NGFW and SASE Solution Functionality

This domain accounts for **18%** of the **NetSec-Pro** certification exam and focuses on understanding the specific use cases and architectures of the Strata (NGFW) and Prisma (SASE) portfolios.

The core distinction is the enforcement point: **Strata NGFW** secures traffic at physical or virtual boundaries (Data Center, Campus, Cloud VPC), while **Prisma SASE** secures traffic at the cloud edge for hybrid workforces and branch locations. Both utilize the **Single Pass Parallel Processing (SP3)** architecture to inspect traffic once for all threats.

1. Firewall Form Factors and Functions (Strata)

You must be able to map the correct firewall series to its deployment scenario. All these form factors run PAN-OS (or compatible code) and enforce the same App-ID/Content-ID/User-ID policies.

- **PA-Series (Hardware):**
  - **Function:** Dedicated physical appliances for high-throughput perimeter, data center, and campus edge security.
  - **Key Use Case:** "Zero Trust" segmentation in physical networks and high-speed core routing/inspection.[1] [2]
- **VM-Series (Virtual):**
  - **Function:** Virtualized NGFW for private clouds (VMware/KVM/Hyper-V) and public clouds (AWS/Azure/GCP).
  - **Key Use Case:** East-West traffic segmentation within virtualized data centers and securing cloud VPCs/VNets.[3] [4]
- **CN-Series (Container):**
  - **Function:** Containerized NGFW designed for Kubernetes environments (K8s, OpenShift).
  - **Key Use Case:** Layer 7 visibility and threat protection *inside* Kubernetes clusters (inter-pod traffic) where traditional VM firewalls cannot see.[5] [4]
- **Cloud NGFW (Managed Service):**
  - **Function:** A cloud-native service (e.g., Cloud NGFW for AWS/Azure) where Palo Alto manages the infrastructure, and you manage the policy.
  - **Key Use Case:** Simplest deployment for public cloud protection without managing VM infrastructure or scaling groups.[6] [4]

2. SASE Solution Functionality (Prisma)

Palo Alto Networks' SASE solution (Prisma SASE) converges networking (SD-WAN) and security (Prisma Access) into a single cloud-delivered platform.

- **Prisma Access (Security Service Edge - SSE):**
  - **Function:** Acts as a global cloud firewall. It connects remote users (via GlobalProtect) and branch offices (via IPsec/SD-WAN) to the nearest cloud Point of Presence (PoP).
  - **Key Capabilities:** Firewall as a Service (FWaaS), Secure Web Gateway (SWG), and ZTNA (Zero Trust Network Access).[4] [5]
  - **Decryption:** Centralized SSL decryption is critical here to inspect traffic from remote users without backhauling it to a data center.[7]
- **Prisma SD-WAN:**
  - **Function:** Replaces traditional routers to provide "Application-Defined" connectivity. It measures app performance (SLA) rather than just packet loss/jitter.
  - **Key Capabilities:** Automates path selection (e.g., send Zoom over fiber, email over 5G) and integrates natively with Prisma Access for security.[4]

3. Management Options

The exam tests your ability to choose the right management plane for these solutions.

- **Panorama:**
  - **Scope:** The traditional centralized manager for all **Strata** firewalls (PA, VM, CN) and historically Prisma Access.
  - **Function:** Manages configuration hierarchies (Device Groups/Templates) and aggregates logs.[8] [4]
- **Strata Cloud Manager (SCM):**
  - **Scope:** The modern, AI-powered unified management platform.
  - **Function:** Native manager for **Prisma SASE** (Access + SD-WAN) and increasingly for Strata NGFWs (Next-Gen CASB, AIOps). It unifies policy across hardware and cloud in a single interface.[9] [4]

Summary Comparison: Strata vs. Prisma SASE

Feature	Strata NGFW (Hardware/VM/CN)	Prisma SASE (Access + SD-WAN)
Primary Goal	Secure physical/virtual boundaries (DC, Campus).	Secure users and branches (Hybrid Work).
Enforcement Point	Local device (On-prem/VPC).	Cloud PoP (Global Network).
Inspection Engine	SP3 (Single Pass) on local hardware/vCPU.	SP3 (Single Pass) in the cloud.
Connectivity	Standard Routing/VPN (IPsec, BGP, OSPF).	App-Defined SD-WAN & ZTNA.

Feature	Strata NGFW (Hardware/VM/CN)	Prisma SASE (Access + SD-WAN)
Management	Panorama or Local Web UI.	Strata Cloud Manager (SCM) or Panorama.
Decryption	Resource-intensive; requires local hardware sizing [7].	Cloud-scalable; offloads processing from local edge.

Exam Tip: DNS Security Functionality

A specific exam objective often covers **Advanced DNS Security**. Remember that this service requires a **Sinkhole** configuration in the Anti-Spyware profile.

- **Function:** It redirects malicious DNS queries (e.g., C2 domains) to a "sinkhole" IP address configured on the firewall.
- **Result:** This prevents the client from resolving the malicious IP and generates a Threat Log that identifies the infected client by its request to the sinkhole IP.[6] [3]

⁂

Perimeter and core security

In the context of the **NetSec-Pro** certification and Palo Alto Networks architecture, the distinction between **Perimeter** and **Core** security relies on traffic flow direction (North-South vs. East-West) and the "Zero Trust" implementation strategy.

1. Perimeter Security (North-South Traffic)

The perimeter is the boundary between your trusted internal network and untrusted external networks (Internet, Partners, Guests).

- **Traffic Flow: North-South** (Entering or leaving the network).
- **Primary Goal: Infiltration Prevention.** Stop initial breaches, malware delivery, and unauthorized access from the outside.[18]
- **Key Design Elements:**
    - **Decryption:** Crucial at the edge to inspect encrypted traffic (TLS/SSL) for hidden threats before they enter.
    - **GlobalProtect:** Secures remote user access (VPN) back into the perimeter or directly to cloud apps (Prisma Access).
    - **Threat Prevention:** Heavy use of IPS, Antivirus, and URL Filtering profiles to block known bad IPs/Domains/Files.[18]
    - **Hardware:** Typically mid-range **PA-Series** (e.g., PA-3400, PA-5400) or **Prisma Access** for cloud-delivered edge security.

2. Core Security (East-West Traffic)

Core security focuses on the internal Data Center or Cloud environment. In a Zero Trust model, we assume the perimeter *will* be breached, so the Core's job is to contain the damage.

- **Traffic Flow: East-West** (Server-to-Server, Application-to-Database).
- **Primary Goal: Lateral Movement Prevention.** Ensure that if one server is compromised, the attacker cannot freely jump to other servers.[19] [18]
- **Key Design Elements:**
  - **Segmentation (Zero Trust):** Dividing the flat network into small, secure zones (e.g., Web-Zone, App-Zone, DB-Zone).
  - **App-ID Enforcement:** Instead of opening "Port 3306" for SQL, you open only the `mysql` application. This prevents attackers from tunneling SSH or C2 traffic over allowed ports.
  - **High Throughput:** Core firewalls require massive throughput to handle internal data transfers without creating bottlenecks.
  - **Hardware:** High-end **PA-Series** (PA-7500, PA-5400) or **VM-Series/CN-Series** for virtualized/containerized micro-segmentation.[19]

Comparison: Perimeter vs. Core (Data Center)

Feature	Perimeter Security	Core (Data Center) Security
Traffic Direction	**North-South** (User to Internet, Internet to Server)	**East-West** (Server to Server, Workload to Workload) [18]
Primary Risk	Initial Infection / Data Exfiltration	Lateral Propagation / Ransomware Spread
Policy Strategy	"Block Known Bad" (Threat Intelligence, URL Filtering)	"Allow Only Known Good" (Strict App-ID Whitelisting) [20]
Throughput Needs	Moderate to High (Internet speed limits)	Extreme (Line-rate 40G/100G/400G+)
Latency Sensitivity	Moderate	Critical (must not slow down app transactions)
Typical Platform	PA-Series, VM-Series (Cloud Edge), Prisma Access	PA-5400/7500, VM-Series (NSX/Hypervisor)

Exam Note: Zero Trust Architecture

For the NetSec-Pro exam, remember that **Zero Trust** eliminates the idea of a "trusted core."

- **Old Model:** "Hard crunchy shell (Perimeter), soft chewy center (Core)." Once inside, you are trusted.
- **Palo Alto Model:** Apply **Perimeter-level enforcement** everywhere. Even inside the core, every packet is inspected (App-ID + User-ID) and verified, creating "micro-perimeters" around critical applications.[21] [22]

⁂

zone security and segmentation

Zone security and segmentation on Palo Alto Networks NGFWs means grouping interfaces into **security zones** and then controlling traffic *between* zones with explicit Security policy rules. Traffic can flow freely within a zone, but inter-zone traffic is blocked unless a rule allows it.[33]

Zones and segmentation

A security zone is a logical segment of your network that the firewall uses as the "from" and "to" context for policy (source zone/destination zone).[34] [33]
Segmenting into more granular zones increases visibility and control, and it reduces the attack surface by limiting who/what can talk to what.[35] [36]

Common zone designs

Typical designs segment by **trust level** and/or **function**, such as Untrust (Internet), DMZ, Trust (Users), and separate Server tiers (Web/App/DB).[36] [34]
Palo Alto explicitly calls out creating zones for functional areas (internet gateway, sensitive data storage, business applications) and also for organizational groups (finance, IT, engineering) where access privileges differ.[36]

Enforcing zone security

Inter-zone traffic is only allowed when a Security policy rule references a source zone and destination zone and permits it.[33]
For "zero trust" style segmentation, combine zones with App-ID and User-ID so access privileges are tied to user/group and application, not just the subnet a device sits on.[36]

Zone Protection and DoS defense

Zone Protection profiles are applied to an ingress zone to protect it from common floods and packet-based attacks.[37]
Flood protection in a Zone Protection profile defends the entire ingress zone against SYN, ICMP/ICMPv6, UDP (and other IP) flood attacks by measuring new connections per second and comparing against configured thresholds.[38]

Practical checklist (exam + ops)

- Create zones, then map/assign interfaces to zones, and build Security policy using zones (not interfaces) as match criteria.[35] [33]
- Use smaller, purpose-based zones (e.g., "DB-Zone" instead of "Servers") to prevent lateral movement and to simplify "only what's needed" rules.[36]
- Apply Zone Protection on exposed ingress zones (Internet-facing, partner-facing) and tune thresholds based on baseline CPS so normal bursts don't trigger drops.[38]

If the target is a specific environment (campus, data center, cloud VPC, branch), say which one and the intended zones can be drafted as a minimal ruleset (allow list + required infra services like DNS/NTP/AD).

Zone Protection profile defends the entire ingress zone against SYN

A **Zone Protection Profile** defends an entire ingress zone against SYN flood attacks by monitoring the **aggregate** rate of new TCP connection requests (SYN packets) entering that zone, regardless of the destination IP. It uses three specific thresholds—Alarm, Activate, and Maximum—to trigger protective actions like **RED** (Random Early Drop) or **SYN Cookies**.

How It Works

The profile is applied to the **ingress zone** (where the traffic enters the firewall, e.g., the "Untrust" zone for internet traffic). It counts every incoming SYN packet matching that zone. If the total number of SYN packets per second (CPS) exceeds your configured thresholds, the firewall intervenes to protect both its own resources and the downstream network.[48]

Protection Mechanisms

When the packet rate crosses the **Activate** threshold, the firewall applies one of two actions:

1. **SYN Cookies (Recommended):**
    - **Mechanism:** The firewall acts as a proxy for the TCP handshake. It intercepts the client's SYN and responds with a SYN-ACK containing a cryptographic "cookie" in the sequence number.[49] [50]
    - **Validation:** It does *not* allocate a session or resources yet. Only if the client responds with a valid ACK (completing the handshake) does the firewall permit the connection and set up the session with the backend server.[49]
    - **Benefit:** This differentiates legitimate users (who complete the handshake) from spoofed attack traffic (which never responds), ensuring legitimate traffic is not dropped. [49]
2. **RED (Random Early Drop):**
    - **Mechanism:** The firewall randomly drops SYN packets. The drop probability increases linearly as the rate climbs from the *Activate* threshold toward the *Maximum* threshold. [51]
    - **Drawback:** It can drop legitimate connections indiscriminately. It is less CPU-intensive than SYN Cookies but less fair to valid users.[49]

Threshold Configuration

The profile uses a "leaky bucket" model with three stages to manage the flood:[52] [51]

Threshold	Description	Recommended Setting
Alarm Rate	Triggers a log entry (Threat Log) but **does not drop** traffic. Warns you that traffic is spiking.	15–20% above your zone's average baseline CPS [52].
Activate Rate	**Starts mitigation** (applies SYN Cookies or RED). The firewall begins intervening to filter the flood.	Just above the zone's normal *peak* CPS to avoid false positives [52].
Maximum Rate	**Hard cap.** All SYN packets exceeding this rate are dropped immediately, regardless of validity, to protect the firewall CPU.	80–90% of the firewall's total datasheet capacity (if protecting the device) [52].

