Palo Alto Conectivity and Security

In the Palo Alto Networks ecosystem, **"Connectivity and Security"** refers to the two fundamental architectural pillars of **Prisma Access (SASE)** and the unified management approach in **Strata Cloud Manager (SCM)**.

For your **Network Security Professional (NSP)** certification studies, understanding this separation is critical because the exam domains and configuration workflows are divided strictly along these lines.

1. The Architectural Split (SASE/Prisma Access)

Palo Alto Networks decouples infrastructure into two distinct layers. This allows "networking" to scale independently from "inspection". [1] [2]

Feature	**Connectivity (Networking Layer)**	**Security (Inspection Layer)**
Role	Gets traffic *to* the cloud. Handles routing, tunnels, and bandwidth.	Inspects traffic *in* the cloud. Enforces policy and threat prevention.
Infrastructure	**Connectivity Nodes:** Dedicated instances that terminate tunnels and handle routing (BGP/Static).	**Security Processing Nodes (SPN):** Dedicated cloud firewalls that process resource-intensive inspections (SSL Decryption, WildFire).
Components	**Service Connections (SC-CAN):** IPSec tunnels to Data Centers/HQ. **Remote Networks (RN-SPN):** IPSec tunnels to Branch Offices. **Mobile Users (MU):** GlobalProtect & ZTNA connectors.	**Security Policies:** Allow/Deny rules (App-ID, User-ID). **Security Profiles:** Antivirus, DNS Security, URL Filtering. **Decryption:** SSL/TLS inspection policies.

2. Strata Cloud Manager (SCM) Implementation

In your lab or production environment, SCM (formerly Prisma Access Cloud Management) organizes these distinct workflows to unify management across Cloud (Prisma) and On-Prem (Strata). [3] [4]

- **Connectivity Configuration:**
  - **Location:** Found under **Workflows > Onboarding** or **Network** settings.
  - **Tasks:** You configure **IPSec Tunnels**, **IKE Gateways**, **BGP Routing**, and **Bandwidth allocation** here.
  - **Goal:** Establish the "pipes" that carry traffic from branches/users to the Palo Alto cloud.
- **Security Configuration:**

- **Location:** Found under **Configuration > Security Policy** or **Security Services**.
- **Tasks:** You configure **Unified Security Policies** that can apply globally to both Prisma Access and physical NGFWs.
- **Goal:** Define "who can access what" and "what threats to block" once the traffic is inside the pipe.

3. NSP Certification Context

The NSP exam structure explicitly mirrors this dichotomy. You should separate your study time into these two buckets:

- **Domain: Secure Connectivity Across Hybrid Environments**
  - **Focus:** How to onboard a Branch Office (Remote Network), how to configure a Service Connection to a Data Center for backend access, and how GlobalProtect connects Mobile Users.[5]
  - **Key Study Topic:** Routing (BGP), QoS, and the difference between Service Connections (which don't inspect traffic) and Remote Networks (which do).
- **Domain: Build a Strong Network Security Foundation**
  - **Focus:** Best Practice Assessment (BPA) rules, App-ID adoption, SSL Decryption (Forward Proxy), and Cloud-Delivered Security Services (CDSS) like Advanced Threat Prevention.[6]

4. Troubleshooting "Connectivity vs. Security"

For the exam, learn to distinguish issues based on this split:

- **Connectivity Issue:** A user **cannot connect** at all (VPN fails, tunnel is down). *Check: IKE crypto profiles, BGP peering, or License bandwidth.*
- **Security Issue:** A user **connects but cannot access a specific site** (Blocked page, connection reset). *Check: Security Policy, Decryption exclusions, or URL Filtering categories.*

⁂

IKE crypto profiles

An **IKE Crypto Profile** defines the protocols and algorithms used to secure the *initial handshake* (Phase 1) between your Palo Alto Networks device (or Prisma Access) and a remote peer (like a branch router or AWS VPN Gateway).

Think of it as the "security badge check" before the actual "data tunnel" (IPSec Phase 2) is built. If this badge check fails, the tunnel never comes up.

1. The Role: Phase 1 vs. Phase 2

For your NSP exam and troubleshooting, you must distinguish between the two profiles:

- **IKE Crypto Profile (Phase 1):** Secures the *management channel*. It negotiates how the two devices will talk securely to exchange keys.
- **IPSec Crypto Profile (Phase 2):** Secures the *actual data*. It defines how user traffic inside the tunnel is encrypted.

