automatically applies to all 500 retail sites.
- **Assign Device:** Assign the claimed ION to this Site.

Step 3: Interface & Circuit Configuration

This is the "Zero Touch Provisioning" (ZTP) phase.

- **Connect:** Plug the WAN 1 port into the internet. The ION calls home.
- **Configure:** In the portal, define the circuits (links).
  - **Circuit Label:** Identify the provider (e.g., `ISP-Vivo-Fiber`).
  - **Attributes:** Define upload/download speeds accurately. The SD-WAN scheduler uses these values to calculate saturation and steer traffic. **Do not estimate this.**.[106]

2. Maintenance & Operations

Software Upgrades

- **Granular Control:** Unlike PAN-OS, ION software upgrades can be extremely granular.
- **Process: Maintenance > Software Images**. You can upgrade a single site, a group of sites (via Tags), or the entire network.
- **Best Practice:** Use the **"Canary Deployment"** method. Upgrade 1 test site → Wait 24h → Upgrade 10% of sites → Upgrade remainder.

Monitoring with AIOps

Prisma SD-WAN relies heavily on "Network Application Performance" scores.

- **App-Response Time (ART):** The system measures the time from SYN to ACK (Network RTT) and ACK to First Byte (Server Response Time).
- **Troubleshooting:** If a user complains "SAP is slow," check the **App Health** dashboard.
  - *High Network RTT:* It's the ISP/VPN.
  - *High Server RTT:* It's the Datacenter/Server (not the network).

3. Key Differentiator: CloudBlades

CloudBlades are API integrations that inject configuration automatically.

- **Use Case:** You want to integration with **Prisma Access** for security.
- **Action:** Enable the "Prisma Access CloudBlade."
- **Result:** The SD-WAN controller automatically builds IPSec tunnels from every ION branch to the nearest Prisma Access cloud node. You do *not* manually configure VPN peers.[107]

Summary Checklist

1. **Claim** IONs via Serial Number.
2. **Create** Sites with descriptive Tags.
3. **Define** accurate bandwidth values for Circuits.

4. **Enable** CloudBlades for automated integration (Prisma Access, ServiceNow, etc.).
5. **Monitor** App Health, not just "Link Up/Down."

⁂

Initial ION setup

The initial setup of a Prisma SD-WAN ION (Instant-On Network) device focuses on establishing the first connection to the cloud controller. Unlike traditional firewalls, the "Config" happens in the cloud *before* or *during* the physical installation, and the device pulls it down via Zero Touch Provisioning (ZTP).

1. Physical Connectivity (Wiring)

Correct cabling is critical for ZTP success.

- **Controller Port (Specific Models):** Larger units (ION 2000/3000/9000) have a dedicated port labeled **CONTROLLER** or **MGMT**. This port *must* be connected to a network with DHCP and Internet access for the initial call-home. It is out-of-band management.
- **Internet Ports (All Models):** On smaller units (ION 1000/1200) or if no dedicated controller port exists, use **Port 1** (often labeled WAN or Internet).
- **LED Status Indicators:**
  - **Power:** Green (Solid) = On.
  - **Controller:**
    - **Green:** Connected to Cloud (Success).
    - **Red:** No connection to Cloud (Check Internet/DNS/Firewall).
    - **Blinking:** Authenticating/Downloading Config.[121] [122]

2. Zero Touch Provisioning (ZTP)

In 90% of cases, you plug it in, and it works.

- **Requirement:** The upstream connection must provide **DHCP** and allow outbound HTTPS (TCP/443) and UDP/4500 to Palo Alto Networks cloud ranges.
- **Process:**
  1. Claim device in Cloud Portal (Serial Number).
  2. Assign to a Site (Config is generated).
  3. Plug in ION WAN/Controller port.
  4. ION gets IP → Calls Home → Downloads Config → Reboots → Online.

3. Manual Configuration (When ZTP Fails)

If you only have a Static IP circuit (no DHCP), ZTP will fail. You must configure the "bootstrap" settings locally.

Method A: Local Web Interface (LUI) - *Newer Models*

1. Connect a laptop to the **LAN** port (often Port 2 or labeled LAN).
2. Your laptop should get a DHCP IP (e.g., 192.168.1.x) from the ION.
3. Browse to `https://192.168.1.1`.
4. Log in (Default credentials are often `admin` / `admin` or the Serial Number - check docs).
5. Navigate to **Uplink Config** and set the Static IP/Gateway/DNS for the WAN port.

Method B: Console Port (CLI) - *Reliable Fallback*

1. Connect a Console cable (RJ45-to-USB) to the **CONSOLE** port.
2. Terminal Settings: `115200` baud rate, 8, N, 1.
3. Login commands:
   - Set Static IP on Controller Port:

     ```
     # config interface controller1 ip static address=10.0.0.50/24 gw=10.0.0.1 dns=8.8
     ```

   - Set Static IP on Internet Port (if no controller port):

     ```
     # config interface 1 ip static address=203.0.113.2/30 gw=203.0.113.1 dns=8.8.8.8
     ```

   - Verify connectivity:

     ```
     # ping bootstrap.prismasdwan.internal
     ```

   - *Note:* If this DNS name resolves, the device can find the cloud.[123] [124]

4. Troubleshooting Initial Setup

- **"Device Unreachable":**
  - Check if an upstream firewall is blocking **TCP/443** or **UDP/123** (NTP). Correct time is mandatory for SSL certificate validation.
  - Verify the **Claim Key** in the portal matches the device.
- **"Authentication Failed":**
  - Often means the device clock is too far off. Rebooting usually forces an NTP sync.
  - Ensure the Serial Number was typed correctly (0 vs O is a common error).
- **Allow-List:** Ensure your edge firewall allows traffic to `*.prismasdwan.internal` and `*.cloudgenix.com`.[125] [126]

5. Post-Connection Verification

Once the Controller LED turns Green:

1. Log in to the Prisma SD-WAN Portal.
2. The device status should change from "Unclaimed" or "Offline" to **"Online"**.
3. The device will immediately download the software version specified in your Site Policy. **Expect a 2nd reboot** roughly 10-15 minutes after the first connection. Do not unplug it.

⁂

Pathing

In Prisma SD-WAN, "Pathing" refers to the intelligent selection of network circuits (MPLS, Internet, LTE) based on application requirements. It moves beyond static routing (OSPF/BGP) to "Application-Aware Routing."

1. The Core Components of Path Selection

Prisma SD-WAN evaluates paths using a logical stack. If the top condition isn't met, it falls through to the next.

Component	Function	Example
Path Policy	The "Rule" that matches traffic.	"Match App: `Microsoft Teams` → Use Profile: `Real-Time-Video`"
Path Quality Profile	Defines the "SLA" (thresholds) for a path to be considered "healthy."	**Voice SLA:** Latency < 150ms, Jitter < 30ms, Loss < 1%.
Traffic Distribution	Decides *how* to use the healthy paths found by the Quality Profile.	**Best Available:** Pick the single best path. **Active/Active:** Load balance across all paths that meet the SLA.
Circuit Labels	Tags assigned to physical interfaces to group them logically.	`INET-Fast`, `MPLS-Gold`, `LTE-Backup`.

2. Configuring Path Policies (Step-by-Step)

You don't configure routes; you configure **Intent**.