Difference from DoS Protection Policy

- **Zone Protection (Aggregate):** Protects the "pipe." It triggers if the *total* traffic enters the zone is too high (e.g., 10,000 users each sending 1 packet, or 1 attacker sending 10,000). It saves the *firewall* from collapse.[48]
- **DoS Protection Policy (Granular):** Protects a specific "target." It triggers only if a *specific* IP (e.g., your Web Server) is hit by too many packets. It saves the *server* from collapse.[48]

⁂

tune thresholds based on baseline CPS

Tuning Zone Protection thresholds based on baseline CPS (Connections Per Second) means configuring your **Alarm**, **Activate**, and **Maximum** rates to match the actual traffic patterns of your network. If you set these values too low, you will block legitimate traffic (false positives). If you set them too high, you leave the network open to floods.

To find the right numbers, you must first measure your **normal** and **peak** traffic rates.

1. How to Measure Baseline CPS

You cannot guess these numbers; you must measure them from the firewall itself.

- **CLI Method (Snapshot):**
  Run the command `show session info` on the CLI. Look for the `cps` (New connection establish rate) value.[63]
  - *Note:* This shows the *global* CPS for the whole box, not per zone. It gives you a rough upper limit for your busiest zone.
- **ACC Method (Historical - Recommended):**
  Use the **Application Command Center (ACC)** in the web interface to see per-zone data over time.[63]
  1. Set the time range (e.g., "Last 7 Days" or "Last Month") to capture peaks like Monday morning logins or backups.
  2. Check the **Network Activity** tab.
  3. Look at the "Source IP Activity" or "Destination IP Activity" widgets.

4. **Calculate:** Take the total session count for the peak hour and divide by 3,600 (seconds in an hour) to get the average CPS for that period.[63]

- **AIOps for NGFW (Automated):**
  If you have AIOps enabled (PAN-OS 10.0+), it automatically calculates these baselines and provides "Threshold Recommendations" directly in the GUI, saving you the manual math. [64]

2. Calculating the Thresholds

Once you have your **Peak CPS** (the highest normal traffic rate you ever see), use these multipliers to set your thresholds.

Threshold	Formula / Rule of Thumb	Purpose
Alarm Rate	**1.2x Peak CPS** (20% above peak)	Warns you when traffic is abnormally high but doesn't drop anything. Use this to validate your baseline without risk [65].
Activate Rate	**1.5x Peak CPS** (50% above peak)	**Start Mitigation.** This is when SYN Cookies or RED drops begin. It must be high enough to allow legitimate "micro-bursts" without triggering [65].
Maximum Rate	**2.0x Peak CPS** (Double peak)	**Hard Cap.** Everything above this is dropped. This protects the firewall CPU from reaching 100% usage during a massive attack [65].

3. Pro Tip: The "Assessment Mode" Strategy

When deploying Zone Protection for the first time, do not enable "Block" or "SYN Cookies" immediately.

1. Set the **Alarm** threshold to your calculated baseline.
2. Set **Activate** and **Maximum** to very high values (or leave the action as "Alert" if the specific protection type supports it).
3. Monitor the System Logs for a week.
4. If you see "Flood Alarm" logs during normal business hours, your baseline was too low. Raise the Alarm threshold.
5. Once the alarms stop triggering during normal traffic, you can safely lower the **Activate** and **Maximum** thresholds to their enforcement levels.[64] [63]

⁂

High availability (HA)

High Availability (HA) on Palo Alto Networks firewalls ensures business continuity by grouping two identical firewalls into a synchronized pair. If one fails, the other takes over with minimal or no disruption to traffic.

1. HA Modes: Active/Passive vs. Active/Active

Choose the mode based on your network design, not just for "more throughput."

Feature	Active/Passive (Recommended)	Active/Active
Traffic Handling	**One** firewall handles all traffic. The passive unit is on standby (interfaces logically down) and only syncs state.	**Both** firewalls handle traffic simultaneously.
Complexity	**Low.** Troubleshooting is simple because traffic paths are deterministic. No asymmetric routing issues.	**High.** Requires complex routing/floating IP designs to ensure sessions return to the *owner* firewall (asymmetric routing) [79].
Supported Deployments	Layer 2, Layer 3, Virtual Wire (V-Wire).	Layer 3 and Virtual Wire (V-Wire) only. **No Layer 2.** [79]
Performance	Performance is limited to the capacity of *one* device.	Theoretically higher throughput, but often used for *resiliency* in async routing environments rather than just speed [79].

2. HA Links: The "Heartbeat" and "Brain"

The firewalls communicate over dedicated physical ports. You must cable these correctly for the cluster to form.

- **HA1 (Control Link):**
  - **Function:** The "Management" sync. It exchanges **Heartbeats** (are you alive?), **Hellos**, and synchronizes the **Configuration** (policies, objects) and **User-ID** info.[80]
  - **Port:** Dedicated HA1 port or MGMT port.
- **HA2 (Data Link):**
  - **Function:** The "Session" sync. It synchronizes **Session Tables**, ARP tables, and IPSec Security Associations. This ensures that if failover happens, the new active firewall already knows about all existing connections (users don't get disconnected).[81]
  - **Port:** Dedicated HA2 port or a high-speed data interface (HSCI on high-end models).
  - **Backup:** Always configure an **HA2 Backup** link on a different physical path to prevent "split-brain" scenarios.[80]
- **HA3 (Packet Forwarding Link):**
  - **Function: Active/Active ONLY.** It forwards packets between the two firewalls if a packet arrives at the "wrong" unit (the one that doesn't own the session).[81]
- **HA4 (Cluster Link):**
  - **Function:** Used only in larger **HA Clusters** (up to 16 devices) for session sync, not typical 2-node HA pairs.[80]

3. Requirements for HA

To form a successful HA pair, the two devices must be virtually identical "twins":[82]

- **Same Model:** (e.g., PA-3410 with PA-3410). You cannot mix models.
- **Same PAN-OS Version:** Both must run the exact same version (e.g., 11.0.2). *Exception:* During an upgrade, they can temporarily differ.[83]
- **Same Licenses:** Both must have the same set of valid licenses (Threat, WildFire, etc.) or failover capabilities will be mismatched.[84]
- **Same Interfaces:** Physical link speeds and interface configurations must match.

Exam Tip: Failover Triggers

The firewall will trigger a failover if:

1. **Heartbeat Loss:** It stops hearing from the peer via HA1 (device failure).
2. **Link Monitoring:** A critical interface (e.g., Uplink to ISP) goes down. You must *configure* Link Monitoring groups for this to happen; it's not automatic.
3. **Path Monitoring:** The firewall can no longer ping a critical external IP (e.g., Default Gateway).[79]

⁂

ARP Tables

The ARP (Address Resolution Protocol) table on a Palo Alto Networks firewall maps IPv4 addresses to MAC addresses for connected Layer 3 interfaces. Proper management of this table is critical for connectivity and troubleshooting.

1. Viewing the ARP Table

You primarily view ARP entries via the CLI.

- **Command:** `> show arp all`
  - **Output Columns:** Interface, IP Address, MAC Address, Port, Status, TTL.[94] [95]
- **Filter by Interface:** `> show arp interface ethernet1/1`
- **Filter by Sub-interface:** `> show arp interface ethernet1/1.10` (Note: Manually add the sub-interface ID).[96]

2. ARP Entry Status Codes

When viewing the table, the **Status** column indicates the health of the resolution:[97] [98]

- **c (Complete):** Valid entry. The firewall knows the MAC address and can forward traffic.
- **s (Static):** Manually configured entry. It never expires.

- **i (Incomplete):** The firewall sent an ARP Request but **received no reply**. This usually means the destination host is down, the IP doesn't exist, or a firewall on the host is blocking ARP.
- **e (Expiring):** The entry is nearing its timeout and will soon be refreshed or removed.

3. Clearing the ARP Table

If you replace a router or server (changing its MAC address but keeping the IP), the firewall may hold the "stale" MAC address, breaking connectivity.

- **Clear All:** `> clear arp all`
- **Clear Specific IP:** `> clear arp interface ethernet1/1 ip 10.1.1.5`.[99]
- **Clear Entire Interface:** `> clear arp interface ethernet1/1`.[99]

4. Configuring ARP Settings

- **Default Timeout:** Entries stay in the cache for **1800 seconds** (30 minutes) by default.[100] [97]
- **Change Timeout:**
  - Command: `> set system setting arp-cache-timeout <seconds>` (Range: 60–65535).[100]
  - *Why change it?* Lowering the timeout (e.g., to 300s) can help in dynamic environments where devices move frequently, but it increases broadcast traffic (ARP Requests).
- **Maximum Entries:** To check the hardware limit for your specific model: `> show system state filter cfg.general.max* | match arp` [100].

Troubleshooting "Incomplete" Entries

If you see **(incomplete)** entries, check:

1. **Direct Connectivity:** Is the device actually on that subnet?
2. **PBF Rules:** A Policy Based Forwarding (PBF) rule with an empty "Next Hop" can cause phantom incomplete ARP entries for IPs not on the local subnet.[97]
3. **NAT Configuration:** An incorrect Source NAT policy (e.g., masking a whole subnet instead of `/32`) can cause the firewall to answer ARP requests for IPs it doesn't own, or fail to resolve them correctly.[98]

```
4.  **Gratuitous ARP (GARP):** To force downstream devices to update *their* ARP tables (
```

⁂

Security and NAT policy implementation

Security and NAT policies on Palo Alto Networks firewalls are implemented as two distinct rulebases that interact in a specific order. Understanding this interaction—particularly the "Pre-NAT IP, Post-NAT Zone" rule—is critical for passing the NetSec-Pro exam and for operational configuration.

1. Evaluation Order (The Golden Rule)

While the firewall *evaluates* both policies early in the packet flow, the matching logic is distinct:

- **NAT Policy Evaluation:** Happens **first**. The firewall checks if the traffic matches a NAT rule to determine the *final* destination IP and zone (via a route lookup). It does not *apply* the translation yet, but it calculates the result.[108] [109]
- **Security Policy Evaluation:** Happens **second**. Crucially, the Security policy matches based on:
    - **Source IP:** The **original (Pre-NAT)** IP address.
    - **Destination IP:** The **original (Pre-NAT)** IP address.
    - **Destination Zone:** The **final (Post-NAT)** zone. This is the tricky part. The firewall uses the result of the NAT lookup to determine where the packet is *going* (e.g., DMZ) rather than where it *looked like* it was going (e.g., Untrust/Public IP).[109] [110]

2. NAT Policy Types

You must select the correct translation type for the use case.

Source NAT (Outbound Access)

Used when internal users access the Internet.

- **Dynamic IP and Port (DIPP):** Maps many private IPs to a single public IP (e.g., interface IP) by varying the source port. Standard "PAT" for office internet access.[111]
- **Dynamic IP:** Maps internal IPs to a *pool* of public IPs. Used when you have a block of public IPs but many more internal users.
- **Static IP:** 1-to-1 mapping. Used for specific servers that need a consistent outbound IP (e.g., mail servers).

Destination NAT (Inbound Access)

Used when external users access internal servers (Port Forwarding).

- **Static IP (with Port Forwarding):** Maps a public IP:Port (e.g., 203.0.113.10:80) to a private IP:Port (10.1.1.5:8080).
- **Bi-directional:** An option in Static NAT rules. It automatically creates a "reverse" Source NAT rule so the server replies with the correct public IP.

3. Security Policy Best Practices

- **Rule Shadowing:** This occurs when a broad rule (e.g., "Allow All to Internet") is placed *above* a specific rule (e.g., "Block HR from Social Media"). The specific rule is never reached.
  - **Fix:** Always place specific rules at the top and general rules at the bottom. [112] [113]
  - **Tool:** The firewall generates a commit warning if it detects shadowing.
- **Intrazone vs. Interzone:**
  - **Intrazone (Same Zone):** Allowed by default. You should create a "Deny Intrazone" rule at the bottom to enforce Zero Trust even within a zone. [113]
  - **Interzone (Different Zones):** Blocked by default. You must explicitly allow traffic. [114]
- **Use Tags:** Tag rules (e.g., "Inbound", "Outbound", "DMZ") to make the policy readable and filterable. [113]

Example: Publishing a Web Server

Scenario: Public IP `1.1.1.1` maps to Internal Server `10.1.1.5` in the DMZ.