2. Configuration in Strata Cloud Manager (SCM)

In SCM, unlike PAN-OS where profiles have their own top-level menu, these are often embedded within the workflow.[27]

- **Location: Workflows > Onboarding > Remote Networks > [Select Site] > Primary Tunnel > IKE Advanced Options**.
- **Alternative (Direct): Manage > Configuration > Network > Network Profiles > IKE Crypto**.

3. Critical Parameters

You must match these exactly on both sides (Local and Peer), or the connection will fail immediately.[28]

Parameter	Function	Recommendation (Best Practice)	Avoid (Legacy/Weak)
DH Group	Diffie-Hellman key exchange group. Determines the strength of the key generation.	**Group 19** (256-bit Elliptic Curve) or **Group 20** [29]	Group 1, 2, 5 (Too weak for modern standards)
Encryption	Scrambles the handshake packets.	**AES-256-GCM** or **AES-256-CBC**	3DES, DES, RC4
Authentication	Verifies data integrity (hash).	**SHA-384** or **SHA-256**	MD5, SHA-1
Lifetime	How long the security association (SA) lasts before re-keying.	**8 Hours** (28,800 seconds) or **24 Hours**	Less than 1 hour (causes excessive overhead)

Note on AES-GCM: If you select **AES-GCM** for encryption, the "Authentication" field is often set to 'None' or ignored because GCM handles both encryption and integrity authentication natively.[29]

4. Troubleshooting Phase 1 Failures

When a tunnel is down, check **Monitor > System Logs** (filter: `subtype eq vpn`). Look for these specific errors to identify IKE Profile mismatches:[30] [31]

- **Error:** `"IKE phase-1 negotiation is failed"`
- **Detail:** `"no proposal chosen"` or `"mismatched proposal"`

    - **Meaning:** The peer sent a list of algorithms (e.g., DH2, AES128, SHA1), but your IKE Crypto Profile only allows stronger ones (e.g., DH19, AES256, SHA256). They couldn't agree on a common language.
- **Detail:** `"authentication failed"`
    - **Meaning:** Usually a Pre-Shared Key (PSK) mismatch, not necessarily the crypto profile itself, but often grouped in Phase 1 troubleshooting.

5. Best Practice Strategy

Do not just create one profile with every possible algorithm (e.g., adding MD5 and 3DES "just in case"). This is a security risk (downgrade attack).

- **Create a "Modern" Profile:** (AES-256-GCM, SHA-384, DH19) for new sites.
- **Create a "Legacy" Profile:** (AES-128, SHA-1, DH2) *only* for old hardware that cannot support better standards, and migrate them as soon as possible.

⁂

maintain and configure network security of on-premisses, cloud, and hybrid networks network segmentation

To **maintain and configure network security** with a focus on **network segmentation** across hybrid environments (On-Premises, Cloud, and Hybrid), you should align your strategy with the **Zero Trust** methodology and use **Strata Cloud Manager (SCM)** as your unified command center.

This aligns directly with the "Build a Strong Network Security Foundation" and "Secure Connectivity" domains of the **NSP certification**.[42]

1. The Strategy: Zero Trust Segmentation

In the Palo Alto Networks ecosystem, segmentation is not just about VLANs; it is about defining **Trust Boundaries** using the "Kipling Method" (Who, What, Where, When, Why, How).[43]

- **Identify the Protect Surface:** Instead of protecting the whole "Attack Surface," identify specific Critical Assets (DAAS - Data, Applications, Assets, Services).[44]
- **Define Transactions:** Map how traffic flows between these assets.
- **Architect the Zero Trust Network:** Place a segmentation gateway (NGFW or Prisma Access) as close to the asset as possible.

2. Configuration: Implementing Segmentation in SCM

Strata Cloud Manager unifies segmentation for both physical firewalls and cloud services.

A. On-Premises (NGFW)

You use **Zones** and **Tags** to create logical boundaries, regardless of the physical wiring.[45] [46]

- **Configure Zones:**
  - **Path:** `Configuration > NGFW > Device Settings > Zones`
  - **Action:** Create separate zones for `Trust`, `Untrust`, `DMZ`, `Guest`, `IoT`, and `DataCenter`.
  - **Best Practice:** Never create a rule that allows traffic from `Any` zone to `Any` zone. Always be explicit (e.g., `IoT` to `DataCenter`).
- **Micro-Segmentation (Tags & DAGs):**
  - **Path:** `Configuration > Objects > Tags`
  - **Action:** Create Dynamic Address Groups (DAGs) that group servers based on tags (e.g., `Windows`, `Web-Server`) rather than static IPs. This allows policy to follow the workload automatically.[47] [48]