1. **Define Circuit Labels:** Go to **Configuration > Overlays > Circuit Labels**. Create tags like `Internet-Fiber` and `Internet-Cable`.
2. **Assign Labels to Interfaces:** On the Site configuration, tag Port 1 as `Internet-Fiber` and Port 2 as `Internet-Cable`.
3. **Create a Path Quality Profile:**
   - Navigate to **Configuration > Policies > Path Quality Profiles**.
   - Set thresholds. *Example:* For VoIP, set Packet Loss to 1%. If a circuit hits 2% loss, it is marked "Out of Policy" and removed from the selection pool.[136] [137]

4. **Create a Traffic Distribution Profile:**
    - **Method:** Choose "Best Available Path" (most common) or "Active/Active" (for bandwidth aggregation).
    - **Priority:** Drag and drop Circuit Labels.
        - *Priority 1:* `MPLS-Gold`
        - *Priority 2:* `Internet-Fiber`
        - *Priority 3:* `LTE-Backup`
    - *Logic:* "Try MPLS first. If it violates the SLA (Quality Profile), switch to Fiber. If that fails, use LTE.". [138] [139]

3. Advanced Error Correction (Brownout Mitigation)

What happens if *all* paths are "okay" but have slight packet loss? You use **Error Correction Profiles** to fix the line digitally without switching.

- **Forward Error Correction (FEC):**
    - **How it works:** Sends parity packets (like RAID 5 for network traffic). If 1 packet is lost, the receiver reconstructs it from the parity data.
    - **Cost:** Adds ~10-20% bandwidth overhead.
    - **Use Case:** Real-time UDP traffic (Voice/Video) on lossy Internet links.
- **Packet Duplication:**
    - **How it works:** Sends the *same* packet down two different paths simultaneously. The receiver accepts the first one to arrive and discards the duplicate.
    - **Cost:** 100% bandwidth overhead (Double bandwidth usage).
    - **Use Case:** Critical transaction data (Credit Card Swipe) or VIP Voice calls where 0% loss is acceptable. [140] [141]

4. Troubleshooting Path Selection (Flow Browser)

When a user asks, "Why is my Zoom call lagging?" check the **Flow Browser**.

1. Navigate to **Activity > Flows**.
2. Filter by the user's IP or Application (`Zoom`).
3. Click on a flow to see the **Path Decision**.
    - **Current Path:** Shows which circuit is being used (e.g., `Internet-Cable`).
    - **Path Reason:** Crucial field. It will say:
        - `Policy Configured`: It's following your priority list.
        - `Performance-SLA-Exceeded`: It moved off the primary path because the SLA was violated.
        - `Circuit-Down`: The primary path is physically down. [142] [143]

Summary: The "Why" of Pathing

If you configure a "Standard" VPN, traffic follows the routing table. If you configure a **Path Policy**, traffic follows the **Application Performance**.

- **Best Practice:** Always define a "Backup" path in your distribution profile (e.g., LTE). If you only define one path and it fails the SLA, the system has nowhere to go and might drop traffic even if the link is technically "Up."

⁂

Monitoring and logging

Monitoring and logging in a Palo Alto Networks ecosystem relies on "Source of Truth" visibility. The location of your logs (On-prem vs. Cloud) dictates your troubleshooting workflow.

1. Strata NGFW (On-Prem / VM)

You own the logs. The firewall generates them, but it shouldn't store them long-term.

Core Log Types

- **Traffic Logs:** Session data (Source IP, Dest IP, Bytes, Rule Name).
  - *Best Practice:* Log at "Session End" to see total bytes. Only log "Session Start" for troubleshooting TCP handshake issues.[151] [152]
- **Threat Logs:** Security events (Virus, Spyware, Vulnerability).
  - *Best Practice:* These are high-fidelity. Alert on *every* Critical/High severity threat log. [153] [151]
- **System Logs:** Hardware/OS health (Link down, Fan failure, HA failover).
- **Config Logs:** Audit trail of *who* changed *what*. Mandatory for compliance.[154]

Log Forwarding (The "Profile" Method)

To send logs off-box (to SIEM, Panorama, or Syslog), you must use a **Log Forwarding Profile**.

1. **Create Profile: Objects > Log Forwarding**.
2. **Add Destination:** Select "Panorama" or a Syslog server profile.
3. **Attach to Rule:** You must attach this profile to *every* security policy rule. A common mistake is creating the profile but forgetting to apply it to the rules.[155] [156]

2. Prisma Access (SASE)

You do not own the infrastructure, so you cannot SSH in to check `/var/log`. You rely on cloud telemetry.

Strata Logging Service (SLS)

- **What it is:** The cloud database where Prisma Access dumps all logs.
- **Access:** You view these logs via **Strata Cloud Manager (SCM)** or Panorama (if configured as the interface for SLS).
- **Difference from On-Prem:** You cannot "delete" these logs manually. Retention is based on your purchased quota (e.g., 30 days).[157] [158]

Autonomous DEM (ADEM)

- **The Problem:** "My internet is slow" complaints from remote users.
- **The Solution:** ADEM is an agent on the GlobalProtect client that actively pings/curls synthetic tests to Zoom, Office365, and your Data Center.
- **Visibility:** It tells you if the latency is caused by:
    - **Device:** High CPU/Wi-Fi signal strength.
    - **Local ISP:** High packet loss at the user's home router.
    - **Internet:** Backbone latency.
    - **Application:** The SaaS provider is down.[159] [160]

3. Prisma SD-WAN

Monitoring focuses on **App Health** rather than "Link Up/Down."

Health Scores

- **Circuit Health:** Uses "Synthetic Probes" (ICMP/HTTP) to measure Loss, Latency, and Jitter.
- **App Health:** Measures actual user traffic (TCP/UDP metrics).
- **Calculation:** If a link has 0% packet loss but 500ms latency, the "Voice" application health will be **Poor**, but "Email" health might be **Good**. This context-aware scoring drives the Path Selection engine.[161] [162]

Troubleshooting Workflow

- **Alarms:** SD-WAN alarms are "Stateful." A "Link Down" alarm opens when the link fails and *auto-closes* when it recovers. You don't need to manually clear them like on traditional SNMP systems.
- **Flow Browser:** Use this to see exactly which path a specific user's session took.
    - *Filter:* `source_ip == 192.168.1.50` AND `app == Zoom`.
    - *Result:* "Switched from Comcast to MPLS at 10:05 AM due to Jitter > 30ms".[162]

Summary: Where to Look?

Scenario	Tool/Location	Key Metric
"Why was this packet blocked?"	**Monitor > Traffic Logs** (Firewall/Panorama)	`Session End Reason` (Policy Deny, Threat)
"Is the hardware overheating?"	**Monitor > System Logs**	`Temperature`, `Fan`
"Why is Zoom slow for everyone?"	**Prisma SD-WAN > App Health**	`Network RTT` vs `Server RTT`
"Why is Zoom slow for ONE user?"	**ADEM (Prisma Access)**	`Wi-Fi Signal Strength`, `Local ISP Latency`

⁂

Maintain and configure Prisma Access

Prisma Access is a managed service, so maintenance shifts from "box management" (OS upgrades, hardware health) to **Service Management** (configuration consistency, bandwidth planning, and client version control).

1. Configuration Best Practices

Since the dataplane is abstract, your configuration dictates performance more than hardware specs.

Service Connections (SC)

This is the most critical "pipe" in your SASE deployment. It connects the cloud users to your Data Center.

- **Bandwidth Sizing:** SC bandwidth is a licensed limit, not a physical port speed.
  - *Action:* Monitor "Egress Peak Bandwidth" in Prisma Access Insights. If you consistently hit 90% of your licensed cap (e.g., 500 Mbps), packets will drop, and users will complain of "slow internal apps".[166] [167]
  - *Best Practice:* If you need >1 Gbps, you must onboard multiple SCs to the same site and use ECMP (Equal Cost Multi-Path) to aggregate bandwidth.[168]
- **Routing:** Avoid advertising the default route (`0.0.0.0/0`) from your Data Center into Prisma Access via SC. This forces all internet traffic from mobile users to hairpin through your DC, destroying SASE performance benefits.