1. **NAT Rule:**
   - **Source Zone:** Untrust
   - **Dest Zone:** Untrust (Because the *original* destination IP 1.1.1.1 lives on the Untrust interface).
   - **Dest IP:** 1.1.1.1
   - **Translation:** Destination Translation → 10.1.1.5
2. **Security Rule:**
   - **Source Zone:** Untrust
   - **Dest Zone: DMZ** (Post-NAT zone!).
   - **Dest IP: 1.1.1.1** (Pre-NAT IP!).
   - **Application:** web-browsing
   - **Action:** Allow. [110] [115]

⁂

monitoring and logging

The **Monitoring and Logging** domain tests your ability to visualize network activity, investigate threats, and export data to external systems.

1. Key Log Types

Palo Alto Networks firewalls generate several distinct log types. You must know what each contains to troubleshoot effectively.

Log Type	Content & Use Case
Traffic	Records session flows (Source, Dest, App-ID, Bytes). **Critical:** By default, logs are generated at **Session End** to capture the full duration and byte count.
Threat	Records security violations (Virus, Spyware, Vulnerability, DNS Sinkhole). Generated *immediately* when a threat profile triggers [123].
System	Hardware/Software events (HA failover, Link Down, User Login, NTP sync). Essential for ops troubleshooting [123].
Config	Audit trail of *who* changed *what*. (e.g., "admin" deleted "Rule-5").
HIP Match	(GlobalProtect) Logs which Host Information Profile (HIP) objects matched a remote user (e.g., "OS=Windows 10", "Disk Encrypted=Yes") [124].
Unified	A consolidated view of Traffic, Threat, URL, and Data logs in one stream to simplify correlation [124].

2. Log Forwarding

Logs should not just stay on the box; they must be sent to external collectors for retention and analysis.

- **Log Forwarding Profile:** This object is attached to **Security Policy Rules**. It tells the firewall: "If traffic hits this rule, send the log to Syslog Server A and Email Admin B."
  - *Note:* System and Config logs are global, so you configure their forwarding under **Device > Log Settings**, *not* in a policy profile.[125] [126]
- **Destinations:**
  - **Syslog:** Standard for SIEMs (Splunk, QRadar).
  - **Email:** For high-priority alerts (e.g., Critical System Alarms).
  - **SNMP Traps:** For NMS integration.
  - **HTTP/HTTPS:** For API-based collectors.

3. Monitoring Tools

- **ACC (Application Command Center):**
  - **Function:** A graphical, interactive dashboard that visualizes network trends (e.g., "Top High-Risk Applications," "Top Threats," "Top Users") over time.[127] [128]
  - **Use Case:** Executive reporting and "at-a-glance" health checks. You can click on any widget (e.g., "BitTorrent") to drill down into the specific logs.[128]
- **Automated Reports:**
  - You can schedule PDF reports (e.g., "Daily Threat Summary") to be emailed automatically to management.

- **Strata Logging Service (formerly Cortex Data Lake):**
  - **Function:** Cloud-based log storage. Required for **Prisma Access** (SASE) and **Cloud NGFW** since they don't have local hard drives. It centralizes logs from all hardware and cloud firewalls into one pool.[129] [130]

4. Best Practices

- **Log at Session End:** Always configure traffic logging at **Session End**.
  - *Why?* "Session Start" logs are incomplete (0 bytes transferred, App-ID might change from "web-browsing" to "facebook" later). Logging both Start and End doubles the log volume and CPU load.[131] [132] [133]
- **Log Forwarding for "Deny" Rules:** Ensure your "Deny All" or "Cleanup" rule at the bottom *has* a Log Forwarding Profile attached. Otherwise, you will never see *what* is being blocked, making troubleshooting impossible.

⁂

WAN Optimization

The implementation of "WAN Optimization" differs significantly between Palo Alto Networks' two main product lines: **Prisma SASE** (Cloud-Delivered) and **Strata NGFW** (Hardware/VM).

1. Prisma SASE: "App Acceleration"

Palo Alto Networks has moved away from traditional "caching/compression" WAN optimization in favor of a modern approach called **App Acceleration** (formerly part of Prisma Access).

- **Mechanism:** Instead of just caching static files, it uses "Predictive Analytics." It learns a user's behavior within an application (e.g., Salesforce, ServiceNow) and *pre-fetches* dynamic content before the user even clicks the next link.[138]
- **Result:** This can improve application performance by up to **5x**, especially for dynamic, personalized content that traditional caching misses.[139] [140]
- **Use Case:** Ideal for remote users (mobile/home) and branch offices connecting to SaaS applications over the internet.[141]

2. Strata NGFW (PAN-OS): "QoS & Traffic Shaping"

The physical firewalls (PA-Series) do **not** perform traditional WAN optimization (deduplication/compression) natively. Instead, they rely on **SD-WAN** intelligence and **QoS** to optimize the *delivery* of packets.

- **Application-Aware QoS:**
  - **Classification:** You don't prioritize "Port 80"; you prioritize "Zoom-Video" or "SAP-ERP" using App-ID.
  - **Action:** You can guarantee bandwidth (min/max), limit bandwidth for non-critical apps (YouTube), and mark packets (DSCP) for downstream routers.[142] [143]

- **SD-WAN Path Selection:**
  - **Mechanism:** The firewall measures the real-time health (Jitter, Latency, Packet Loss) of all WAN links.
  - **Optimization:** If the primary link degrades, the firewall automatically fails over traffic to a healthier path (e.g., MPLS → 5G) to maintain the application's SLA.[144] [145]
  - **FEC (Forward Error Correction):** It can reconstruct lost packets on the receiving end, effectively "optimizing" a lossy link without retransmission.[145]

Summary Comparison

Feature	Prisma SASE (Cloud)	Strata NGFW (On-Prem)
Optimization Method	**App Acceleration** (Predictive Pre-fetching)	**QoS & SD-WAN** (Path Selection & Prioritization)
Target Traffic	Dynamic SaaS (Salesforce, M365) & Web Apps	All Traffic (Data Center, Internet, WAN)
Performance Gain	"Speed up" the app logic (up to 5x) [140].	"Clean up" the pipe (prevent congestion) [143].
Configuration	Enable in SASE/Cloud Manager (simple toggle).	Define QoS Profiles, Policies, and Limits manually [146].

⁂

Path and NAT Policies

Path and NAT Policies interact closely to determine how traffic flows through the firewall. Understanding the precedence and logic is essential, especially when troubleshooting routing issues or dual-ISP setups.

1. Path Selection Precedence

When the firewall decides where to send a packet (Egress Interface), it follows a strict hierarchy. If a higher-priority method finds a path, it stops looking.

1. **Policy-Based Forwarding (PBF):**
   - **Priority:** Highest. PBF overrides everything else.
   - **Logic:** "If traffic is from Source A going to Dest B, force it out Interface X (regardless of the routing table)."
   - **Use Case:** Sending specific application traffic (e.g., VoIP) over a dedicated MPLS link while everything else uses the cheap Internet link.[153]
   - **Caveat:** PBF happens **before** NAT. If you use PBF to force traffic out a specific interface, the NAT policy must align with that egress interface, or traffic will be dropped. [154]
2. **Static Routes:**

   - **Priority:** Medium. Manually defined routes in the Virtual Router.
   - **Use Case:** Default routes (0.0.0.0/0) or specific subnets.
3. **Dynamic Routes (OSPF/BGP):**
   - **Priority:** Medium (Admin Distance determines priority vs. Static). Learned from neighbors.

2. NAT Policy and Path Selection

The interaction between NAT and Path Selection is a common exam "gotcha."

- **Routing Happens FIRST:** The firewall performs a route lookup (or PBF check) to determine the **Egress Interface** and **Destination Zone**.
- **NAT Rule Evaluation Happens SECOND:** The firewall *then* checks the NAT policy.
  - **Critical:** Because routing happens first, your NAT rule must match the *original* destination IP but the *post-routing* destination zone.
  - **Example:** If routing sends the packet out `ethernet1/1` (Untrust Zone), your NAT rule must say "Destination Zone: Untrust".[155] [156]

3. Active/Active HA Path Monitoring Issues

In Active/Active HA, path monitoring can be tricky because both firewalls are passing traffic.

- **Issue:** If one firewall loses its path to the internet (e.g., ISP failure) but the other doesn't, you need asymmetric routing or PBF to redirect traffic to the healthy peer.
- **Floating IP:** NAT rules in Active/Active often use Floating IPs to ensure return traffic hits the correct firewall owner. If the path fails, the Floating IP must move.[157]

4. Policy Based Forwarding (PBF) Monitoring

PBF rules can monitor a target IP (like a next-hop gateway).

- **Action:** If the monitor fails (Gateway unreachable), the PBF rule is **disabled**.
- **Result:** The firewall falls back to the standard Routing Table (Static/Dynamic routes). This provides an automatic failover mechanism for ISP links.[158] [153]

⁂

Dynamic Routes (OSPF/BGP):

Dynamic routing protocols (OSPF and BGP) on Palo Alto Networks firewalls are configured within the **Virtual Router** (VR). A key concept is that the firewall acts like a standard router but integrates security.

1. OSPF Area Types

When configuring OSPF, the Area Type determines how routing information (LSAs) is filtered to reduce table size and CPU load.[168]

Area Type	Function & Behavior
Normal (Standard)	The default. Accepts all LSAs (internal, external, and summaries). The backbone (Area 0.0.0.0) MUST be a Normal area.
Stub	**Block External Routes (Type 5 LSAs).** Useful for branch offices with only one exit. It replaces all external routes with a single default route.
Totally Stubby	**Blocks External (Type 5) AND Summary (Type 3) LSAs.** Only accepts a default route. Configured by checking the "No Summary" box in the Stub area settings [168] [169].
NSSA (Not-So-Stubby)	**Allows External Routes IN, but blocks them from others.** Allows you to import external routes (e.g., from a partner) into a Stub area using Type 7 LSAs, which the ABR converts to Type 5 for the rest of the network [168] [170].

2. BGP Conditional Advertisement

This advanced feature solves the "Dual-ISP Failover" problem without asymmetric routing. It allows the firewall to advertise a prefix to a neighbor (ISP B) *only* if a specific condition is met (e.g., ISP A goes down).

- **Logic:** "Advertise my IP range `203.0.113.0/24` to ISP-Backup **IF AND ONLY IF** the route to ISP-Primary (e.g., `0.0.0.0/0` via 1.1.1.1) is missing from my routing table".[171] [172]
- **Configuration Steps:**
  1. **Non-Exist Filter:** Create a filter that checks for the *absence* of the primary route (e.g., primary default gateway).
  2. **Advertise Filter:** Select the prefix you want to advertise (e.g., your public IP block).
  3. **Apply to Peer:** Attach this conditional policy to the BGP Export rules for the *Backup* peer.[173] [172]

3. Redistribution Profiles

Since the firewall often sits between different routing domains (e.g., OSPF Internal ↔ BGP External), you must explicitly configure **Redistribution Profiles** to move routes between them.[174]

- **Best Practice:** Never redistribute "everything." Always use filters (by interface or prefix) to prevent routing loops or route leaks (e.g., advertising private 10.x.x.x IPs to the public internet).[174] [171]
- **Precedence:** Routes redistributed into OSPF become Type 5 (External) LSAs. Routes redistributed into BGP carry the origin of "Incomplete" (?) by default unless set otherwise.

⁂

LSA's

Link State Advertisements (LSAs) are the data packets OSPF routers exchange to build their "map" of the network (Link State Database). Understanding LSA types is crucial for configuring Stub areas and NSSAs on Palo Alto firewalls.

Key OSPF LSA Types

You will typically encounter Types 1, 2, 3, 4, 5, and 7.