B. Cloud (Prisma Access)

Segmentation in the cloud moves away from physical interfaces to **Service Connections** and **User-ID**.[49] [50]

- **Remote Networks (Branches):** Traffic from branches is segmented by the tunnel it arrives on. You can assign different Security Zones to different Remote Network IPSec tunnels.
- **Mobile Users:** Segment users based on **User-ID** groups (e.g., "HR-Users" vs. "IT-Admins") rather than IP subnets.
- **Traffic Steering:** Use **Traffic Forwarding Rules** to ensure sensitive traffic (e.g., to the ERP system) is routed through a specific Service Connection that enforces strict inspection, while general web traffic goes direct-to-internet (after inspection).

C. Hybrid (Unified Policy)

Use SCM to create **Device Groups** or **Folders** that apply a baseline segmentation policy across *all* environments.

- **Hierarchy:** Create a `Global` folder for universal blocks (e.g., Block QUIC, Block High-Risk Geos).
- **Specifics:** Create child folders for `Cloud-Prisma` and `OnPrem-HQ` to handle environment-specific segmentation nuances.

3. Maintenance: Keeping Segmentation "Clean"

Segmentation "rot" occurs when rules become too open over time.

- **Policy Optimizer:** Use this tool (found in the Policy tab) to identify "Over-provisioned" rules. It shows you rules that allow `App-ID: Any` but actually only see 3 specific applications. Convert these to explicit allow rules to tighten segmentation.[42]

- **Best Practice Assessment (BPA):** Run the BPA regularly. It specifically checks if your zones are distinct and if you are using "Zone Protection Profiles" to prevent packet-flood attacks across segment boundaries.
- **Log Monitoring:** Filter logs for `action=allow` and `zone_from != zone_to` to audit cross-segment traffic regularly.

4. Summary Table: Segmentation Across Environments

Feature	On-Premises (NGFW)	Cloud (Prisma Access)	Hybrid Integration (SCM)
Boundary	Physical Interface / VLAN	Service Connection / Tunnel	Folder / Device Group
Enforcement	Zone Protection Profile	Security Processing Node (SPN)	Unified Security Policy
Identity	User-ID Agent	GlobalProtect / Cloud Identity	Cloud Identity Engine (CIE)
Dynamic Grouping	Dynamic Address Groups (DAG)	User Groups (AD/SAML)	Shared Tags & Objects

For your NSP exam, remember: **Segmentation is the primary defense against Lateral Movement.** If an examiner asks how to stop ransomware spreading from a user laptop to a server, the answer is "Strict Zone-based Segmentation and App-ID policies," not just "Antivirus."

⁂

maintain and configure network security of on-premisses, cloud, and hybrid polices (security and network)

For your **Network Security Professional (NSP)** certification and real-world administration, "Maintaining and Configuring" involves using **Strata Cloud Manager (SCM)** to unify rule sets across On-Premises (NGFW), Cloud (Prisma Access), and Hybrid environments.

The key to mastering this is understanding that SCM separates **Security** (Access Control) from **Network** (Connectivity/Traffic Handling) while using **Folders** to manage the hybrid scale.

1. Unified Management Structure (Hybrid Policies)

Instead of managing distinct "cloud rules" and "firewall rules," SCM uses a hierarchical **Folder** structure. Policies defined at the top flow down to all environments.[57] [58]

- **The Folder Hierarchy (Inheritance):**
  - **All Firewalls (Global):** Place universal rules here.
    - *Security Ex:* "Block High-Risk Geographies" or "Block QUIC protocol."
    - *Network Ex:* "Global QoS Profile" for VoIP.

- **Environment Folders (Child):** Create folders like "Prisma Access" and "Data Center."
  - *Inheritance:* A rule created in "All Firewalls" appears in "Data Center" as **read-only** (often highlighted in green/gray). You cannot delete it locally, ensuring compliance.
  - *Shadowing:* If you create a local rule that conflicts with a global rule, SCM will warn you about "Rule Shadowing".[59]

2. Configuring Security Policies (Access Control)

This domain focuses on "Who can access What".[60]

- **The Goal:** Move from Port-based rules (Legacy) to App-ID (Zero Trust).
- **Workflow:**
  1. **Define Objects:** Create address objects and Tags (e.g., `Tag: Web-Server`).
  2. **Create Rule:** `Source: Any` → `Dest: Web-Server` → `App: ssl, web-browsing` → `Action: Allow` → `Profile: Best-Practice-Security`.
- **Hybrid Tip:** Use **Variables**.
  - Create a variable `$DNS_Servers`.
  - In the "Data Center" folder, set `$DNS_Servers = 10.1.1.5`.
  - In the "Prisma Access" folder, set `$DNS_Servers = 8.8.8.8`.
  - Write *one* security rule: `Allow Trust to $DNS_Servers`. It works everywhere automatically.