Mobile User IP Pools

- **Sizing Rule:** Configure an IP pool size that is **2x** your expected user count.
    - *Why?* Mobile users roaming between Wi-Fi and 5G consume 2 IPs temporarily. If the pool exhausts, new users cannot connect.
    - *Alerting:* Configure an alert in **Strata Cloud Manager > Insights** to notify you when IP Pool Utilization hits **85%**. SASE will auto-scale gateways, but it cannot auto-magically create more private IP subnets—you must add them.[169] [170]
- **Regional vs. Worldwide:** Use "Worldwide" pools to allow Prisma Access to automatically assign subnets to regions where demand spikes. Hard-coding small regional pools often leads to exhaustion in one region (e.g., "Why can't London users connect?") while others sit empty.[170]

2. Maintenance Lifecycle

GlobalProtect Client Version Management

Prisma Access hosts the GlobalProtect installer for your users. You must actively manage this version.

- **Upgrade Strategy:** Do not use "Always Latest." This turns your users into beta testers.
    - *Recommendation:* Stay **N-1** (one version behind the bleeding edge) or sticking to the configured "Preferred" release.
- **Update Method:**
    - **Transparently:** Updates happen in the background. Best for corporate-managed machines.
    - **Prompt User:** "A new version is available. Update now?" Best for BYOD to avoid interrupting a presentation.
    - *Config Location:* **Mobile Users > GlobalProtect > App Settings**.[171] [172]

Prisma SD-WAN Integration (CloudBlades)

If you also use Prisma SD-WAN, do *not* build manual IPSec tunnels to Prisma Access. Use the **CloudBlade**.

- **Workflow:**
    1. Go to **Prisma SD-WAN > CloudBlades**.
    2. Select "Prisma Access for Networks."
    3. Enter your Prisma Access Tenant ID.
    4. *Result:* The CloudBlade automatically spins up IPSec tunnels from every branch SD-WAN device to the nearest Prisma Access node. It handles IKE re-keying and failover automatically.[173] [174]

3. Monitoring for Maintenance

Use **Prisma Access Insights** (not just system logs) for proactive maintenance.

- **Tunnel Status:** Check "Service Connection Status" weekly. A "Down" status might mean your on-prem router changed keys or public IP.[175] [166]
- **User Experience:** Use ADEM (Autonomous DEM) to prove innocence. When a user says "SASE is slow," ADEM can show "Local Wi-Fi Latency: 400ms," proving the issue is their home router, not your configuration.

Summary Checklist

1. **Check SC Bandwidth:** Are you hitting the license cap?
2. **Review IP Pools:** Is any region >80% full?
3. **Update GlobalProtect:** Is the hosted version EoL?
4. **Verify BGP:** Are you receiving the correct internal routes from the SC?

⁂

Security Policies

Prisma Access modifies the traditional "Security Policy" concept by splitting it into distinct **enforcement points** (Mobile Users vs. Remote Networks) and using a unified cloud management approach (Strata Cloud Manager or Panorama).

The core difference is that while NGFW policies are "Interface-Zone based" (Trust to Untrust), SASE policies are "Identity and Direction based" (User to App).

1. Architecture: Variable Policy Scope

In Prisma Access, you don't push policies to a "box"; you push them to a **Service Type**.

- **Mobile Users (GlobalProtect):** Policies follow the user. Source is always the "User" identity.
- **Remote Networks (Branch/Site):** Policies follow the subnet. Source is the IP range of the branch site.
- **Service Connections (Data Center):** Policies govern backend traffic. *Critical:* This is often a "transit" node.

Management: Strata Cloud Manager (SCM) vs. Panorama

- **Panorama:** Uses **Device Groups**. You create a distinct Device Group for "Mobile Users" and another for "Remote Networks."
  - *Constraint:* You cannot mix these. A rule meant for both must be duplicated or placed in a parent Device Group.
- **Strata Cloud Manager (SCM):** Uses **Folders & Scopes**.[181]

  - *Global Scope:* Create a rule once (e.g., "Block Malware"), and it applies to *all* enforcement points (Mobile, Branch, and Campus). This is significantly more efficient than Panorama's hierarchy.

2. Policy Structure: Pre-Rules, Local, and Post-Rules

In a cloud environment, "Local" rules don't exist in the traditional sense. The hierarchy shifts:

Rule Type	Managed By	Application Scope	Example
Pre-Rules	Security Admin	**Global** (All Tenants/Nodes)	"Block Crypto-Mining," "Block Geo-Risky Countries."
Local Rules	Region/Site Admin	**Specific Folder** (e.g., "HR-Users")	"Allow HR Users to Workday."
Post-Rules	Security Admin	**Global**	"Deny All + Log."

Best Practice: Use **Tags** extensively. Since you cannot physically "see" the firewall, tags like `Region:EU` or `App:Financial` are the only way to filter the massive rulebase effectively.[182]

3. Decryption: The "Privacy vs. Performance" Balance

Decryption in SASE is computationally expensive but necessary.

- **Privacy (The "Do Not Touch" List):**
  - Create a "No Decrypt" policy for **Health**, **Finance**, and **Legal** categories. Privacy laws (GDPR/CCPA) often mandate this.
  - *Configuration:* Create a Decryption Profile that excludes these categories *before* creating the "Decrypt All" rule.[183] [184]
- **Performance (Bypass):**
  - **Pinned Certificates:** Some apps (Dropbox, Zoom, Office 365 Client) break if you intercept their certs.
  - *Action:* Use the **"SSL Decryption Exclusion"** list (Device > Certificate Management) rather than writing manual "No Decrypt" policy rules. This list is auto-updated by Palo Alto Networks.

4. Special Policy Types

- **Internet Access Rules (SCM Only):** SCM introduces a simplified rule type for web browsing. It merges "Security Policy" and "Decryption Policy" logic into a single workflow for common web access use cases.[185]
- **User-ID vs. IP:**
  - **Mobile Users:** *Always* write rules based on **User-ID** (AD Group), not Source IP. IPs change every time the user reconnects.

    - **Remote Networks:** You can use Source IP (Subnets) because the branch office tunnel is static. However, using User-ID (via Directory Sync) is still preferred for granularity. [186]

5. Migration Strategy: Policy Optimizer

Migrating from on-prem to SASE?

1. **Don't "Lift and Shift" Port Rules:** Do not blindly copy `Allow Any Any Service: 80/443` rules to the cloud. This defeats the Zero Trust purpose of SASE.
2. **Use Policy Optimizer:**
    - Run the traffic in "Learning Mode" (Allow All) for 2 weeks.
    - Use Policy Optimizer to see "Apps Seen."
    - Convert to **App-ID** based rules before switching to "Block" mode.

Summary Checklist

1. **Scope:** Are you applying the rule to *Mobile Users*, *Remote Networks*, or *Both*?
2. **Identity:** Are you using User Groups (Marketing) instead of IP ranges?
3. **Decryption:** Have you excluded "Finance/Health" to comply with privacy laws?
4. **Logging:** Is "Log at Session End" enabled? (Session Start is noisy and expensive in cloud storage).

⁂

Profiles

Prisma Access (SASE) utilizes the same core Threat Prevention profiles (AV, Vulnerability, Spyware) as the NGFW, but it introduces distinct profiles for **Zero Trust Identity** and **Cloud Data**.

While traffic profiles filter *packets*, SASE profiles filter *Context* (User Identity, Device Health, and Data Sensitivity).

1. Host Information Profiles (HIP) - *The "Device Identity" Gatekeeper*

HIP is the most critical SASE-specific profile. It inspects the endpoint's health before granting access, effectively replacing NAC (Network Access Control).

- **How it works:** The GlobalProtect agent scrapes the endpoint (Windows/Mac) for patch levels, encryption status, and AV signatures.
- **Best Practice Workflow:**
    1. **Create HIP Objects:** Define granular checks.
        - *Obj-1:* `Disk-Encrypted` (BitLocker = On).
        - *Obj-2:* `OS-Patched` (Windows 11 > 22H2).