LSA Type	Name	Generated By	Scope	Description
Type 1	**Router LSA**	**Every Router**	**Area Local**	Describes the router's *own* links, interfaces, and costs. It never leaves the area where it was generated [183] [184].
Type 2	**Network LSA**	**DR (Designated Router)**	**Area Local**	Describes the "transit network" (subnet) and lists all routers attached to it. Only exists on multi-access networks (Ethernet) where a DR is elected [183].
Type 3	**Summary LSA**	**ABR (Area Border Router)**	**Inter-Area**	Summarizes routes from *one* area to inject them into *another* area. This is how Area 0 learns about Area 1's subnets [185] [186].
Type 4	**ASBR Summary**	**ABR**	**Inter-Area**	Tells other areas *where* the ASBR is located. It says: "To reach the external world, send traffic to Router X" [185].
Type 5	**AS External**	**ASBR (Autonomous System Boundary Router)**	**Domain Wide**	Describes routes to *external* destinations (e.g., Internet, BGP, Static Redistributed). Flooded to *all* normal areas [183] [187].
Type 7	**NSSA External**	**ASBR (in NSSA)**	**NSSA Local**	Identical to Type 5, but designed for **NSSA** (Not-So-Stubby Areas). Since Type 5s are blocked in NSSAs, Type 7s carry external routes *inside* the NSSA. The ABR then converts them to Type 5 for the rest of the network [183] [188].

LSA Filtering by Area Type

The choice of Area Type on the Palo Alto firewall determines which LSAs are blocked to save resources.

- **Stub Area:** Blocks **Type 5** (External). Replaces them with a default route.
- **Totally Stubby:** Blocks **Type 5** (External) AND **Type 3** (Summary). The area only knows about its own links and a default route.
- **NSSA:** Blocks **Type 5** (External) from *entering*, but allows **Type 7** (External) to be *originated* inside. [189] [188]

Troubleshooting Tip

If you see routes missing in the routing table:

- Check the database: `> show routing protocol ospf lsdb`
- If a **Type 5** LSA exists but isn't in the routing table, check if "Forwarding Address" is reachable via an OSPF intra-area or inter-area route (a common requirement for Type 5 validity).[190]

⁂

zone-based firewall

A **Zone-Based Firewall** architecture is the core security model of Palo Alto Networks NGFWs (and SASE). Instead of writing rules for physical interfaces (e.g., `Allow Eth1/1 to Eth1/2`), you group interfaces into logical **Security Zones** and write policies between those zones.

Core Architecture

1. **Zones are Logical Containers:** A zone represents a trust level or function (e.g., "Trust," "Untrust," "DMZ," "Users-WiFi").
2. **Interfaces Must Belong to a Zone:** An interface (physical or virtual) cannot process traffic until it is assigned to a zone. A zone can contain multiple interfaces, but an interface can belong to only *one* zone.[198] [199]
3. **Default Security Posture:**
    - **Intra-Zone (Same Zone):** Traffic is **Allowed** by default. (e.g., Computer A in "Trust" can talk to Computer B in "Trust").
    - **Inter-Zone (Different Zones):** Traffic is **Blocked** by default. You must explicitly create a Security Policy rule to allow traffic from "Trust" to "Untrust".[200] [201]

Benefits vs. Interface-Based Firewalls

- **Abstraction & Scalability:** If you add a new uplink or replace a cable, you just assign the new interface to the existing "Untrust" zone. You do *not* need to rewrite your 5,000 security rules because the rules target the *Zone*, not the *Interface*.[198]
- **Simplified Policy:** It reduces "Rule Sprawl." Instead of 10 rules for 10 different VLAN interfaces, you have 1 rule for the "User-Zone".[198]

Configuration Steps

1. **Define Zones:** Create zones based on trust/function (e.g., `Network > Zones`).
2. **Assign Interfaces:** Link physical interfaces, sub-interfaces (VLANs), or tunnel interfaces to these zones.
3. **Create Policy:** Write rules using Source Zone and Destination Zone as the primary match criteria.[202] [203]

Advanced Zone Features

- **Zone Protection Profiles:** You attach these to a zone (not a rule) to protect it from floods (SYN, UDP) and reconnaissance (Port Scans).[204] [202]
- **Packet Buffer Protection:** Enabled per zone to prevent a single abusive session from hogging the firewall's entire packet buffer memory.[202]

⁂

Prisma SD-WAN Monitoring and logging

Monitoring and logging in Prisma SD-WAN (and SASE) differs from traditional firewalls because it is application-centric and relies on AIOps to reduce noise.

1. Application-Centric Monitoring

The Prisma SD-WAN dashboard focuses on **App Health**, not just "Link Up/Down."

- **Performance SLAs:** You define SLAs per application (e.g., "Zoom Latency < 150ms"). The dashboard tracks compliance with these thresholds, showing metrics like **Transaction Time**, **Init Failure Rate**, and **Media Mean Opinion Score (MOS)**.[213] [214]
- **Flow Browser:** Unlike a simple log viewer, the **Flows** tab allows you to visualize traffic paths in real-time. It shows the **Source**, **Destination**, **Path ID** (which WAN link was used), and importantly, the **SLA Status** (why the path was chosen).[215] [216]

2. AIOps & Event Correlation

Prisma SD-WAN uses AIOps to solve "Alert Fatigue."

- **Event Correlation:** Instead of sending 1,000 alerts when a core router fails (one for every site that can't reach it), AIOps correlates these into a **single Root Cause event**.[217] [218]
- **Anomaly Detection:** It learns "normal" behavior. If bandwidth usage spikes at 2 AM (unusual), it triggers an alert, whereas a spike at 9 AM (normal login time) might be ignored. [218]

3. Log Export

- **Syslog:** You can export flow logs and event logs to an external collector (Splunk/SIEM).
    - **Configuration:** Create a **Syslog Profile** in the Prisma SD-WAN controller. You can filter by severity (Critical, Major) and export type (Flows vs. Events).[219] [215]
    - **CloudBlades:** For seamless integration, you use **CloudBlades** (API connectors) to push logs directly to third-party platforms like ServiceNow or Prisma Cloud without complex manual forwarding rules.[220]

4. Circuit Monitoring

- **Bandwidth Subscription:** The system monitors your aggregate bandwidth usage across all sites to ensure you are within your licensed capacity.[221]
- **Circuit Health:** It tracks the physical health (Jitter, Loss, Latency) of every underlay link (MPLS, Broadband, LTE) to make intelligent path selection decisions.[222]

⁂

SIEM

Integration with a **SIEM** (Security Information and Event Management) system is critical for aggregating Palo Alto Networks logs with other infrastructure data for broader threat analysis.

1. Integration Methods

You can send logs to a SIEM in two primary ways:

- **Direct Syslog (Strata NGFW):**
  - **Mechanism:** The firewall or Panorama sends standard Syslog (UDP/514, TCP/514, or TCP/6514 TLS) directly to the SIEM receiver.
  - **Configuration:** Create a **Syslog Server Profile** (Device > Server Profiles > Syslog) and attach it to a **Log Forwarding Profile** in your Security Policy.
  - **Format:** Typically **CEF** (Common Event Format) or **LEEF**, which are standard formats most SIEMs parse automatically.[228] [229]
- **Cloud API (Prisma Access / Cortex Data Lake):**
  - **Mechanism:** Since cloud-delivered firewalls (Prisma Access) don't have a "cable" to your on-prem SIEM, they store logs in **Cortex Data Lake** (CDL). Your SIEM must "fetch" these logs via API or use a **Log Forwarding App** (a cloud-to-ground bridge).
  - **Cortex Data Lake (CDL):** Acts as the central reservoir. It can forward logs to an on-prem Syslog receiver (via an HTTPS-to-Syslog bridge app) or directly to cloud SIEMs.[230] [231]

2. Major SIEM Integrations

- **Splunk:**
  - **Splunk App for Palo Alto Networks:** A robust, pre-built app that offers extensive dashboards (Threat, WildFire, User-ID) and CIM (Common Information Model) compliance. It visualizes data immediately without writing custom queries.[232] [233]
  - **Add-on:** The "Splunk Add-on" handles the backend data ingestion and parsing, while the "App" provides the frontend visualization.[234]
- **Microsoft Sentinel:**
  - **Data Connector:** Microsoft provides a native "Palo Alto Networks Cortex Data Lake" data connector. It uses an Azure Function or Linux agent (AMA) to pull logs from CDL or

receive Syslog and ingest them into Sentinel workspaces.[235] [229]

3. Noise Reduction Best Practices

Sending *every* log to a SIEM is expensive and overwhelming.

- **Filter at Source:** In the Log Forwarding Profile, use filters to send only "Traffic End" logs (drop "Start"), or only "Threat" logs of severity "Medium" and higher.
- **Exclude High-Volume/Low-Value:** Don't log "Allow DNS" (UDP/53) traffic to the SIEM unless debugging. Use the "Log at Session End" setting to halve the log volume (one log per session instead of two).[236]
- **Track Settings:** In security rules, set **Log at Session End** (recommended) and disable **Log at Session Start** to reduce volume by ~50% immediately.[236]

⁂

Prisma Access Remote user configuration

Configuring Remote Users (Mobile Users) in **Prisma Access** is functionally similar to a traditional GlobalProtect on-prem deployment but with key architectural differences in how gateways and portals are provisioned.

1. Architectural Components

- **Mobile Users (GlobalProtect):** This is the licensed module for securing remote workers. It scales automatically.
- **Service Connection (SC):** Connects the Prisma Access cloud to your *internal* resources (Data Center/HQ) via IPsec. Mobile users traffic destined for "10.x.x.x" flows through the SC.[243] [244]
- **Remote Networks (RN):** Connects branch offices. Typically, Mobile Users do *not* talk to Remote Networks directly unless a Service Connection acts as the hub.[244]

2. Configuration Workflow (Strata Cloud Manager or Panorama)

The process involves three main steps:

Step 1: Infrastructure Setup

1. **Select Locations:** Choose the Prisma Access regions (e.g., "US East", "Europe Central") where you want to deploy gateways. Choose locations closest to your users to minimize latency.[245]
2. **IP Pools:** Assign a **Worldwide IP Pool** (recommended) or Regional Pools. The system automatically assigns subnets to each gateway from this pool.
    - *Requirement:* Minimum size is usually a `/23` (512 IPs) per location to allow for scaling and seamless updates.[245]

3. **Gateways & Portal:** Unlike on-prem where you configure `Network > Interfaces` and `Network > GP Gateway`, in Prisma Access, the cloud *automatically* spins up the gateways and portal at the chosen locations. You just configure the *settings* (client config, auth).[246] [245]

Step 2: Authentication

1. **Cloud Identity Engine (CIE):** The modern standard. You integrate your IdP (Azure AD/Entra ID, Okta) with CIE, and Prisma Access consumes it.
2. **LDAP/RADIUS:** Legacy method using a Service Connection to reach on-prem AD.[247] [246]

Step 3: Client Configuration (Agent Settings)

- **On-Demand vs. Always-On:** Configured in the **App Settings** (just like on-prem).
- **Split Tunneling:** Critical for SaaS performance. Configure "Exclude Video Traffic" or specific SaaS domains from the tunnel to offload bandwidth.[248]

3. Traffic Flow

- **Internet Traffic:** Mobile User → Prisma Access Gateway → Inspection (Firewall/SWG) → Internet.
- **Internal Traffic:** Mobile User → Prisma Access Gateway → **Service Connection** → Data Center.[244]
- **User-to-User:** By default, mobile users cannot talk to each other. If needed, this requires specific policy/routing enablement.[243]

4. Verification

- **Status Dashboard:** Use `Panorama > Cloud Services > Status` or the Strata Cloud Manager dashboard to see "Green" status for the Mobile User container.[245]
- **Verify Region:** Ensure the user connects to the gateway in their *local* region (e.g., a German user connects to "Europe Central", not "US East") for performance.[245]

⁂

Prisma Access Remote network configuration

Configuring a **Remote Network (RN)** connects a physical branch office (CPE) to the Prisma Access cloud via an IPsec tunnel. Unlike Service Connections (which are for inbound/DC access), Remote Networks are primarily for **outbound** branch security (Internet & SaaS access).[258] [259]

1. Configuration Workflow (Strata Cloud Manager / Panorama)

The onboarding process connects your branch router/firewall to a nearby Prisma Access "Compute Location."