3. Configuring Network Policies (Traffic Handling)

"Network Policies" in SCM/NSP typically refer to **QoS**, **NAT**, and **PBF** (Policy Based Forwarding). These do not block traffic; they manipulate how it flows.[61] [62]

- **QoS Policy:** Critical for SASE. You must prioritize Zoom/Teams traffic over YouTube.
  - *Config:* Create a QoS Profile (Class 1 = Realtime). Apply a QoS Policy rule: `App: Zoom` → `Class: 1`.
- **NAT Policy:**
  - *Prisma Access:* mostly handles Source NAT automatically for internet traffic. You configure specific NAT rules for "Service Connections" (overlapping subnets).
  - *On-Prem:* You must manually configure Source NAT (for internet) and Destination NAT (for hosted servers).
- **PBF (Policy Based Forwarding):**
  - *Use Case:* Force specific traffic (e.g., Office 365) to go out a cheap local ISP link instead of the expensive MPLS tunnel.

4. Maintenance & Lifecycle (The "Maintain" Phase)

Policies rot over time. You must actively clean them.[63] [60]

- **Policy Optimizer:** This is your primary maintenance tool.
  - *Action:* Go to **Policies > Security > Policy Optimizer**.
  - *Task:* Look for "Port-Based Rules." It will show you "Rule #5 allows port 443, but only `facebook-base` has been seen on it for 30 days."
  - *Fix:* Click "Create Cloned Rule" to replace the generic port 443 rule with an explicit `App-ID: facebook-base` rule.
- **Best Practice Assessment (BPA):** SCM allows you to run an "On-Demand BPA." It audits your config against NIST/CIS standards. Run this monthly.
- **Rule Usage Filters:** Filter your policy view by `Hit Count = 0` (Unused) or `Last Hit Date > 90 days`. Disable and eventually delete these rules to reduce attack surface.

Summary Checklist for NSP Exam

- **Connectivity (Network):** Focus on **QoS** for user experience and **PBF/Routing** for path selection.
- **Security:** Focus on **App-ID adoption** and **SSL Decryption**.
- **Management:** Focus on **Folder Inheritance** and **Variables** to minimize administrative overhead.

⁂

maintain and configure network security of on-premisses, cloud, and hybrid Monitoring and logging

For the "Monitoring and Logging" domain of your **Network Security Professional (NSP)** preparation, you must focus on how **Strata Cloud Manager (SCM)** serves as the unified visibility pane for both On-Premises and Cloud (Prisma Access) environments, backed by **Cortex Data Lake**.

1. Unified Visibility Architecture

In the old world, you looked at logs on the local firewall or Panorama. In the SCM/SASE world, **all logs** from all locations (Branch firewalls, Prisma Access users, Data Centers) are sent to **Cortex Data Lake (CDL)**.

- **Strata Cloud Manager (SCM)** acts as the *viewer* for this data.
- **Cortex Data Lake** acts as the *storage* backend.

2. Key Monitoring Workflows in SCM

For the exam and daily operations, master these three SCM sections:

A. Dashboards (High-Level Visibility)

- **Path:** `Dashboards`
- **Use Case:** Quick health and threat checks.
  - **Prisma Access Usage:** Shows active mobile users, bandwidth consumption, and licensing peaks.
  - **Threat Insights:** Summarizes top blocked threats (Malware, C2) across the hybrid estate.[72]
  - **AIOps Integration:** SCM automatically flags "Operational Health" issues, such as a firewall with high CPU or a tunnel with frequent flaps, often predicting bottlenecks before they cause outages.[73]

B. Explore (The Log Viewer)

- **Path:** `Monitor > Logs > Explore` (or sometimes `Incidents > Explore`)
- **Function:** This is the equivalent of the `Monitor > Traffic` tab in PAN-OS.
- **Query Language:** SCM uses a SQL-like query language (Cortex Query Language - CQL) which is more powerful than the legacy filter.
  - *Example:* `network.app eq 'facebook' and action eq 'block'`
- **Unified Context:** A single query returns results from your physical HQ firewall AND your remote users in Prisma Access. You don't need to switch contexts.[74]

C. Application Command Center (ACC)

- **Function:** Visualizes trends. "Who is my top bandwidth user?" or "What is the most common high-risk application?"
- **NSP Tip:** Know that ACC data is aggregated. If you see a spike in "Web-Browsing," you can drill down (click on the graph) to jump directly to the **Explore** tab for the raw logs.