        - *Obj-3:* `Corporate-CrowdStrike` (Process `Falcon.exe` is running).[196] [197]
    2. **Create HIP Profile:** Combine objects into logic.
        - *Profile:* "Corporate-Healthy" `=` `Disk-Encrypted` AND `OS-Patched` AND `Corporate-CrowdStrike`.
    3. **Enforce in Policy:**
        - *Rule:* Allow "Corporate-Healthy" to access "SAP-HR".
        - *Rule:* Allow "Any-Device" to access "Internet-Only".
- **Maintenance:** You must regularly update HIP objects as OS versions evolve (e.g., adding Windows 12 support when released).[198] [199]

2. SaaS Security & DLP Profiles - *The "Data" Gatekeeper*

Since users are off-network, you need profiles that inspect data leaving the endpoint for the cloud.

Enterprise DLP (Data Loss Prevention)

- **Profile Type: Data Filtering Profile**.
- **Configuration:**
    - **Patterns:** Use predefined patterns for PII (Credit Cards, Social Security Numbers) or regex for internal Project Codes.
    - **Action:** `Block` for High Confidence, `Alert` for Low Confidence to avoid blocking legitimate business traffic.
- **Integration:** This profile is attached to the Security Policy rule (e.g., "Allow Upload to Box, but Block PII").[200] [201]

SaaS Security Inline (CASB)

- **Goal:** Discover and control "Shadow IT" (unsanctioned apps).
- **Profile:** This is less of a "profile" per rule and more of a **SaaS Policy**.
- **Best Practice:** Enable the **SaaS Security Inline** subscription. It automatically tags thousands of apps with a "Risk Score."
    - *Policy:* Block all apps with `Risk Score > 4` (High Risk) or `Compliance != SOC2`.[202] [203]

3. Authentication Profiles - *The "User Identity" Gatekeeper*

SASE relies on **SAML** (Azure AD / Okta) rather than LDAP.

- **Best Practice:**
    - **MFA Integration:** Do not configure MFA on the Prisma Access portal directly if possible. Instead, rely on the **IdP (Identity Provider)** to handle MFA (Conditional Access in Azure AD).

    - **Cookie Lifetime:** In the Authentication Profile, set the "Authentication Cookie" (Auth Override) to balance security vs. friction.
        - *Corporate Device:* 24 Hours or 7 Days (Reduce login fatigue).
        - *BYOD:* Session cookies only (Force login every time).[204] [205]

4. Decryption Profiles (SASE Nuances)

Decryption in the cloud requires handling privacy at scale.

- **Exclude Default Categories:** Always exclude `Health`, `Finance`, `Legal`, and `Government` to comply with global privacy laws.
- **Bypass Pinned Certs:** Use the "SSL Decryption Exclusion" list (managed by PANW) to automatically bypass apps that break with interception (Dropbox, WebEx).[206]

Summary: Profile Matrix for SASE

Profile Type	Inspects...	Use Case	Managed In
HIP Profile	**Device**	"Block unpatched Windows laptops from accessing HR Data."	GlobalProtect
Data Filtering	**Content**	"Block 'Confidential' PDFs from being uploaded to Personal Gmail."	DLP
SaaS Inline	**Application**	"Block any file sharing site that is not SOC2 compliant."	SaaS Security
Authentication	**User**	"Force MFA every 24 hours for Finance users."	Mobile Users (Portal)

⁂

Updates

For Prisma Access (SASE), the update model splits responsibilities: Palo Alto Networks manages the **backend infrastructure** (Cloud Nodes/Dataplane), while you manage the **client-side components** and **configuration interface**.

1. Infrastructure Upgrades (Dataplane)

You cannot download a "PAN-OS image" for Prisma Access. Instead, you manage the rollout schedule.

- **Notification Window:** PANW notifies you **21 days** before a major backend upgrade (e.g., upgrading cloud nodes from 10.2 to 11.0 code).
- **The 7-Day Rule:** You *must* log in to **Strata Cloud Manager** (or the Prisma Access app in the Hub) and select your preferred 4-hour upgrade window (e.g., Saturday 2 AM - 6 AM).
    - *Constraint:* If you do not select a window by **7 days** prior to the start date, the system auto-assigns a slot, potentially during business hours.[212] [213]

- **Best Practice:** Always select the **"Preferred"** release track for production tenants. Use the **"Innovation"** track only for lab tenants to test new features early.

2. Client-Side Upgrades (GlobalProtect)

Prisma Access hosts the GlobalProtect installer, but it does *not* force users to upgrade automatically. You control this version.

- **Version Selection:**
  - Go to **Service Setup > GlobalProtect App Version**.
  - You will see a list of hosted versions. Select the one you want to be "Active."
  - *Warning:* Do not select "Always Latest." Stay **N-1** (one version behind) to avoid zero-day bugs in the agent.[214] [215]
- **Deployment Method:**
  - **Transparent:** Configure the GlobalProtect Portal **App Settings** to "Allow with Prompt" or "Transparent."
  - **Staged Rollout:** Prisma Access allows you to host *multiple* versions simultaneously (e.g., v6.1 for IT, v6.0 for everyone else) by using different Client Configs, but usually only *one* version is "Active" for download on the portal.[215] [214]

3. Management Interface Updates (Panorama vs. Cloud)

If Managed by Panorama:

- **Cloud Services Plugin:** You must manually upgrade the **Cloud Services Plugin** on Panorama to support new Prisma Access features.
  - *Dependency:* Often, you *cannot* upgrade the plugin until the backend Prisma Access infrastructure upgrade is complete. Watch the "Plugin Compatibility Matrix" closely.[216] [217]
- **Panorama Version:** You might be forced to upgrade Panorama itself (e.g., to 11.1) to support the latest Cloud Services Plugin.[218]

If Managed by Strata Cloud Manager (SCM):

- **Zero Maintenance:** The management plane (SCM) is SaaS. It updates automatically with no downtime or action required from you.[219]

4. Dynamic Updates (Threat Intelligence)

Prisma Access handles most of this, but you control the policy application.

- **WildFire & Antivirus:** These are **Cloud Controlled**. Prisma Access automatically applies Real-Time WildFire updates and Hourly AV updates. You cannot pause or defer these.[218]
- **GlobalProtect Data File:** This updates the Host Information Profile (HIP) checks (e.g., recognizing a new version of macOS). It updates hourly.

- **Action Required:** Ensure your security policies (HIP Profiles) reference valid OS versions. If the Data File adds support for "Windows 12" but your policy explicitly lists "Windows 11," users might fail checks until you update the policy logic.[220]

Summary Checklist

1. **Dataplane:** Did you select your weekend upgrade window in the Insights Dashboard?
2. **GlobalProtect:** Is the hosted agent version supported (not EoL)?
3. **Panorama:** Is your Cloud Services Plugin compatible with the current Prisma Access version?
4. **Notifications:** Are you subscribed to email alerts for "Upgrade Preferences Available"?

⁂

Upgrades

Since we have covered Prisma Access upgrades, the following guide details the **Prisma SD-WAN (ION)** upgrade lifecycle and the **Operational Impact** of SASE upgrades, which are often the most critical "missing manual" details.

1. Prisma SD-WAN (ION) Upgrades

Unlike firewalls, ION devices are distributed edge compute nodes. Their upgrade logic prioritizes "controller connectivity" over everything else.

Software Upgrade Strategy

- **The "Canary" Deployment:** Never upgrade all sites at once. Use tags to create upgrade rings.
  - *Ring 1 (Canary):* IT Office, Test Lab (Immediate).
  - *Ring 2 (Early Adopters):* Non-critical retail branches (Wait 48h).
  - *Ring 3 (Production):* Data Centers and HQs (Wait 1 week).
- **Version Dependency:** You cannot jump indefinitely.
  - *Path:* 5.4.x → 5.6.x → 6.1.x → 6.3.x → 6.5.x.[228]
  - *Constraint:* **Data Center First.** Always upgrade your Data Center IONs *before* your Branch IONs. If a Branch is on 6.1 and the DC is on 5.6, the VPN tunnels may fail to establish due to backward compatibility limits.[229]

Execution Workflow

1. **Schedule:** Go to **Configuration > ION Devices > Claimed Devices**.
2. **Action:** Select devices → **Schedule Software Upgrade**.
3. **Options:**
   - *Download Only:* Pre-stages the image (do this during the day).