1. **Allocate Bandwidth:**
   - **Aggregate Model:** You allocate a pool of bandwidth (e.g., 200 Mbps) to a **Compute Location** (e.g., "Asia Southeast"). Prisma Access dynamically shares this bandwidth among all sites in that region.[260]
   - **Site-Based Model (New in 6.0):** You purchase specific license tiers per site (e.g., 50 Mbps, 500 Mbps, 1 Gbps). This prevents "noisy neighbor" issues but is less flexible.[261]
   - *Minimum:* The smallest allocation is 50 Mbps per compute location.[260]
2. **Configure the Tunnel (Onboard Site):**
   - **Tunnel Type:** Standard IPsec Site-to-Site.
   - **Parameters:** You define the Peer IP (your branch public IP), Pre-Shared Key (PSK), and IKE/IPsec crypto profiles (or use the "Palo Alto Recommended" defaults).
   - **Redundancy:** You configure a **Primary Tunnel** and an optional **Secondary Tunnel**. If Primary fails, traffic automatically shifts to Secondary.[262]
   - **Monitor:** Enable **Tunnel Monitoring** with a destination IP (like a loopback on the branch router) to ensure fast failover if the path degrades.[263]
3. **Enable Routing (BGP vs. Static):**
   - **Static Routing:** Simple. You tell Prisma Access, "To reach 192.168.10.0/24, go down Tunnel A."
   - **BGP (Recommended):** Dynamic.
     - **Peer AS:** Configure your branch ASN and the Prisma Access ASN (default 65534).
     - **Peering Addresses:** You must assign a `/30` (or similar) subnet for the inside tunnel interface (e.g., 169.254.20.1/30) so BGP neighbors can talk.[264]
     - **Local Address:** If your branch device (like AWS VGW) requires a specific peer IP, you can manually set the Prisma Access side IP.[265]

2. Service Connection vs. Remote Network

A common exam question involves knowing *when* to use which.

Feature	Remote Network (RN)	Service Connection (SC)
Primary Purpose	**Secure Branch Internet Access** (Outbound).	**Connect to Data Center/HQ** (Inbound/Hybrid).
Internet Access	**Yes.** Traffic egresses to Internet via Prisma Cloud SWG/FW.	**No.** Traffic cannot egress to Internet directly from SC [259].
User Access	Connects Branch Users.	Connects Internal Servers/Apps.

Feature	Remote Network (RN)	Service Connection (SC)
Routing	Advertises branch subnets to Cloud.	Advertises DC subnets (e.g., 10.0.0.0/8) to Cloud.

3. Traffic Flow Example

- **Branch to Internet:** Branch Router → IPsec Tunnel → **Remote Network** → Security Processing → Internet.
- **Branch to DC:** Branch Router → IPsec Tunnel → **Remote Network** → Cloud Backbone → **Service Connection** → DC Router → Server.[259]

⁂

Prisma Access Public and private appliction access

Prisma Access architecture divides application access into two primary flows: **Public** (SaaS/Internet) and **Private** (Internal/Data Center). Each uses distinct mechanisms for connectivity and security.

1. Private Application Access (Zero Trust)

To allow remote users or branches to access internal apps (e.g., Jira, SAP, intranet) without exposing the entire network, Prisma Access uses two main methods:

- **Service Connections (Legacy/Network-Centric):**
  - **Architecture:** An IPsec tunnel connects Prisma Access to your Data Center (DC).
  - **Routing:** It routes full subnets (Layer 3) to the DC.
  - **Pro:** Supports server-to-client traffic (VoIP, Helpdesk push).[273]
  - **Con:** Can provide excessive access ("network-level trust") if not segmented properly.
- **ZTNA Connector (Modern/App-Centric):**
  - **Architecture:** A lightweight VM ("Connector") sits inside your DC or Cloud VPC. It establishes an *outbound* tunnel to the Prisma Access cloud.[274] [273]
  - **Function:** It publishes *specific* applications (FQDNs or IPs) to Prisma Access. Users connect to the *app*, not the *network*.
  - **Benefits:**
    - **No Inbound Ports:** You don't open firewall ports at the DC edge; the connector reaches out.
    - **Overlapping IPs:** Handles overlapping IP ranges (e.g., two acquired companies both using 10.0.0.0/8) because it maps apps by DNS/FQDN.[273]
    - **Auto-Discovery:** Can automatically find new apps running in the environment.[273]

2. Public Application Access (SWG/CASB)

For traffic going to the Internet (Salesforce, Microsoft 365, YouTube), Prisma Access acts as a **Cloud Secure Web Gateway (SWG)**.

- **Connectivity Methods:**
  - **GlobalProtect (Standard):** Full tunnel or split tunnel captures traffic and sends it to the gateway.
  - **Explicit Proxy:** Browsers are configured (via PAC file) to point to `proxy.prismaaccess.com`. Useful for unmanaged devices or where IPsec isn't feasible. [275]
  - **Transparent Proxy:** The Prisma Access Agent redirects traffic to the proxy without explicit browser config. [275]
- **Security Stack:**
  - **Visibility:** Decrypts SSL/TLS to see the actual application function (e.g., "Facebook-Posting" vs. "Facebook-Chat").
  - **SaaS Security (CASB):** Uses "App-ID" to identify 40,000+ SaaS apps. It can block risky apps (Shadow IT) or enforce granular controls (e.g., "Allow Box Download, Block Box Upload"). [276]
  - **Private App Security:** Can also protect private web apps by applying WAF and WAAP protections inline. [277]

Summary: Flow Comparison

Feature	Private Access (ZTNA)	Public Access (SWG/CASB)
Destination	Internal DC / Private Cloud	Internet / SaaS
Connectivity	**Service Connection** (IPsec) or **ZTNA Connector** (VM)	**Internet Gateway** (Direct Egress from Cloud)
Trust Model	**Zero Trust:** "Connect user to App X only" [273].	**Secure Gateway:** "Inspect all traffic for threats."
Inbound Ports	**None** (with ZTNA Connector).	**N/A** (Outbound only).
Overlap Support	**Yes** (via ZTNA FQDN mapping) [273].	**N/A** (Public IPs don't overlap).

⁂

Prisma Access Security and NAT Policy implementation

Security and NAT policies in Prisma Access function similarly to Strata NGFWs (following the same evaluation logic), but the **Source NAT** implementation is handled differently due to the cloud architecture.

1. Security Policy

You write Security rules in **Strata Cloud Manager** or **Panorama** just like on-prem firewalls.

- **Zones:**
  - **Trust:** Interfaces facing the branch (Remote Network) or user (GlobalProtect).
  - **Untrust:** The Prisma Access egress to the Internet.
  - **Service Connection:** A dedicated zone type for traffic heading back to your Data Center.[288]
- **Evaluation:** Top-down. Specific rules (User-ID + App-ID) must be at the top.[288]

2. NAT Policy & Public IPs

Prisma Access manages the public IPs for you. You don't "buy a block" from an ISP; you request them via API or let the system allocate them.

- **Outbound Source NAT (Internet Access):**
  - **Remote Networks:** By default, traffic from a branch to the Internet is NATed to a public IP allocated to that specific Compute Node.
  - **Mobile Users:** Traffic is NATed to a public IP from the Gateway's pool.
- **Inbound Destination NAT:**
  - **Limitations:** Prisma Access is primarily for *outbound* protection. While it *can* support inbound NAT (publishing a server), it is generally recommended to use **GlobalProtect** or **ZTNA** for access rather than opening public ports.[289]

3. Service Connection Source NAT (The "Gotcha")

When Mobile Users or Branches access your Data Center via a **Service Connection**, IP overlap is a common issue.

- **The Problem:** If your Mobile User pool (192.168.10.x) overlaps with a subnet in your Data Center, routing breaks.
- **The Solution:** You can enable **Source NAT on the Service Connection**.
  - **Traffic Flow:** Mobile User (192.168.10.5) → Service Connection.
  - **Action:** The SC translates the source IP to a unique IP (e.g., 10.50.0.5) that *is* routable in your DC.

    - **Configuration:** Check the "Source NAT" box in the Service Connection settings and assign a non-overlapping pool.[290]
    - **Default Behavior:** By default, Source NAT is **disabled** on Dedicated Service Connections, meaning the DC sees the real user IP.[291]

4. Policy Implementation Steps

1. **Define Objects:** Create address groups for "HQ-Servers" and "Branch-Subnets."
2. **Create Security Rule:** Allow `Zone: Trust` → `Zone: Service-Conn` for App: `SAP-ERP`.
3. **Create NAT Rule (If needed):** If going to Internet, create a NAT rule `Zone: Trust` → `Zone: Untrust` using "Dynamic IP and Port" (Interface Address).[292] [293]

⁂

Prisma Access Monitoring and Logging (Strata Logging Service)

To monitor and log traffic in Prisma Access, you must use the **Strata Logging Service** (formerly Cortex Data Lake). Because Prisma Access consists of ephemeral cloud containers with no persistent local storage, it cannot store logs "on the box" like a physical firewall.

1. Strata Logging Service (SLS)

SLS is the centralized, cloud-native repository for all logs generated by Palo Alto Networks cloud products (Prisma Access, Cloud NGFW) and on-premise firewalls that are configured to send logs there.

- **Role:** It acts as the "hard drive" for your cloud firewalls.
- **Region Selection:** When deploying Prisma Access, you select a "Logging Region" (e.g., US, EU) to ensure data residency compliance (GDPR, etc.). All logs stay within that boundary.[304]
- **Quota:** You purchase storage based on retention days (e.g., 30 days, 1 year) or daily ingestion rate (GB/day).

2. Monitoring Interfaces

You visualize the data stored in SLS using two primary tools:

- **Strata Cloud Manager (SCM):**
    - **Unified Dashboard:** The modern interface. It shows real-time dashboards for **Mobile Users** (connected status, gateway location) and **Remote Networks** (tunnel status, bandwidth usage).[305]
    - **Autonomous DEM (ADEM):** A critical add-on integrated into SCM. It provides *hop-by-hop* visibility from the user's laptop → WiFi → ISP → Prisma Access → SaaS App. It tells you if the "slowness" is the user's home WiFi or the application itself.[306]

- **Panorama:**
    - If you manage Prisma Access via Panorama, it pulls log *metadata* or queries SLS to display logs in the familiar `Monitor > Traffic` tab. You do *not* store the heavy logs on Panorama itself; it just acts as a viewer for the cloud data.[307]

3. Log Forwarding (Getting Data OUT)

SLS is not a "black hole." You can forward logs from SLS to your own SIEM or archive.

- **Log Forwarding App:** A cloud service that functions as a bridge. It reads logs from SLS and forwards them to:
    - **Syslog:** Sends logs to an on-prem HTTPS-to-Syslog collector.
    - **Email:** For alerts.
    - **HTTPS:** For generic API ingestion.
- **ServiceNow Integration:** Native integration to open tickets based on alerts in SLS.

4. Application Experience (ADEM)

Standard firewall logs show "Allow/Block." They do not show "Slow."

- **ADEM (Autonomous Digital Experience Management):**
    - **Synthetic Tests:** The GlobalProtect agent runs periodic ping/http tests to common apps (Zoom, O365).
    - **Visualization:** SCM displays a "Experience Score" (0-100) for every user. If a user complains, you check their score to see exactly which segment (Device, WiFi, ISP, Gateway) is failing.[306]

Exam Note: Connectivity

Prisma Access nodes (Gateways/Portals) must have connectivity to the Strata Logging Service. If this link breaks, the nodes will queue logs locally in a small buffer until connectivity is restored, ensuring no data loss during brief outages.

⁂

Options for managing Strata and SASE Solutions

There are two primary options for managing Palo Alto Networks Strata (NGFW) and SASE solutions, plus a local option for standalone devices. The choice depends largely on whether your environment is "cloud-first" or "hardware-heavy."

1. Strata Cloud Manager (SCM)

Strata Cloud Manager (formerly Prisma Access Cloud Management) is the modern, AI-powered unified management platform. It is the default for new SASE deployments and is increasingly capable of managing physical NGFWs.

- **Scope:** Native management for **Prisma SASE** (Prisma Access + Prisma SD-WAN) and **Strata NGFW** (Hardware PA-Series, VM-Series, and Cloud NGFW).[308] [309]
- **Key Features:**
    - **Unified Policy:** Manage firewalls and SASE from a single rulebase.
    - **AIOps Integration:** Built-in predictive analytics to detect misconfigurations (e.g., "This rule shadows another") and health issues before they cause outages.[310]
    - **No Infrastructure:** It is a SaaS service; you do not need to install or patch a management server.[311]
- **Best For:** Cloud-first organizations, SASE deployments, and those wanting "single pane of glass" visibility across hybrid estates without maintaining on-prem management servers.

2. Panorama

Panorama is the traditional, on-premise (or virtual appliance) centralized management solution. It is the industry standard for managing large estates of physical firewalls.