3. Configuring Log Forwarding (The "Hybrid" Aspect)

To send logs *out* of the Palo Alto ecosystem (e.g., to Splunk or a SIEM), you configure **Log Forwarding Profiles** in SCM.[75] [76]

Component	Configuration in SCM
Profile Location	`Objects > Log Forwarding Profile`
Scope	Create in a **Folder** (e.g., "Global") to apply to all firewalls/Prisma Access, or a specific folder for local-only logging.
Destinations	**Syslog, Email, HTTP/S, SNMP**.

Component	Configuration in SCM
Auto-Tagging	*Critical Exam Topic:* You can set a Log Forwarding Profile to **automatically tag** a source IP if it triggers a specific threat ID. This tag can then be used in a Dynamic Address Group to block that IP instantly across the whole network.

4. Maintenance: Cortex Data Lake Quotas

You don't "clear logs" on the firewall anymore. You manage **Quotas** in CDL.[77]

- **Path:** `Configuration > Data Lake > Log Storage`
- **Action:** You must allocate percentages of your total storage to different log types.
  - *Traffic Logs:* High volume, usually get ~40-50%.
  - *Threat Logs:* Lower volume but critical retention, usually ~20%.
  - *Decryption Logs:* Extremely high volume; ensure you have enough quota or disable them for trusted traffic if space is tight.
- **Retention Policy:** If logs exceed the quota, oldest logs are overwritten. SCM will warn you if your retention drops below compliance limits (e.g., < 30 days).[78]

Summary Checklist for NSP Exam

- **Troubleshooting:** Use **Explore** to find "Why was this packet dropped?" (Look for `session_end_reason`).
- **Capacity:** Use **Dashboards** to see if you are hitting User/Bandwidth license limits.
- **Configuration:** Always attach a **Log Forwarding Profile** to your Security Policy rules; otherwise, traffic is not logged to the SIEM.
- **Storage:** If logs are missing from 3 months ago, check your **CDL Quotas**, not the firewall disk space.

⁂

maintain and configure network security of on-premisses, cloud, and hybrid certificates

For the **NSP certification** and enterprise security operations, **certificate management** is critical across hybrid environments because certificates enable **SSL Decryption** (visibility into encrypted traffic), **secure management interfaces**, and **GlobalProtect VPN authentication**.

In **Strata Cloud Manager (SCM)**, certificate configuration extends across both On-Premises NGFWs and Prisma Access, requiring unified PKI planning.

1. The Three Certificate Use Cases

Understanding *where* and *why* certificates are used is essential for the NSP exam:[87] [88]

Certificate Type	Purpose	Trust Requirement	Deployment Location
Forward Trust Certificate	Used in SSL Forward Proxy (outbound decryption). The firewall presents this to clients when it intercepts HTTPS traffic.	Must be **trusted** by all clients (installed in their cert stores).	On-Prem NGFW & Prisma Access
Forward Untrust Certificate	Used to authenticate to external servers during SSL Forward Proxy.	Must **NOT** be trusted by clients (it's the firewall's client-side cert).	On-Prem NGFW & Prisma Access
Management Interface Certificate	Secures the web GUI and API access to the firewall/SCM.	Trusted by administrators' browsers.	On-Prem NGFW, Panorama, SCM

2. Configuring Certificates in Strata Cloud Manager

A. SSL Decryption Certificates (Forward Trust)

This is the most common certificate use case and a **critical NSP exam topic**.[89] [87]

Best Practice Workflow:

1. **Generate a Certificate Signing Request (CSR) in SCM:**
   - **Path:** `Configuration > NGFW and Prisma Access > Objects > Certificate Management > Generate`
   - **Settings:**
     - **Certificate Name:** Use a unique name per device or location (e.g., `HQ-FW01-ForwardTrust`)
     - **Signed By:** Select `External Authority (CSR)`
     - **Certificate Use For:** Select `Forward Trust Certificate`
     - **Algorithm:** RSA 2048-bit (minimum), RSA 4096-bit (recommended)
     - **Digest:** SHA-256 or SHA-384
2. **Sign the CSR with Your Enterprise PKI:**
   - Export the CSR and submit it to your internal Certificate Authority (Active Directory Certificate Services or similar).
   - The CA signs it and returns a signed certificate.[90] [91]
3. **Import the Signed Certificate:**
   - **Path:** `Configuration > Objects > Certificate Management > Import`
   - Upload the signed certificate and the **complete certificate chain** (Root CA + Intermediate CA).[88]