- *Upgrade:* Applies the image and reboots (do this during maintenance window).
- *Max Upgrade Time:* Set a limit (e.g., 30 mins). If the device cannot complete the upgrade within this window (e.g., slow download), it aborts the attempt to prevent being "stuck" offline.[230] [231]

Cellular Modem Firmware

- **Separate Lifecycle:** The ION OS (e.g., 6.1.1) does *not* automatically upgrade the 4G/5G modem firmware.
- **Why Upgrade?** Carrier network changes (e.g., T-Mobile shutting down 3G) often require modem firmware updates to maintain LTE connectivity.
- **Process: Configure Device > Interface > Firmware**. Check the "Recommended" version against the "Running" version. This upgrade resets the cellular radio, causing a brief LTE outage.[232]

2. Operational Impact of Prisma Access Upgrades

When Palo Alto Networks upgrades the cloud backend, your traffic is shifted. Understanding this behavior prevents false alarms.

Component	Upgrade Impact	Behavior
Mobile Users	**Low**	Users might experience a "Reconnect" event. GlobalProtect automatically finds the next available gateway. Existing TCP sessions (SSH/RDP) will likely reset.
Remote Networks	**Medium**	The upgrade performs a "Make-Before-Break" shift, but BGP sessions inside the tunnel *will* flap. Ensure your on-prem router is configured for **Graceful Restart** to hold routes during the 30-second transition.
Service Connections	**High**	This is the most sensitive. If you have only *one* SC, you will lose connectivity to the DC for ~5-15 minutes during the node upgrade. **Mitigation:** You *must* have 2+ SCs in different zones for redundancy [233].

3. Rollback Procedures

- **ION Device:**
  - If an upgrade fails, the ION uses a **Dual Partition** system. It automatically boots back into the previous "Good" partition after 3 failed boot attempts.
  - *Manual Rollback:* In the portal, select the device → **Upgrade Software** → Select the *previous* version. This is treated as an "Upgrade to an older version".[230]
- **Prisma Access:**
  - You cannot "Rollback" the cloud infrastructure yourself. If a preferred release causes issues, you must open a P1 Support Ticket to request a backend rollback or engineering fix.

4. Summary Checklist for Upgrades

1. **[SD-WAN]** Are Data Center IONs on a version ≥ Branch IONs?
2. **[SD-WAN]** Have you pre-downloaded the image to branches with slow LTE links?
3. **[Access]** Is BGP Graceful Restart enabled on your Service Connection routers?
4. **[Access]** Do you have a secondary Service Connection to handle traffic while the primary upgrades?

⁂

monitoring and logging

Effective monitoring in the Prisma ecosystem (SASE & SD-WAN) requires shifting focus from "Up/Down" SNMP traps to **User Experience** and **Application Performance** metrics. The following guide details how to monitor the upgrades and configurations discussed in previous turns.

1. Prisma SD-WAN (ION) Monitoring

Prisma SD-WAN is "noisy" if you treat every link flap as a critical alert. You must tune it to focus on *impact*.

Reducing Alert Fatigue (Incident Policies)

- **The Problem:** An LTE backup link flapping every 5 minutes generates hundreds of tickets.
- **The Solution:** Configure **Incident Management Policies**.
  - **Action:** Go to **Alarms > Incident Management**.
  - **Suppression:** Create a rule to *suppress* alarms for non-critical circuits (e.g., LTE) unless the outage persists for >10 minutes.
  - **Correlation:** Enable "Event Correlation" so that if a WAN link goes down, you get *one* "Link Down" ticket, not 50 "Application Unreachable" tickets for every app using that link.[243] [244]

Application Health (Flow Browser)

- **Metric: Network RTT** (Time to reach Server) vs. **Server RTT** (Time for Server to respond).
  - *Scenario:* Users complain SAP is slow.
  - *Check:* If Network RTT is low (20ms) but Server RTT is high (500ms), the issue is the SAP server CPU/Disk, not the network.
- **Flow Browser:** Use this to prove "Innocence."
  - *Filter:* `source_ip = [User_IP]`
  - *Result:* Shows the exact path taken (e.g., "Path: MPLS, Reason: Policy Configured"). If it shows "Reason: Performance-SLA-Exceeded," it proves the primary path was degraded.[245]

2. Prisma Access (SASE) Monitoring

Since you cannot CLI into the cloud nodes, you rely on the **Insights Command Center**.

Upgrade Monitoring (The "Black Box" Phase)

When a backend upgrade is scheduled (as discussed in Turn 7):

- **Dashboard:** Go to **Insights > Upgrade Dashboard**.
- **Metrics to Watch:**
  - **Upgrade Status:** "In Progress" vs. "Completed."
  - **Mobile User Reconnections:** Watch for a spike in "GlobalProtect Reconnects." A small spike is normal; a sustained spike indicates clients are failing to auth to the new version.
  - **Service Connection Status:** Monitor BGP status here. If it stays "Down" for >15 mins, your on-prem router might need a BGP reset.[246]

BGP Monitoring (Service Connections)

- **Symptom:** "Flapping" BGP sessions during upgrades or heavy load.
- **Troubleshooting:**
  - Check **System Logs** in Panorama/SCM for "Route Refresh" events.
  - *Common Issue:* MTU mismatches causing BGP Keepalives to drop. Ensure your on-prem router interface MTU matches the Prisma Access standard (typically 1450-1500 bytes depending on IPSec overhead).[247]

3. Unified Monitoring (Strata Cloud Manager)

Strata Cloud Manager (SCM) is the single pane of glass for both SD-WAN and Access.

- **Best Practice Dashboard:**
  - Use the **Best Practices** widget to see a "Credit Score" for your security posture. It flags insecure configurations (e.g., "Allow Any" rules or "Telnet Enabled") across your entire estate.[248] [249]
- **Activity Dashboards:**
  - **New Flows:** Monitor the rate of new TCP connections per second. A sudden spike here often indicates a ransomware infection (scanning) or a DDoS attack originating *from* your user base.[250]

4. Summary: What to Alert On?

Do not alert on everything. Configure your SIEM/Ticketing system to trigger *only* on these high-fidelity signals:

Component	Alert Name	Threshold	Why?
Prisma Access	**IP Pool Exhaustion**	> 85% Usage	Users will be denied connection soon.
Prisma Access	**Service Connection Down**	Immediate	Data Center connectivity is lost for all mobile users.
Prisma SD-WAN	**Site Offline**	> 5 Mins	Isolate simple reboots from actual power/ISP outages.
Prisma SD-WAN	**MOS Score Drop**	< 3.5 (Voice)	Call quality is degrading before calls actually drop.