- **Scope:** Manages all **Strata NGFW** form factors (PA, VM, CN) and historically **Prisma Access** (via the "Panorama Managed" mode).[312] [308]
- **Key Features:**
    - **Device Groups & Templates:** Hierarchical management (e.g., Global Rules → Regional Rules → Local Rules).
    - **Log Aggregation:** Acts as a local log collector (with optional dedicated Log Collectors) for compliance and reporting.
    - **Air-Gapped Support:** Can run in completely isolated networks (SCM cannot).
- **Transition Note:** Existing "Panorama Managed" Prisma Access customers can migrate to SCM using a one-way automated tool, but new SASE features (like SASE 3.0) often debut in SCM first.[311]

3. Local Management (On-Box)

You can manage any physical or virtual firewall directly via its HTTPS web interface.

- **Scope:** Single device only.
- **Best For:** Small businesses with 1-2 firewalls, or troubleshooting when the central manager is unreachable.

Comparison Table

Feature	Strata Cloud Manager (SCM)	Panorama
Deployment	**SaaS** (Cloud-Hosted)	**On-Prem** (VM or Hardware Appliance)
Primary Focus	**SASE** (Prisma Access/SD-WAN) & Modern NGFW	**NGFW** (Physical/Virtual) & Legacy SASE
Maintenance	Auto-updated by Palo Alto Networks	Manual upgrades/patches required
Policy Logic	Unified Rulebase (Cloud + On-Prem)	Device Groups & Templates hierarchy
AIOps	Native / Built-in	Requires AIOps Premium license/connector
Prisma SASE	**Recommended** (Native Support)	Supported (Legacy Mode)

Exam Tip: Management Coexistence

For the NetSec-Pro exam, remember that you cannot manage the *same* specific firewall instance with *both* Panorama and SCM simultaneously for configuration. You must choose one "source of truth" for the config. However, SCM can often overlay *monitoring* (AIOps) on Panorama-managed devices.[310]

⁂

Panorama

Panorama is the centralized management system for Palo Alto Networks firewalls. It provides a single pane of glass for managing configuration, policies, and logs across potentially thousands of devices.

1. Management Architecture (The "Brain")

Panorama splits configuration into two distinct hierarchies: **Device Groups** and **Templates**.

- **Device Groups (Policy):**
    - **Function:** Manage **Security Policies** (Rules) and **Objects** (Addresses, App-ID).
    - **Hierarchy:** You can nest groups (e.g., Global > Regional > Local). Rules cascade down.
        - **Pre-Rules:** Pushed *before* any local firewall rules (top priority).
        - **Post-Rules:** Pushed *after* local firewall rules (bottom priority/cleanup).
        - **Default Behavior:** Firewalls can belong to only **one** device group.[323]
- **Templates & Template Stacks (Network):**
    - **Function:** Manage **Network/Device Settings** (Interfaces, Zones, DNS, NTP, RADIUS).
    - **Stacking:** You combine multiple templates into a **Template Stack** (e.g., "Global_Base" + "NTP_Settings" + "Site_A_Network"). The stack is then assigned to the firewall.[324]

    - **Variable:** You can use variables (e.g., `$Public_IP`) in a template so that multiple firewalls share the same template but have unique IP values.[324]

2. Log Collection (The "Memory")

Panorama can act as a Log Collector, or you can deploy dedicated **Log Collectors (M-Series or Virtual)**.

- **Managed Collectors:** Dedicated appliances (e.g., M-600, M-700) whose sole job is to ingest and store logs.
- **Collector Groups:** You group collectors (e.g., "US-East-Logs") and assign firewalls to send logs to that group.
- **Sizing:** Critical factors are **Ingestion Rate** (Logs/Sec) and **Retention Period**.
    - *Limit:* A single M-600 can handle ~50,000 logs/sec.[325]
    - *Design:* Use "Collector Groups" to redistribute load if you exceed the limit of one box.[325]

3. High Availability (HA)

Panorama supports **Active/Passive** HA to ensure management availability.

- **Sync:** The two Panorama appliances synchronize their configuration and log metadata.
- **Failover:** If the Primary fails, the Secondary takes over IP addresses (if configured) or admins just log into the Secondary.
- **Requirement:** Both peers must be the same model and software version.[326]

4. Commit Process

Committing in Panorama is a two-step process:

1. **Commit to Panorama:** Saves changes to the Panorama database itself.
2. **Push to Devices:** Sends the configuration (XML) to the managed firewalls.
    - *Note:* You can "Commit and Push" in one action, or push to specific Device Groups/Templates.[327]
    - *Validation:* Panorama validates the config against the target device model *before* pushing to prevent errors (e.g., pushing 100Gbps interface settings to a PA-220).[327]

⁂

strata cloud manager (SCM)

Strata Cloud Manager (SCM) is the unified, AI-powered management platform for the entire Palo Alto Networks estate (NGFW, Prisma Access, and SD-WAN). It represents the shift from "static" management (Panorama) to "active" operations.

1. Unified Management

SCM replaces the need for separate managers (Panorama for firewalls, Cloud Management for SASE).

- **Scope:** Manages physical **PA-Series**, virtual **VM-Series**, **Prisma Access**, and **Cloud NGFW** from one dashboard.
- **Workflow:** Uses a modern "Config → Push" model similar to Panorama but cloud-native. It supports **Snippets** (reusable config blocks) which are more flexible than Panorama's Templates.[338]
- **Zero Touch Provisioning (ZTP):** Simplified onboarding. You claim a device by Serial Number in the portal, and it automatically connects, downloads its config, and updates itself—no "staging" needed.[339] [338]

2. AIOps Integration

This is SCM's "killer feature." It doesn't just manage config; it manages *health*.

- **Predictive Analytics:** Analyzes 50,000+ data points to predict hardware failures (e.g., "Disk will fill up in 48 hours") or capacity issues.[340] [341]
- **Best Practice Validation:** Before you commit a rule, SCM analyzes it against industry standards (NIST, CIS) and warns you if it creates a security gap.[342]
- **Policy Analyzer:** Automatically finds unused rules, shadowed rules, and overly permissive rules, offering "Clean Up" suggestions.[342]

3. Licensing Tiers

SCM introduced a simplified licensing model in late 2024/2025.

- **SCM Essentials (Free):** Basic config management and lifecycle operations. Available to anyone with a valid support contract.[343] [344]
- **SCM Pro (Paid):** Adds the advanced "AI" features: AIOps, ADEM (User Experience monitoring), Strata Logging Service (unlimited storage/1 year retention), and predictive forecasting.[343]

4. Migration from Panorama

For existing customers, SCM includes a **Migration Tool**.

- **Capabilities:** It can import Panorama configuration (Device Groups/Templates) and convert them into SCM Folders and Snippets.
- **Coexistence:** You can migrate *parts* of your estate (e.g., branch firewalls) to SCM while keeping complex Data Center firewalls on Panorama, or move everything at once.[345] [341]

Exam Note: Onboarding

To onboard a firewall to SCM:

1. **License:** Ensure the device has a valid support license.
2. **App Connect:** The device must talk to the cloud (Strata Logging Service).
3. **Claim:** Enter the Serial Number in SCM.
4. **Verify:** The device status changes to "Connected," and SCM pushes a "Day 1" config.[346][339]

⁂

1. https://www.youtube.com/watch?v=aXk-UwpcrCY
2. https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-firewall-ngfw
3. https://www.pass4success.com/palo-alto-networks/exam/netsec-pro
4. https://www.nwexam.com/palo-alto/palo-alto-netsec-pro-certification-exam-syllabus
5. https://www.youtube.com/watch?v=CnAXJ770yHs
6. https://www.scribd.com/document/894523978/Paloalto-Networks-NetSec-Pro-unlocked-2
7. https://www.perplexity.ai/search/4b2b7484-e5e0-457b-ac36-c4ea7313003d
8. https://www.reddit.com/r/Practicequestion/comments/1okk4m5/netsecpro_questions_for_passing_palo_alto/
9. https://www.perplexity.ai/search/c9acdef9-4ba0-4565-8e39-cad5f07c20cd
10. https://www.passquestion.com/news/PaloAlto-Networks-Certified-Network-Security-Professional-NetSec-Pro-Exam-Questions.html
11. https://www.slideshare.net/slideshow/palo-alto-netsec-pro-study-notes-and-practice-tests/283770130
12. https://www.globalknowledge.com/en-ae/products/palo_alto_networks/pan-cnsp
13. https://www.marks4sure.com/NetSec-Generalist-exam.html
14. https://www.scribd.com/document/894523996/Paloalto-Networks-NetSec-Pro-unlocked-1
15. https://www.uninets.com/blog/network-security-generalist-certification-guide
16. https://www.passsureexam.com/NetSec-Pro-pass4sure-exam-dumps.html
17. https://www.paloaltonetworks.com/services/education/palo-alto-networks-netsec-professional
18. https://www.paloaltonetworks.com/cyberpedia/what-is-a-perimeter-firewall
19. https://www.youtube.com/watch?v=Oopl6mQ7PIM
20. https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation
21. https://inspiritvision.com/perimeter-security-vs-zero-trust-architecture/
22. https://www.aztechit.co.uk/blog/zero-trust-vs-traditional-perimeter-security
23. https://www.nwexam.com/palo-alto/palo-alto-netsec-pro-certification-exam-syllabus
24. https://www.networkworld.com/article/4089591/arista-palo-alto-bolster-ai-data-center-security.html
25. https://dev.to/clouddefenseai/zero-trust-security-vs-perimeter-security-key-differences-48jk
26. https://datacipher.net/palo-alto-networks-netsec-professional-certification-guide/
27. https://www.youtube.com/watch?v=XzbnFbbzzoE

28. https://www.paloaltonetworks.com/cyberpedia/sase-vs-firewall
29. https://www.pass4success.com/palo-alto-networks/exam/netsec-pro
30. https://www.paloaltonetworks.com/services/education/palo-alto-networks-netsec-professional
31. https://www.reddit.com/r/paloaltonetworks/comments/1p33mm1/palo_alto_certifications_postupdate_pcnsa_vs/
32. https://www.linkedin.com/posts/palo-alto-networks-education-services_get-ready-to-validate-your-expertise-at-the-activity-7389712850698629121-L6Hg
33. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/network/network-zones/security-zone-overview
34. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/getting-started/segment-your-network-using-interfaces-and-zones
35. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/panorama-integration-overview/configure-zone-based-policy-rules
36. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/network-segmentation-using-zones
37. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-zone-protection
38. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection
39. https://www.thenetworkdna.com/2023/02/a-comprehensive-guide-to-palo-alto-zone.html
40. https://faatech.be/security-policies-best-practices-palo-alto-networks-next-gen-firewalls/
41. https://docs.prismacloud.io/en/enterprise-edition/policy-reference/panos-policies/panos-policies-index/ansible-panos-14
42. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/flood-protection
43. https://help.ivanti.com/ps/help/en_US/IPS/22.x/ag/configuring_palo_alto_networks_firewall.htm
44. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles
45. https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-security-zones-creation-and-configuration.html
46. https://networkdevicesinc.com/community/blog/palo-alto-firewall-setup-pan-os-guide
47. https://www.youtube.com/watch?v=dBKC6Q0dpdk
48. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-zone-protection
49. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles
50. https://www.scribd.com/document/909011186/DoS-Zone-Protection
51. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clm9CAC&lang=en_US
52. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection
53. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004O5JCAU&lang=en_US

54. https://ninjamie.fandom.com/wiki/Network_Profiles
55. https://www.stigviewer.com/stigs/palo_alto_networks_alg/2025-03-12/finding/V-228860
56. https://www.reddit.com/r/paloaltonetworks/comments/ys50sj/help_with_dos_protection_for_inbound_tcp_floods/
57. https://www.tenable.com/audits/items/CIS_Palo_Alto_Firewall_10_Benchmark_v1.2.0_L1.audit:711b838f8a01b447ad06ee56bb88d4b5
58. https://www.youtube.com/watch?v=YM4jXOx1ZTQ
59. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/flood-protection
60. https://www.reddit.com/r/paloaltonetworks/comments/4tkgd4/zone_protection_profiles_best_practice/
61. https://www.sunmanagement.net/wp-content/uploads/2020/01/Lab2-Zone-DoS-Protection-V1.1.pdf
62. https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices
63. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-cps
64. https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dos-protection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds/how-to-measure-cps
65. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles/flood-protection
66. https://www.coursehero.com/file/248106651/dos-and-zone-protection-best-practicespdf/
67. https://faspco.com/academy/Ebook/Microsoft/9781803241418-MASTERINGPALOALTONETWORKS_1_.pdf
68. https://www.reddit.com/r/paloaltonetworks/comments/8bwaw4/zone_protection_setting_and_tuning_best_practices/
69. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZKCA0
70. https://xsoar.pan.dev/docs/reference/integrations/palo-alto-networks-prisma-cloud-compute
71. https://www.cliffsnotes.com/study-notes/28488996
72. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking
73. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds
74. https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dos-protection/zone-defense/take-baseline-cps-measurements-for-setting-flood-thresholds
75. https://myworldofit.net/?p=11069
76. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-protection-profiles
77. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClsVCAS
78. https://docs.prismacloud.io/en/enterprise-edition/content-collections/administration/anomalies/anomaly-thresholds
79. https://docs.paloaltonetworks.com/ngfw/administration/high-availability/ha-modes
80. https://docs.paloaltonetworks.com/ngfw/administration/high-availability/ha-links-and-backup-links