4. **Distribute the Root CA to All Clients:**
    - **For Windows Domain:** Use Group Policy to push the enterprise Root CA to `Trusted Root Certification Authorities` on all workstations.
    - **For GlobalProtect Clients:** Configure auto-deployment via the GlobalProtect Portal configuration.[92]
        - **Path:** `Network > GlobalProtect > Portal > [Edit Portal] > Agent > Trusted Root CA`
        - Check **"Install in Local Root Certificate Store"** to transparently push the certificate to endpoints.

B. Certificate Profile Configuration

After importing certificates, create a **Certificate Profile** to reference them in decryption policies.[87]

- **Path:** `Configuration > Objects > Certificate Profile`
- **Action:** Add your Forward Trust certificate and the CA certificate chain.
- **Usage:** Attach this profile to your **Decryption Policy Rule** (type: SSL Forward Proxy).

3. Hybrid Certificate Challenges & Solutions

Challenge 1: Multiple Firewalls with the Same Certificate

If you use the same Forward Trust certificate on 100 firewalls and later need to revoke it, all 100 devices lose decryption capability.[87]

Solution: Generate unique certificates per device or per location. When troubleshooting, users will see which specific firewall is intercepting their traffic in the certificate error details.

Challenge 2: Linux/Non-Windows Clients

Linux systems and some applications (Java, Python) do not use the Windows certificate store.[91]

Solution:

- Manually import the Root CA into the system-specific trust store (e.g., `/etc/ssl/certs/` on Ubuntu).
- For containerized applications, inject the CA certificate into the container image build process.

Challenge 3: Prisma Access + On-Prem Certificate Consistency

When migrating from Panorama to SCM, default Prisma Access certificates may not match your on-prem PKI, causing trust errors for remote users.[93]

Solution: Use the **Global Scope** in SCM to define a unified Forward Trust certificate that applies to both Prisma Access and physical NGFWs, ensuring consistent trust across the hybrid environment.

4. Maintenance: Certificate Lifecycle Management

Expiration Monitoring

- **Path:** `Monitor > Logs > System` (filter for `certificate expiration warnings`)
- **Best Practice:** Set alerts 90 days before expiration. Renew certificates at least 60 days in advance to allow time for client distribution.[94]

Certificate Revocation

If a certificate is compromised:

1. Revoke it via your enterprise PKI's Certificate Revocation List (CRL).
2. Replace the certificate in SCM and push the updated certificate profile to all managed devices.
3. Verify that clients receive the updated Root CA via GlobalProtect or Group Policy.

5. NSP Exam Focus: SSL Forward Proxy Workflow

For the exam, memorize this end-to-end flow:[95] [87]

1. **Client** initiates HTTPS request to `google.com`.
2. **Firewall (NGFW/Prisma Access)** intercepts the connection using the **Forward Untrust Certificate** to authenticate to Google.
3. **Firewall** generates a **new certificate** for `google.com`, signed by the **Forward Trust CA**.
4. **Client** receives the firewall-generated certificate. If the Forward Trust CA is in the client's trust store, the connection succeeds without warning.
5. **Firewall** decrypts, inspects (applies Security Policies, Threat Prevention), and re-encrypts the traffic before forwarding to Google.

Key Troubleshooting: If users see "Certificate Not Trusted" warnings, the Forward Trust certificate is not installed in their certificate store or has expired.

⁂

Maintain connectivity and security of remote users

To **maintain and configure connectivity and security** for remote users (Prisma Access Mobile Users / GlobalProtect) in Strata Cloud Manager (SCM), you must manage the end-to-end lifecycle: from the **GlobalProtect App** on the device to the **Service Connection** in the cloud.