⁂

1. https://www.libertyuae.com/blog/firewall-maintenance-checklist/
2. https://www.youtube.com/watch?v=OsjVGTSGcDQ
3. https://www.scribd.com/document/597227790/Palo-Alto-Checklist
4. https://docs.paloaltonetworks.com/content/techdocs/en_US/best-practices/security-policy-best-practices/security-policy-best-practices/maintain-security-policy-best-practices
5. https://www.youtube.com/watch?v=UzrM6oQU1h0
6. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/planning-checklist-for-globalprotect-on-prisma-access
7. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-upgrades/select-the-active-globalprotect-app-version-for-prisma-access
8. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-upgrades/allow-users-to-upgrade-the-globalprotect-app
9. https://ine.com/blog/palo-alto-networks-firewall-management-best-practices
10. https://networkdevicesinc.com/community/blog/palo-alto-firewall-setup-pan-os-guide
11. https://www.tufin.com/blog/a-palo-alto-firewall-checklist-for-improving-network-security
12. https://www.orangecyberdefense.com/be/palo-alto/firewall-best-practice/full-best-practices-assessment
13. https://4719eaee91034be722d8-c86a406a93c55de2464febd03debd4f0.ssl.cf1.rackcdn.com/127_best-practice-assessment-ngfw-panorama-partner-faq.pdf
14. https://www.paloaltonetworks.com/services/bpa
15. https://docs.paloaltonetworks.com/strata-cloud-manager/aiops/best-practices-in-ngfw
16. https://www.reddit.com/r/paloaltonetworks/comments/esj3xs/daily_maintenance_tasks/
17. https://docs.paloaltonetworks.com/network-security/security-policy/administration/objects/schedules
18. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-setup
19. https://docs.paloaltonetworks.com/iot/iot-security-best-practices/iot-security-best-practices/monitor-iot-security-deployment-using-best-practices
20. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/performance-policy-with-forward-error-correction-fec/best-practices-and-recommendations

21. https://www.paloaltonetworks.com/cyberpedia/firewall-best-practices
22. https://www.youtube.com/watch?v=fmxLfukF-Zg
23. https://docs.paloaltonetworks.com/fedramp/prisma-sase/fedramp-moderate-and-high-requirements/fedramp-moderate-and-high-support
24. https://cyber.levelblue.com/m/1353e7cf2e566ec2/original/SVG-SASE-Palo-Alto-Networks-Service-Guide-Sept-2024.pdf
25. https://www.youtube.com/watch?v=QYy-5XTUICo
26. https://live.paloaltonetworks.com/t5/general-topics/pci-dss-3-2-1-responsibility-matrix-for-saas-services/td-p/517802
27. https://www.orangecyberdefense.com/be/palo-alto/prisma-access
28. https://docs.prismacloud.io/en/enterprise-edition/content-collections/get-started/access-prisma-cloud
29. https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Palo-Alto-Networks-datasheet-PRISMA-prisma-access-privacy.pdf
30. https://docs.paloaltonetworks.com/vm-series/11-1/vm-series-deployment/about-the-vm-series-firewall/sr-iov-and-dpdk-driver-support
31. https://www.ateam-oracle.com/oci-and-palo-alto-vm-series-firewall-throughput
32. https://docs.paloaltonetworks.com/vm-series/11-1/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/about-the-vm-series-firewall-on-aws/performance-tuning-of-the-vm-series-on-aws
33. https://docs.paloaltonetworks.com/content/techdocs/en_US/cn-series/upgrade/upgrade-the-cn-series-firewall
34. https://docs.paloaltonetworks.com/content/techdocs/en_US/cn-series/deployment/cn-deployment/deploy-the-cn-series-firewalls-new/deploy-cn-series-firewalls-with-and-without-the-helm-repository
35. https://github.com/PaloAltoNetworks/cn-series-helm
36. https://secureitconsult.com/kubernetes-security-cn-firewalls/
37. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/cloud-ngfw-native-policy-management/about-rulestacks-and-rules
38. https://docs.paloaltonetworks.com/cloud-ngfw-aws/getting-started
39. https://docs.paloaltonetworks.com/content/techdocs/en_US/cn-series/deployment/cn-deployment/deployment-modes-of-cn-series-firewalls/deploy-the-cn-series-firewall-as-a-service
40. https://www.reddit.com/r/kubernetes/comments/1oefmtx/how_do_you_upgrade_your_helm_charts/
41. https://www.westconcomstor.com/content/dam/wcgcom/pan-vip/cn-series.pdf
42. https://docs.aws.amazon.com/waf/latest/developerguide/cloud-ngfw-policies.html
43. https://www.youtube.com/watch?v=IqUUfRfAiSw
44. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/cloud-ngfw-native-policy-management/security-profiles
45. https://www.linkedin.com/posts/tanzuguo_palo-alto-networks-panorama-pre-rules-vs-activity-7368456007330582529-Z3DT
46. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-web-interface-help/panorama-web-interface/defining-policies-on-panorama
47. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/security-policy
48. https://docs.paloaltonetworks.com/ngfw/administration/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules

49. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices
50. https://www.sunmanagement.net/palo-alto-firewalls-migration-to-app-id-security-tool/
51. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/panorama-integration-overview
52. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/panorama-integration-overview/use-panorama-for-cngfw-policy-management
53. https://secureitconsult.com/kubernetes-security-cn-firewalls/
54. https://docs.paloaltonetworks.com/best-practices
55. https://www.youtube.com/watch?v=J-58RtoTeAw
56. https://www.darkreading.com/vulnerabilities-threats/palo-alto-networks-announces-pan-os-11-0-nova-to-help-keep-organizations-one-step-ahead-of-zero-day-threats
57. https://www.tufin.com/blog/a-palo-alto-firewall-checklist-for-improving-network-security
58. https://www.reddit.com/r/paloaltonetworks/comments/1hj9uln/firewall_zone_design_and_best_practices/
59. https://www.reddit.com/r/paloaltonetworks/comments/woxbse/help_what_are_the_use_cases_of_prerules_and/
60. https://docs.paloaltonetworks.com/best-practices/10-1/best-practices-for-migrating-to-application-based-policy
61. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles
62. https://www.linkedin.com/posts/routehat_cybersecurity-paloaltonetworks-firewallsecurity-activity-7394605388895203328-MKyB
63. https://kb.wisc.edu/security/90962
64. https://www.youtube.com/watch?v=hWzdRyJvpvs
65. https://www.youtube.com/watch?v=_-cbTXDpNsM
66. https://www.paloguard.com.au/URL-Filtering.php
67. https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention/set-up-credential-phishing-prevention
68. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-wildfire
69. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-wildfire/configure-a-wildfire-analysis-profile-cm
70. https://www.reddit.com/r/paloaltonetworks/comments/nk3l1b/is_it_secure_to_apply_a_vulnerability_protection/
71. https://docs.paloaltonetworks.com/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/transition-safely-to-best-practice-security-profiles
72. https://docs.paloaltonetworks.com/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles
73. https://docs.paloaltonetworks.com/best-practices/10-2/data-center-best-practices/data-center-best-practice-security-policy/how-to-create-data-center-best-practice-security-profiles
74. https://docs.paloaltonetworks.com/content/techdocs/en_US/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/transition-safely-to-best-practice-security-profiles/transition-antivirus-profiles-safely-to-best-practices

75. https://www.reddit.com/r/paloaltonetworks/comments/1hj9uln/firewall_zone_design_and_best_practices/
76. https://www.reddit.com/r/paloaltonetworks/comments/1d4tfzp/wildfire_increase_dynamic_update_interval/
77. https://www.youtube.com/watch?v=XBCTrFOA2YY
78. https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-web-interface-help/panorama-web-interface/panorama-device-deployment/schedule-dynamic-content-updates
79. https://docs.paloaltonetworks.com/ngfw/administration/app-id/manage-new-app-ids-introduced-in-content-releases/disable-or-enable-app-ids
80. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClSgCAK
81. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path
82. https://www.reddit.com/r/paloaltonetworks/comments/1g6oou2/upgrade_path_from_101_to_111/
83. https://www.reddit.com/r/paloaltonetworks/comments/1d3d7v4/best_practice_for_dynamic_content_updates_between/
84. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/software-and-content-updates/best-practices-for-app-and-threat-content-updates
85. https://community.indeni.com/t/wildfire-content-update-schedule-is-not-following-best-practices-paloaltonetworks-panos/3479
86. 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
87. https://blogs.cisco.com/customerexperience/navigating-firewall-migrations-best-practices-and-palo-alto-to-cisco-next-gen-firewall-specifics
88. https://live.paloaltonetworks.com/t5/general-topics/upgrade-pan-os-from-10-1-to-11-1/td-p/578600
89. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-upgrade/software-and-content-updates/dynamic-content-updates
90. 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
91. https://www.reddit.com/r/paloaltonetworks/comments/1g68cti/consideration_when_upgrading_firewall_via_panorama/
92. https://www.firewall.cx/security/palo-alto-networks/how-to-upgrade-standalone-palo-alto-firewall-pan-os.html
93. https://www.analysisman.com/2020/07/pan-upgrade-ha.html
94. https://indepthtechno.wordpress.com/2020/07/05/palo-alto-panorama-and-firewall-upgrade-procedure/
95. https://live.paloaltonetworks.com/t5/panorama-discussions/upgrade-to-11-1-4-h1-for-both-panorama-and-managed-firewalls/td-p/607093
96. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/use-the-prisma-access-app-to-get-upgrade-alerts-and-updates
97. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/release-definitions
98. https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-insights/insights/upgrade-preferences

99. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000XhHJCA0&lang=en_US

100. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000oN17CAE&lang=en_US

101. https://www.paloaltonetworks.com/services/support/end-of-life-announcements

102. https://docs.paloaltonetworks.com/compatibility-matrix

103. https://docs.paloaltonetworks.com/compatibility-matrix/reference/supported-os-releases-by-model/palo-alto-networks-next-gen-firewalls

104. https://www.reddit.com/r/paloaltonetworks/comments/18mikdm/upgrading_ha_firewall_question/

105. https://thedxt.ca/2022/10/upgrade-palo-alto-ha-pair-active-passive/

106. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/configure-the-ion-at-a-data-center

107. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/cloudblades/cloudblade-integrations/pagerduty-notifier-cloudblade-integration/best-practices-and-troubleshooting-scenarios

108. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-sites/sase-bulk-site-configuration-template

109. https://www.youtube.com/watch?v=OuGhKGpRhqM

110. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/deployment/understand-installation-workflow

111. https://documentation.solarwinds.com/en/success_center/npm/content/npm-prisma-sdwan.htm

112. https://www.youtube.com/watch?v=svb1-GfbOk8

113. https://www.reddit.com/r/paloaltonetworks/comments/1nxqyp7/using_new_scm_interface/

114. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-devices/assign-the-ion

115. https://pan.dev/sdwan/docs/prismasdwanconfig/

116. https://www.reddit.com/r/paloaltonetworks/comments/1fu0dik/sdwan_features_and_setup_difficulty/

117. https://www.paloguard.com/ION-1000.asp

118. https://docs.paloaltonetworks.com/content/techdocs/en_US/sd-wan/administration/sd-wan-deployment-workflow

119. https://www.site24×7.com/learn/prisma-sdwan-troubleshooting.html

120. https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/get-started-with-prisma-sd-wan

121. https://docs.paloaltonetworks.com/hardware/ion-1000-hardware-reference/ion-1000-overview/ion-1000-leds

122. https://docs.paloaltonetworks.com/hardware/ion-1200-hardware-reference/ion-1200-overview/ion-1200-led

123. https://docs.paloaltonetworks.com/prisma-sd-wan/ion-cli-reference/access-the-ion-cli-commands/assign-a-static-ip-address-using-the-console

124. https://www.scribd.com/document/862371757/prisma-sd-wan-ion-cli-reference

125. https://www.soniccomponents.com/wp-content/uploads/2025/06/onpremises-controller-for-prisma-sd-wan-deployment-guide.pdf

126. https://rowelldionicio.com/allow-ping-traceroute-prisma-sd-wan-ion/

127. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/prisma-sd-wan-ports-and-interfaces/configure-internet-ports

128. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000XhdPCAS
129. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/prisma-sd-wan-ports-and-interfaces/port-panel-overview-and-status-indicators
130. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/prisma-sd-wan-ports-and-interfaces/configure-a-controller-port
131. https://www.youtube.com/watch?v=OuGhKGpRhqM
132. https://www.ibm.com/docs/en/sevone-npm/8.0.0?topic=troubleshooting-sd-wan-palo-alto-prisma-guide
133. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-devices/connect-the-ion
134. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/configure-the-ion-at-a-data-center
135. https://docs.paloaltonetworks.com/prisma-sd-wan/deployment/understand-installation-workflow/connect-the-device-to-the-on-premises-controller
136. https://docs.paloaltonetworks.com/sd-wan/administration/enable-sd-wan-without-auto-vpn/manage-sd-wan-link-failovers/sd-wan-traffic-distribution-profiles
137. https://docs.paloaltonetworks.com/sd-wan/administration/enable-sd-wan-without-auto-vpn/manage-sd-wan-link-failovers/define-your-custom-sd-wan-application-thresholds
138. https://docs.paloaltonetworks.com/content/techdocs/en_US/sd-wan/administration/enable-sd-wan-without-auto-vpn/manage-sd-wan-link-failovers/define-path-selection-for-sd-wan-traffic
139. https://www.scribd.com/document/892938630/Pan-Os-Sd-Wan-Path-Selection-Primer
140. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/performance-policy-with-forward-error-correction-fec/best-practices-and-recommendations
141. https://www.gtt.net/resources/blog/sd-wan-and-forward-error-correction-mitigating-packet-loss/
142. https://www.reddit.com/r/paloaltonetworks/comments/1f0196r/prisma_sdwan_faulty_line_path_selection/
143. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/incidents-and-alerts/troubleshoot-incidents
144. https://pan.dev/panos/docs/tutorials/redundant-internet/
145. https://live.paloaltonetworks.com/t5/prisma-access-discussions/understand-flow-decision-bitmap-of-prisma-sd-wan/td-p/438326
146. https://www.westconcomstor.com/content/dam/wcgcom/Global/CorpSite/pdfs/Palo-Alto-Networks-SD-WAN-administrators-guide-EN.pdf
147. https://www.reddit.com/r/paloaltonetworks/comments/1bduoc7/palo_alto_panorama_sdwan_commit_issues/
148. https://docs.paloaltonetworks.com/sd-wan/administration/monitoring-and-reporting/monitor-prisma-access-hub-application-and-link-performance
149. https://www.networkacademy.io/ccie-enterprise/sdwan/forward-error-correction-fec
150. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-stacked-policies/add-a-path-policy-rule
151. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/view-and-manage-logs/log-types-and-severity-levels

152. https://edgedelta.com/company/blog/how-to-improve-palo-alto-logs-for-stronger-threat-monitoring-and-analysis
153. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/threat-log-fields
154. https://www.sumologic.com/help/docs/integrations/security-threat-detection/palo-alto-networks-9/
155. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding
156. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding/configure-log-forwarding-pan-os
157. https://www.linkedin.com/pulse/when-strata-cloud-manager-scm-replace-panorama-complex-joe-brunner-bpyhe
158. https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/panorama-overview/centralized-logging-and-reporting
159. https://docs.paloaltonetworks.com/autonomous-dem
160. https://docs.paloaltonetworks.com/autonomous-dem/china-administration/get-started-with-adem/go-to-autonomous-dem-in-prisma-access
161. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/get-started-with-prisma-sd-wan/site-summary-dashboard
162. https://www.scribd.com/document/855721168/Prisma-Sd-Wan-Admin
163. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/monitor/monitor-logs/log-types
164. https://www.youtube.com/watch?v=90--_o4rnKA
165. https://docs.cloud.google.com/chronicle/docs/ingestion/default-parsers/pan-firewall
166. https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-insights/insights/service-connections-dashboard
167. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-service-connections/configure-a-service-connection
168. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/service-connection-advanced-deployments/create-a-high-bandwidth-network-using-multiple-service-connections
169. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008WyDCAU&lang=en_US
170. https://www.youtube.com/watch?v=gGwFvi8rvqU
171. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-upgrades/allow-users-to-upgrade-the-globalprotect-app
172. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-upgrades/select-the-active-globalprotect-app-version-for-prisma-access
173. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/cloudblades/prisma-access-integrations/configure-and-install-prisma-access-cloudblade/configure-and-integrate-prisma-access-cloudblade-cloud-managed-cloudblade
174. https://www.coursehero.com/file/213339827/prisma-access-cloudblade-integration-guidepdf/
175. https://www.youtube.com/watch?v=9CkpAO3DQbs