81. https://www.examsnap.com/certification/configuring-high-availability-on-palo-alto-firewalls-step-by-step/
82. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/high-availability/ha-clustering-best-practices-and-provisioning
83. https://www.reddit.com/r/paloaltonetworks/comments/xi8fxw/paloalto_cluster_upgrade_diffrent_nodes_version/
84. https://www.reddit.com/r/paloaltonetworks/comments/102pvjc/palo_alto_licensing_conundrum/
85. https://www.cbtnuggets.com/blog/certifications/security/what-is-palo-alto-fw-high-availability
86. https://www.jscape.com/blog/active-active-vs-active-passive-high-availability-cluster
87. https://www.reddit.com/r/networking/comments/12zeflz/question_regarding_ha_firewall_in_activepassive/
88. https://www.youtube.com/watch?v=l27tr7LxZk0
89. https://www.linkedin.com/posts/anupam-singh1986_networking-firewall-cybersecurity-activity-7387311147840028672-zfCH
90. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004OKTCA2
91. https://live.paloaltonetworks.com/t5/general-topics/active-passive-vs-active-active/td-p/68584
92. https://www.youtube.com/watch?v=qINhuFI2Fv4
93. https://www.megaport.com/blog/high-availability-with-palo-alto-networks-and-megaport/
94. https://digitalscepter.com/articles/2022-11-11-cli-cheatsheet
95. https://github.com/PacktPublishing/Mastering-Palo-Alto-Networks/blob/master/chapter 13 - CLI cheat sheet
96. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClpnCAC
97. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000004MiOCAU&lang=en_US
98. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cla2CAC&lang=en_US
99. https://www.reddit.com/r/paloaltonetworks/comments/uhxf47/am_i_crazy_is_there_no_way_to_clear_arp_on_an/
100. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000g1QwCAI&lang=en_US
101. https://docs.paloaltonetworks.com/prisma-sd-wan/ion-cli-reference/use-cli-commands/inspect-commands/inspect-system-arp
102. https://community.spiceworks.com/t/how-to-properly-clear-arp-cache-from-domain-server/585432
103. https://www.youtube.com/watch?v=4ZMYlEwtVXs
104. https://blog.ipspace.net/2023/08/arp-static-routes/
105. https://docs.paloaltonetworks.com/prisma-sd-wan/ion-cli-reference/use-cli-commands/clear-commands/clear-flow-arp
106. https://www.reddit.com/r/networking/comments/z9z4tq/activepassive_f5_behind_activepassive_palo_alto/
107. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-cli-quick-start/cli-cheat-sheets/cli-cheat-sheet-networking
108. https://www.reddit.com/r/paloaltonetworks/comments/so38t8/policy_order/
109. https://live.paloaltonetworks.com/t5/general-topics/precedence-of-routing-nat-policy/td-p/525630
110. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/nat/nat-policy-rules

111. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClhwCAC
112. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rule-best-practices
113. https://docs.paloaltonetworks.com/content/techdocs/en_US/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rulebase-best-practices
114. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-policy
115. https://www.linkedin.com/pulse/palo-alto-networks-network-address-translation-nat-part-rivai
116. https://www.routeprotocol.com/palo-alto-edu-110-security-and-nat-policies/
117. https://docs.paloaltonetworks.com/ngfw/networking/nat/source-and-destination-nat-example
118. https://berkeley.service-now.com/kb_view.do?sys_kb_id=3e1073cb470c6a50702449df016d43e0
119. https://trainingcamp.com/glossary/rule-shadowing/
120. https://www.facebook.com/groups/460147274176964/posts/1083366725188346/
121. https://www.youtube.com/watch?v=WFowKYo5ZPQ
122. https://cybrec.com/blog/network-security/nat-palo-alto-firewall/
123. https://www.ibm.com/docs/en/security-qradar/log-insights/saas?topic=series-palo-alto-pa-data-source-type-specifications
124. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/view-and-manage-logs/log-types-and-severity-levels
125. https://docs.arcticwolf.com/bundle/m_syslog/page/configure_a_palo_alto_networks_panorama_platform_to_send_log.html
126. https://docs.taegis.secureworks.com/integration/connectNetwork/palo_alto_firewall/
127. https://www.youtube.com/watch?v=f2lrt6gDnu0
128. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-the-application-command-center
129. https://docs.paloaltonetworks.com/strata-logging-service
130. https://xsoar.pan.dev/docs/reference/integrations/cortex-data-lake
131. https://pan.dev/splunk/docs/tune-or-reduce-firewall-logs/
132. https://cordero.me/palo-alto-session-logging/
133. https://knowledgebase.paloaltonetworks.com/articles/en_US/Knowledge/Session-Log-Best-Practices-59397
134. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/monitor/monitor-logs/log-types
135. https://docs.paloaltonetworks.com/network-security/security-policy/administration/objects/log-forwarding/configure-a-log-forwarding-profile-pm
136. https://docs.cloud.google.com/chronicle/docs/ingestion/default-parsers/pan-firewall
137. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding
138. https://www.paloaltonetworks.com/sase/app-acceleration
139. https://siliconangle.com/2024/05/02/palo-alto-networks-launches-prisma-sase-3-0-enhanced-device-security/
140. https://www.thefastmode.com/technology-solutions/35777-palo-alto-networks-launches-prisma-sase-3-0

141. https://www.youtube.com/watch?v=kn-OR-tt_v0
142. https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/quality-of-service
143. https://docs.paloaltonetworks.com/network-security/quality-of-service/administration/prioritize-network-traffic-using-qos
144. https://directortic.es/exclusive-networks/wp-content/uploads/sites/7/2023/12/salesforce.pdf
145. https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/sd-wan-strata.pdf
146. https://www.firewall.cx/security/palo-alto-networks/configuring-qos-on-palo-alto-firewalls.html
147. https://www.paloaltonetworks.com/cyberpedia/what-is-wan-optimization-wan-acceleration
148. https://www.paloaltonetworks.com/sase/sd-wan
149. https://docs.paloaltonetworks.com/prisma-sd-wan
150. https://www.reddit.com/r/paloaltonetworks/comments/1bx1ii6/what_are_disadvantages_of_palo_alto_sdwan_not/
151. https://www.paloguard.com/sd-wan.asp
152. https://www.cisco.com/c/dam/en/us/products/collateral/routers/competitive-comparison-chart.pdf
153. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/policy-based-forwarding/pbf
154. https://live.paloaltonetworks.com/t5/general-topics/does-palo-alto-do-nat-before-doing-policy-based-forwarding/td-p/327440
155. https://www.youtube.com/watch?v=Ahrao6kBg8w
156. https://www.linkedin.com/pulse/palo-alto-networks-network-address-translation-nat-part-rivai
157. https://docs.paloaltonetworks.com/ngfw/administration/high-availability/set-up-activeactive-ha/configure-activeactive-ha
158. https://www.reddit.com/r/paloaltonetworks/comments/i17sh8/policybased_routing_vs_routes_defined_on_vr/
159. https://weberblog.net/policy-based-forwarding-pbf-on-a-palo-alto-firewall/
160. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/device/device-high-availability/ha-link-and-path-monitoring
161. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/policies/policies-nat
162. https://www.reddit.com/r/paloaltonetworks/comments/pt79l0/traffic_flow_based_on_the_nat_table/
163. https://bluecatnetworks.com/blog/palo-alto-networks-advanced-administration-tips/
164. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000010zHNCAY&lang=en_US
165. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/nat/nat-policy-rules
166. https://www.reddit.com/r/paloaltonetworks/comments/199lhwn/path_monitoring_on_static_routes_vs_policy_based/
167. https://docs.paloaltonetworks.com/ngfw/networking/nat/configure-nat
168. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/advanced-routing/configure-ospfv2-on-an-advanced-routing-engine
169. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/advanced-routing/configure-ospfv3-on-an-advanced-routing-engine
170. https://ipwithease.com/configuring-the-ospf-not-so-stubby-area-nssa/
171. https://blog.davidvassallo.me/2013/04/04/palo-alto-networks-implementing-conditional-advertising-in-bgp/

172. https://www.reddit.com/r/paloaltonetworks/comments/1q1pri8/can_palo_alto_ngfw_do_bgp_conditional/
173. https://adminsave.wordpress.com/2019/07/05/bgp-conditional-advertisement-palo-alto-ngfw/
174. https://www.youtube.com/watch?v=PSJK8WF9pO0
175. https://www.youtube.com/watch?v=JWFdpYCDGso
176. https://live.paloaltonetworks.com/t5/general-topics/ospf-between-virtual-routers/td-p/63380
177. https://www.reddit.com/r/paloaltonetworks/comments/oboozs/bgp_best_practices_in_palo_alto/
178. https://www.youtube.com/watch?v=78×7_7og9XA
179. https://ns3edu.com/blog/steps-to-configure-ospf-open-shortest-path-first-on-a-palo-alto-networks-firewall/
180. https://www.youtube.com/watch?v=PA0Bo3K2N8A
181. https://docs.paloaltonetworks.com/ngfw/networking/configure-virtual-routers
182. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/bgp
183. https://networklessons.com/ospf/ospf-lsa-types-explained
184. https://www.uninets.com/blog/ospf-lsa-types
185. https://letmetechyou.com/how-ospf-link-state-advertisement-works/
186. https://www.kwtrain.com/blog/ospf-basics-pt3
187. https://www.reddit.com/r/networking/comments/3qc11e/what_is_the_difference_between_ospf_lsa_types_5/
188. https://www.networkacademy.io/ccna/ospf/ospf-area-types
189. https://www.exam-labs.com/blog/understanding-ospf-area-structure-and-lsa-types-enhancing-network-performance-and-scalability
190. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXqCAK
191. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/ospf/ospf-concepts
192. https://www.router-switch.com/faq/6-types-of-ospf-lsa.html
193. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/ospf
194. https://networkjourney.com/ospf-lsa-types-explained-complete-guide-with-cli-eve-ng-lab-real-world-use-cases-ccnp-enterprise/
195. https://www.youtube.com/watch?v=MPPZ7Y0hpzc
196. https://www.digitaltut.com/ospf-lsa-types-lab
197. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/ospf
198. https://www.tufin.com/blog/zone-based-firewall
199. https://www.linkedin.com/pulse/palo-alto-firewalls-security-zones-tap-zone-virtual-wire-partsenidis
200. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/network/network-zones/security-zone-overview
201. https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-security-zones-creation-and-configuration.html
202. https://docs.paloaltonetworks.com/ngfw/getting-started/initial-setup-configuration-ngfws/segment-your-network/configure-interfaces-and-zones
203. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/getting-started/segment-your-network-using-interfaces-and-zones/configure-interfaces-and-zones

204. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/panorama-integration-overview/configure-zone-based-policy-rules

205. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/service-connection-advanced-deployments/use-traffic-forwarding-rules-with-service-connections/configure-zone-mapping-and-security-policies-for-dedicated-connections

206. https://www.youtube.com/watch?v=pu0ITCYtcoI

207. https://www.youtube.com/watch?v=dBKC6Q0dpdk

208. https://www.reddit.com/r/paloaltonetworks/comments/1ksl5p4/destination_zone_specification/

209. https://community.checkpoint.com/t5/General-Topics/Difference-between-interface-based-and-zone-based-firewall/td-p/4191

210. https://www.packtpub.com/en-us/product/mastering-palo-alto-networks-third-edition-9781836644811/chapter/understanding-the-core-technologies-1/section/understanding-the-zone-based-firewall-ch01lvl1sec03

211. https://www.reddit.com/r/paloaltonetworks/comments/1hj9uln/firewall_zone_design_and_best_practices/

212. https://www.reddit.com/r/mikrotik/comments/1mlwqf1/explain_like_im_five_what_is_the_benefits_of_zone/

213. https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/performance-policy-with-forward-error-correction-fec/add-performance-policy-sla

214. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/performance-policy-with-forward-error-correction-fec

215. https://docs.paloaltonetworks.com/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/use-external-services-for-monitoring/syslog-server-support-in-prisma-sd-wan/syslog-flow-export

216. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-sd-wan/administration/prisma-sd-wan-sites-and-devices/set-up-sites/view-flows-tab

217. https://packetpushers.net/blog/simplify-complex-wan-operations-with-next-gen-sd-wan/

218. https://www.paloaltonetworks.com/blog/2021/03/prisma-sd-wan-aiops/

219. https://docs.paloaltonetworks.com/prisma/prisma-sd-wan/prisma-sd-wan-admin/prisma-sd-wan-stacked-policies/configure-syslog-profiles

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

221. 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

222. https://www.ibm.com/docs/en/sevone-npm/8.1.0?topic=other-sdwan-palo-alto-prisma-agent-circuit

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

224. https://www.youtube.com/watch?v=FzFGY281BlI

225. https://www.reddit.com/r/paloaltonetworks/comments/1f0196r/prisma_sdwan_faulty_line_path_selection/

226. https://www.scribd.com/document/845157871/Prisma-Sd-Wan-Administration

227. https://docs.paloaltonetworks.com/autonomous-dem/administration/viewing-adem-data/netsec-health/netsec-health-monitored-apps

228. https://docs.paloaltonetworks.com/saas-security/data-security/syslog-and-api-integration

229. https://marketplace.microsoft.com/en-us/product/azure-applications/azuresentinel.azure-sentinel-solution-paloaltocdl?tab=overview
230. https://pan.dev/cdl/api/log-forwarding/
231. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000saj5CAA&lang=en_US
232. https://splunk.github.io/splunk-app-for-palo-alto-networks/print_page/
233. https://splunkbase.splunk.com/app/7505
234. https://splunk.github.io/splunk-add-on-for-palo-alto-networks/
235. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/integration/microsoft-integrations-with-prisma-access/set-up-syslog-forwarding-to-microsoft-sentinel
236. https://cybersectalk.com/2020/06/26/how-to-reduce-noise-in-your-siem/
237. https://docs.rapid7.com/insightidr/palo-alto-cortex-data-lake/
238. https://www.reddit.com/r/paloaltonetworks/comments/1h0k9yp/syslog_and_cortex_data_lake/
239. https://documentation.securonix.com/bundle/securonix-cloud-user-guide/page/content/data-dictionary/mapping-by-parser/detailed-mapping-for-palo-alto-cortex-xdr-syslog.htm
240. https://github.com/PaloAltoNetworks/cdl-decompress-proxy-sentinel-ingest
241. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding
242. https://invgate.com/itdb/cortex-data-lake
243. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-service-connections/use-a-service-connection-to-enable-access-between-mobile-users-and-remote-networks
244. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-service-connections
245. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/set-up-globalprotect-mobile-users
246. https://www.youtube.com/watch?v=EB4eJ-d6G90
247. https://support.beyondidentity.com/hc/en-us/articles/13104801693079-Integration-Guide-for-Palo-Alto-Networks-Prisma-Access
248. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/globalprotect-app-settings
249. https://docs.paloaltonetworks.com/prisma-access/administration/privileged-remote-access/set-up-the-privileged-remote-access-portal
250. https://www.youtube.com/watch?v=gGwFvi8rvqU
251. https://www.reddit.com/r/paloaltonetworks/comments/10jz6k4/prisma_access_service_connections_remote_networks/
252. https://docs.paloaltonetworks.com/prisma-access-agent/administration/configure-the-agent/set-up-the-agent/configure-gateways
253. https://www.reddit.com/r/paloaltonetworks/comments/1ame0fw/always_on_vpn_global_protect/
254. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-remote-networks
255. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect
256. https://www.youtube.com/watch?v=hldjFFxzZhc
257. https://www.reddit.com/r/paloaltonetworks/comments/1j0i2uk/prisma_access_cloud_globalprotect_authentication/

258. https://www.reddit.com/r/paloaltonetworks/comments/10jz6k4/prisma_access_service_connections_remote_networks/
259. https://www.packetswitch.co.uk/prisma-access-sase-service-connections-vs-remote-networks/
260. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-remote-networks/allocate-remote-network-bandwidth
261. https://docs.paloaltonetworks.com/prisma-access/activation-and-onboarding/your-prisma-access-license/remote-networks-site-based-licensing
262. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/administration/prisma-access-remote-networks/connect-a-remote-network-site-to-prisma-access
263. https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn/set-up-ipsec/set-up-an-ipsec-tunnel
264. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-remote-networks/onboard-a-remote-network
265. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-remote-networks/enable-routing-for-your-remote-network
266. https://www.reddit.com/r/paloaltonetworks/comments/xe8qdm/prisma_access_for_mobile_w_bgp_peering_over/
267. https://www.youtube.com/watch?v=xy1dDSGXqDk
268. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/service-connection-advanced-deployments/bgp-filtering-and-route-metric-support-on-prisma-access
269. https://community.checkpoint.com/t5/General-Topics/IPSec-VPN-between-CheckPoint-and-Prisma-Access/td-p/237160
270. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/service-connection-advanced-deployments/route-preferences-for-service-connection-traffic
271. https://github.com/PaloAltoNetworks/prisma-access-skillets/blob/master/README.md
272. https://docs.cradlepoint.com/r/Connecting-Palo-Alto-Prisma-Access-to-a-Cradlepoint-Router/Configuring-Prisma-Access
273. https://docs.paloaltonetworks.com/prisma-access/administration/ztna-connector-in-prisma-access
274. https://cyber.levelblue.com/m/52d05cb514c89c62/original/PB-Unified-Approach-With-Prisma.pdf
275. https://docs.paloaltonetworks.com/prisma-access-agent/administration/configure-the-agent/set-up-proxy-support-for-prisma-access-agent
276. https://www.paloguard.com/Prisma-Access.asp
277. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/administration/app-security-overview
278. https://www.youtube.com/watch?v=eA-hpo2_uss
279. https://www.nomios.lu/en/partners/palo-alto-networks/prisma-cloud-security/access/
280. https://www.reddit.com/r/paloaltonetworks/comments/1ki3a8v/prisma_access_browser_private_internal_apps/
281. https://structured.com/wp-content/uploads/2020/11/PANW-Prisma-Access-Datasheet.pdf
282. https://www.paloaltonetworks.com/resources/guides/sec-private-app-access-with-ztna-connector-design-guide

283. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/prisma-access-app-features
284. https://www.paloaltonetworks.com/blog/sase/secure-your-app-verse-with-prisma-access-private-application-security/
285. https://www.boll.ch/datasheets/Prisma_Access_AAG.pdf
286. https://www.optiv.com/insights/discover/blog/palo-alto-networks-prisma-access-inbound-traffic-support
287. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/administration/app-security-overview/app-security-visibility-and-logging
288. https://docs.paloaltonetworks.com/network-security/security-policy/administration/all-policy-types
289. https://www.optiv.com/insights/discover/blog/palo-alto-networks-prisma-access-inbound-traffic-support
290. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-service-connections/configure-a-service-connection
291. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/service-connection-advanced-deployments/use-traffic-forwarding-rules-with-service-connections/configure-traffic-steering
292. https://docs.paloaltonetworks.com/network-security/security-policy/administration/all-policy-types/nat
293. https://www.reddit.com/r/paloaltonetworks/comments/ebkq4j/security_rule_and_nat_confusion/
294. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-service-connections/use-a-service-connection-to-enable-access-between-mobile-users-and-remote-networks
295. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-setup/retrieve-ip-addresses-for-prisma-access
296. https://www.reddit.com/r/paloaltonetworks/comments/10jz6k4/prisma_access_service_connections_remote_networks/
297. https://docs.paloaltonetworks.com/content/techdocs/en_US/prisma-access/activation-and-onboarding/onboard-prisma-access/onboarding-workflow-for-service-connections
298. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-rules
299. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-setup/remote-networks-service-ip-and-egress-ip-address-allocation
300. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-remote-networks
301. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-policy
302. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/network-policies
303. https://www.reddit.com/r/paloaltonetworks/comments/p64cgz/strata_vs_prisma_what_did_you_opt_for_and_why/
304. https://docs.paloaltonetworks.com/strata-logging-service
305. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/prisma-access-app-features
306. https://docs.paloaltonetworks.com/autonomous-dem/administration/viewing-adem-data/netsec-health/netsec-health-monitored-apps
307. https://docs.arcticwolf.com/bundle/m_syslog/page/configure_a_palo_alto_networks_panorama_platform_to_send_log.html

308. https://www.wei.com/blog/how-to-strengthen-firewall-automation-with-panorama-and-strata-cloud-manager/
309. https://www.paloaltonetworks.com/network-security/strata-cloud-manager
310. https://www.paloaltonetworks.com/blog/network-security/strata-cloud-manager-the-unified-choice-for-managing-sase-and-ngfw/
311. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/migrate-prisma-access-from-panorama-to-strata-cloud-manager
312. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/how-to-manage-prisma-access
313. https://www.youtube.com/watch?v=5nxt7R9d-YI
314. https://www.reddit.com/r/paloaltonetworks/comments/1bnfo33/strata_cloud_manager_vs_panorama/
315. https://www.youtube.com/watch?v=jORudgknWx8
316. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/migrate-from-panorama-to-strata-cloud-manager
317. https://www.youtube.com/watch?v=z0msWbgTAaI
318. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/prisma-access-app-features
319. https://www.linkedin.com/pulse/when-strata-cloud-manager-scm-replace-panorama-complex-joe-brunner-bpyhe
320. https://live.paloaltonetworks.com/t5/panorama-discussions/panorama-to-strata-cloud-manager-anyone-using-in-production/td-p/628007
321. https://www.reddit.com/r/paloaltonetworks/comments/1ntbnx8/panorama_vs_strata/
322. https://docs.paloaltonetworks.com/compatibility-matrix/reference/feature-parity
323. https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-device-groups
324. https://docs.paloaltonetworks.com/vm-series/10-2/vm-series-deployment/set-up-the-vm-series-firewall-on-nsx/set-up-the-vm-series-firewall-on-nsx-t-east-west/deploy-the-vm-series-firewall-on-nsx-t-east-west/create-templates-and-device-groups-on-panorama-nsx-t-ew
325. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HBw7CAG&lang=en_US
326. https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-high-availability
327. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations
328. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Clc8CAC&lang=en_US
329. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/high-availability/set-up-activepassive-ha/configure-activepassive-ha
330. https://www.pangurus.com/forum/general-discussion/doubts-about-device-group-template-stack-and-shared-objects
331. https://www.youtube.com/watch?v=OqT46zqSB0A
332. https://www.reddit.com/r/paloaltonetworks/comments/xvxpz3/panorama_sizing/
333. https://www.youtube.com/watch?v=Xa11BqHbSSs
334. https://www.reddit.com/r/paloaltonetworks/comments/ggftyy/how_do_you_guys_typically_do_your_device_groups/

335. https://www.techclick.in/differences-between-device-group-and-template-in-panorama-in-paloalto
336. https://pan.dev/terraform/docs/panos/guides/panorama-config/
337. https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups
338. https://www.linkedin.com/pulse/when-strata-cloud-manager-scm-replace-panorama-complex-joe-brunner-bpyhe
339. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/onboard-to-strata-cloud-manager
340. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-august-2025
341. https://docs.paloaltonetworks.com/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-september-2025
342. https://www.scribd.com/document/896583062/Strata-Cloud-Manager-AIOps
343. https://docs.paloaltonetworks.com/whats-new/new-features/october-2024/strata-cloud-manager-licenses
344. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/activate-strata-cloud-manager
345. https://docs.paloaltonetworks.com/strata-cloud-manager/release-notes/new-features-strata-cloud-manager/new-features-in-october-2025/2025-october-features-configuration-management
346. https://docs.paloaltonetworks.com/ngfw/getting-started/onboard-your-ngfws/onboard-a-firewall
347. https://docs.paloaltonetworks.com/content/techdocs/en_US/strata-cloud-manager/getting-started/configuration-scm/configuration-onboarding
348. https://www.youtube.com/watch?v=KVEBpdGZxrc
349. https://docs.paloaltonetworks.com/strata-cloud-manager/activation-and-onboarding/validate-strata-cloud-manager-onboarding
350. https://www.reddit.com/r/paloaltonetworks/comments/1kf2f32/strata_cloud_manager_onboarding_firewall_with/
351. https://www.mbtechtalker.com/scm-device-onboarding/
352. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/overview