1. Connectivity: Configuring GlobalProtect in SCM

Connectivity for remote users relies on the **GlobalProtect App** connecting to a **Gateway**. In SCM, this is unified under Prisma Access configuration.[102] [103]

- **Portal Configuration (The "Manager"):**
  - **Path:** `Configuration > NGFW and Prisma Access > Mobile Users > GlobalProtect > Portals`.
  - **Function:** Tells the app *where* to connect (Gateway list) and *how* to behave (App settings).
  - **Agent Config:** Define "Agent Configs" to assign different settings to different users (e.g., "IT-Admins" get different settings than "HR-Users").
- **Gateway Configuration (The "Tunnel Endpoint"):**
  - **Path:** `Configuration > ... > Gateways`.
  - **Function:** This is where the tunnel terminates. You configure **IP Pools** here to assign internal IP addresses to remote clients.
- **Split Tunneling (Optimizing Traffic):**
  - **Best Practice:** Do not tunnel *everything*. Bandwidth-heavy apps like YouTube or trusted SaaS like Office 365 should go direct-to-internet to save Prisma Access bandwidth.[104]
  - **Config:** inside the **Agent Config > Split Tunnel**, exclude specific domains (e.g., `*.zoom.us`, `*.netflix.com`) or application processes (e.g., `outlook.exe`).

2. Security: Posture & Inspection

Once connected, you must secure the user *and* the device.

- **HIP Checks (Host Information Profile):**
  - **Concept:** "Zero Trust for the Endpoint." Verify the device state before allowing access. [105] [106]
  - **Workflow:**
    1. **Object:** Create a HIP Object (e.g., "Win10-Encrypted-Patched").
    2. **Profile:** Create a HIP Profile that requires that Object *and* "Antivirus = Active."
    3. **Policy:** Add this HIP Profile to your **Security Policy**. Rule: `Source: Mobile_Users` → `HIP Profile: Win10-Secure` → `Action: Allow`.
  - *Result:* If a user turns off their firewall, they instantly lose access to sensitive apps.

- **User-ID:**
  - Ensure your **Cloud Identity Engine (CIE)** is synced with Azure AD/Okta so policies can use user names (`domain\user`) instead of IPs.

3. Maintenance & Troubleshooting (ADEM)

The biggest challenge with remote users is "My internet is slow." Is it the Wi-Fi, the ISP, or Prisma Access?

- **ADEM (Autonomous Digital Experience Management):**
  - **Tool:** Use the **ADEM Dashboard** in SCM. [107] [108]
  - **Capabilities:** It installs a micro-agent with GlobalProtect. It actively pings synthetic tests to Zoom/Teams.
  - **Root Cause Analysis:** It explicitly tells you: "High Latency detected on **User's Local Wi-Fi**" vs "Packet loss on **ISP Hops**." This saves hours of troubleshooting.
- **App Updates:**
  - **Path:** `Configuration > Mobile Users > GlobalProtect > App Activation`.
  - **Strategy:** Always test a new version on an "Early Adopters" group before pushing it to "All Users." Set the update to "Transparent" so users are upgraded automatically without prompts.

Summary Checklist for NSP Exam

- **Connectivity: Split Tunneling** reduces latency for trusted SaaS.
- **Security: HIP Profiles** enforce device compliance (OS patches, Disk Encryption).
- **Troubleshooting: ADEM** is the primary tool for user-experience issues (latency/jitter).
- **Policy:** Always use **User-ID** for mobile user policies, never IP addresses (as they change).

⁂

Maintain connectivity and security of remote users remote access solutions

In the Palo Alto Networks ecosystem, "Remote Access Solutions" now extend well beyond traditional VPNs. For your **NSP certification** and daily "Maintain and Configure" duties in **Strata Cloud Manager (SCM)**, you must master the differences between the four primary solutions: **GlobalProtect**, **Clientless VPN**, **Prisma Access Browser**, and **Explicit Proxy**.

Here is how to maintain and configure each, matching the right solution to the right user.

1. GlobalProtect (The "Standard" Agent)

This is the primary solution for **Managed Devices** where you have full control.

- **Connectivity Maintenance:**
  - **Split Tunneling:** Maintain an "Exclude Video/SaaS" list to optimize bandwidth. A common maintenance task is updating this list as new SaaS apps (like a new HR portal) are adopted.
  - **Gateway Selection:** In SCM, configure "Source Region" priority so users connect to the closest cloud gateway.
  - **Agent Updates:** Use **Transparent Upgrades** in SCM (`Mobile Users > GlobalProtect > App Activation`) to keep agents patched without user interaction.
- **Security Maintenance:**
  - **HIP Checks:** Enforce device posture (Disk Encrypted? OS Patched?) before allowing access.
  - **Decryption:** Deploy the Forward Trust Certificate to the machine store so you can inspect SSL traffic inside the tunnel.