176. https://www.youtube.com/watch?v=Kan53KPRdKU
177. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/activation-and-onboarding/activate-your-prisma-sd-wan-license/bandwidth-subscription-monitoring-and-reporting
178. https://pan.dev/access/docs/insights/examples/service-connections-dashboard/sc-bandwidth-consumption/
179. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/how-bgp-advertises-mobile-user-ip-address-pools
180. https://www.youtube.com/watch?v=oYY243KnHfc
181. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
182. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-rules/enumeration-of-rules-within-a-rulebase
183. https://www.youtube.com/watch?v=Rp9_Ez7hfXU
184. https://docs.paloaltonetworks.com/network-security/decryption/administration/decryption-overview/decryption-policy-rules
185. https://docs.paloaltonetworks.com/network-security/security-policy/administration/internet-access-rules/migration-scenarios-web-security-policy-rules-to-internet-access-rules
186. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-user-based-policy
187. https://www.reddit.com/r/paloaltonetworks/comments/1mp3gcc/in_a_sase_mobile_user_environment_is_there_a_way/
188. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/planning-checklist-for-globalprotect-on-prisma-access
189. https://www.youtube.com/watch?v=QYy-5XTUICo
190. https://packetpushers.net/blog/overcoming-encrypted-traffic-blind-spots-with-prisma-access-browser/
191. https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/718514030930442
192. https://www.youtube.com/watch?v=fmxLfukF-Zg
193. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-remote-networks
194. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users
195. https://www.reddit.com/r/paloaltonetworks/comments/10jz6k4/prisma_access_service_connections_remote_networks/
196. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access-agent/administration/configure-the-agent/configure-hip-notifications/create-and-manage-hip-profiles
197. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-settings
198. https://docs.paloaltonetworks.com/globalprotect/administration/globalprotect-quick-configs/globalprotect-for-internal-hip-checking-and-user-based-access
199. https://docs.paloaltonetworks.com/prisma-access/administration/configure-dynamic-privilege-access-settings/set-up-the-prisma-access-agent-dpa/configure-hip-notifications-for-the-prisma-access-agent-dpa/create-and-manage-hip-profiles-dpa
200. https://docs.paloaltonetworks.com/content/techdocs/en_US/enterprise-dlp/getting-started/edit-the-enterprise-dlp-data-filtering-settings

201. https://docs.paloaltonetworks.com/content/techdocs/en_US/enterprise-dlp/administration/configure-enterprise-dlp/create-an-enterprise-dlp-data-profile/create-a-data-profile
202. https://docs.paloaltonetworks.com/prisma-access/activation-and-onboarding/your-prisma-access-license/all-available-apps-and-services/cheat-sheet-saas-security-with-prisma-access
203. https://docs.paloaltonetworks.com/saas-security/getting-started/whats-saas-security/whats-saas-security-inline
204. https://www.youtube.com/watch?v=qzhe7Vdq580
205. https://docs.paloaltonetworks.com/ngfw/administration/authentication/configure-saml-authentication
206. https://www.youtube.com/watch?v=Rp9_Ez7hfXU
207. https://www.reddit.com/r/paloaltonetworks/comments/1i98n6d/globalprotect_custom_hip_checks_im_going_bonkers/
208. https://www.reddit.com/r/paloaltonetworks/comments/1j4vuom/prisma_access_service_connections_zones/
209. https://www.youtube.com/watch?v=9RknE33O0ZU
210. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users
211. https://www.youtube.com/watch?v=hIdjFFxzZhc
212. https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-insights/insights/upgrade-preferences
213. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/use-the-prisma-access-app-to-get-upgrade-alerts-and-updates
214. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-upgrades/select-the-active-globalprotect-app-version-for-prisma-access
215. https://www.youtube.com/watch?v=fmxLfukF-Zg
216. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/upgrade-types
217. https://www.reddit.com/r/paloaltonetworks/comments/1jd9ywj/prisma_access_backend_upgrade/
218. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/cadence-for-software-and-content-updates-for-prisma-access
219. https://www.reddit.com/r/paloaltonetworks/comments/whqyex/cloud_managed_vs_panorama_for_prisma_access/
220. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access-agent/administration/configure-the-agent/configure-hip-notifications/create-and-manage-hip-profiles
221. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades
222. https://www.youtube.com/watch?v=oYY243KnHfc
223. 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
224. https://docs.prismacloud.io/en/enterprise-edition/content-collections/runtime-security/upgrade/upgrade-process
225. https://www.reddit.com/r/paloaltonetworks/comments/1d3d7v4/best_practice_for_dynamic_content_updates_between/

226. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-upgrades
227. https://docs.paloaltonetworks.com/panorama/11-0/panorama-admin/manage-firewalls/change-between-panorama-management-and-cloud-management
228. https://docs.paloaltonetworks.com/prisma-sd-wan/release-notes/6-5/prisma-sd-wan-ion-device-release-6-5/upgrade-downgrade-considerations-in-prisma-sd-wan-ion-release-6-5
229. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/release-notes/6-3/prisma-sd-wan-ion-device-release-6-3/upgrade-downgrade-considerations-in-prisma-sd-wan-ion-release-6-3
230. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/upgrade-ion-device-software
231. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/upgrade-ion-device-software/schedule-software-upgrade
232. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/prisma-sd-wan-ports-and-interfaces/configure-cellular-interfaces/update-firmware
233. https://www.reddit.com/r/paloaltonetworks/comments/16pfpfh/service_connection_redundancy_for_prisma_access/
234. https://docs.paloaltonetworks.com/prisma-sd-wan/deployment/upgrade-on-premises-controller/upgrade-the-device-software
235. https://www.reddit.com/r/paloaltonetworks/comments/15z45vu/prisma_acces_sc_tunnel_issues/
236. https://pan.dev/sdwan/docs/prismasdwanconfig/
237. https://www.youtube.com/watch?v=ms9oLBXs-EM
238. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Monitor-And-Maintain/monitor-maintain-book/cellular-modem-firmware-upgrade.html
239. https://docs.paloaltonetworks.com/prisma-access/release-notes/5-1/prisma-access-about/new-features
240. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/performance-policy-with-forward-error-correction-fec/best-practices-and-recommendations
241. https://www.reddit.com/r/paloaltonetworks/comments/137vu6c/prisma_sdwan_upgrade_best_practices/
242. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/administration/get-started-with-prisma-sd-wan/prisma-sd-wan-releases-and-upgrades
243. https://docs.paloaltonetworks.com/prisma-sd-wan/incidents-and-alerts
244. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/incidents-and-alerts/incidents-and-alerts-prisma-sd-wan
245. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-sites/view-flows-tab
246. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-releases-and-upgrades/use-the-prisma-access-app-to-get-upgrade-alerts-and-updates
247. https://www.reddit.com/r/paloaltonetworks/comments/10wjmu3/ebgp_flapping_between_service_connection_prisma/
248. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards/best-practices
249. https://www.scribd.com/document/935840767/Strata-Cloud-Manager-Administration

250. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/get-started-with-prisma-sd-wan/prisma-sd-wan-applications-dashboard

251. https://docs.prismacloud.io/en/enterprise-edition/content-collections/application-security/risk-management/monitor-and-manage-code-build/enforcement

252. https://www.ninjaone.com/blog/reduce-alert-noise-using-client-facing-strategies/

253. https://www.logicmonitor.com/support/palo-alto-prisma-sd-wan-monitoring

254. https://docs.paloaltonetworks.com/prisma-access/administration/monitor/activity-dashboards-and-reports

255. https://community.ruijie.com/forum.php?mod=viewthread&tid=560

256. https://www.reddit.com/r/SysAdminBlogs/comments/1pkobe3/how_to_reduce_alert_noisefatigue_tips_from_the/

257. https://docs.prismacloud.io/en/enterprise-edition/content-collections/application-security/risk-management/monitor-and-manage-code-build/suppress-code-issues