2. Privileged Remote Access (PRA)

This is the modern solution for **Unmanaged Devices** (Contractors/OT) needing access to non-web apps (RDP/SSH) without an agent.[117]

- **Use Case:** A vendor needs to RDP into a server, but you cannot install GlobalProtect on their laptop.
- **Configuration:**
  - **Path:** `Configuration > Privileged Remote Access`.
  - **Workflow:** You define a "Target" (the server IP/Protocol) and assign it to a "Portal." The vendor logs into a web portal, clicks "RDP," and the session renders *in their browser* via HTML5.
- **Security Maintenance:**
  - **Session Controls:** In the PRA Profile, you can explicitly **Disable Copy/Paste** or **File Transfer** to prevent data exfiltration.[118]
  - **Session Recording:** Enable recording to audit exactly what commands the contractor typed during their SSH session.

3. Prisma Access Browser (The "Enterprise Browser")

This is replacing Clientless VPN for **Unmanaged Devices** accessing Web Apps (SaaS/Private Web).[119]

- **Concept:** Instead of a full VPN tunnel, the user works inside a managed browser (or a managed profile in Chrome/Edge).
- **Connectivity Maintenance:**

- **No Tunnel:** Connectivity is just HTTPS.

- **Security Maintenance:**
  - **Browser Policy:** You configure policies like "Block Screen Capture," "Block Print," or "Watermark Screens" to protect data displayed on an unmanaged home PC.
  - **Cookie Control:** Ensure session cookies cannot be copied to another browser.

4. Explicit Proxy (The "PAC File" Method)

This is for **Mobile Users** who cannot use the IPsec/SSL VPN driver (e.g., behind a strict partner firewall or on specialized mobile OSs).[120] [121]

- **Connectivity Maintenance:**
  - **PAC Files:** You must maintain a Proxy Auto-Config (PAC) file hosted in Prisma Access.
  - **Task:** Update the PAC file to tell the browser "Send internal traffic to Prisma, send Netflix direct."
- **Security Maintenance:**
  - **Auth Headers:** Unlike GlobalProtect (which authenticates the *interface*), Explicit Proxy authenticates the *HTTP Header*. Ensure your authentication profile (SAML/Okta) supports "Cookie-based" auth for this flow.

Comparison Summary for NSP Exam

Feature	GlobalProtect	Privileged Remote Access (PRA)	Prisma Access Browser	Explicit Proxy
Best For	Managed Laptops (Full Access)	Contractors / OT (RDP/SSH)	Unmanaged / BYOD (Web Apps)	Compliance / Restricted Networks
Connectivity	IPsec/SSL Tunnel	HTML5 (Web Socket)	HTTPS (Browser-based)	HTTP CONNECT / PAC File
Agent Required?	Yes	No	Yes (Managed Browser)	No (PAC File)
Key Maintenance	App Updates, Split Tunnel lists	Session Recording reviews	Data Loss Prevention (DLP) rules	PAC File updates

NSP Exam Tip: If a scenario asks "How to secure a contractor needing RDP access without installing software," the answer is **Privileged Remote Access (PRA)**. If it asks "How to secure a partner accessing a web portal," the modern answer is **Prisma Access Browser** (though Clientless VPN is the legacy answer).

⁂

Maintain connectivity and security of remote users network segmentation

To **maintain and configure network segmentation** for remote users (Prisma Access/GlobalProtect), you must shift away from traditional "VLAN/Subnet" thinking toward **Identity-Based Segmentation (User-ID)** and **Traffic Steering**.

In a cloud-native world, users don't have a fixed "desk" or "VLAN," so their security segment must travel with them.

1. Identity-Based Segmentation (The Zero Trust Standard)

The primary method for segmenting remote users is not by IP, but by **who they are**.[132] [133]

- **User-ID Group Mapping:**
  - **Concept:** Integrate **Cloud Identity Engine (CIE)** with Azure AD/Okta. This lets you write rules like `Source: "HR-Users"` rather than `Source: 10.50.1.0/24`.
  - **Configuration:**
    1. Sync your directory groups to CIE.
    2. In **Security Policy**, create a rule:
       - **Source User:** `group-finance`
       - **Destination:** `finance-server-ip`
       - **Application:** `sap-financials`
       - **Action:** `Allow`
  - **Why it's better:** If a user moves from "Marketing" to "Finance" in Active Directory, their access automatically updates without you touching the firewall policy.

2. IP-Based Segmentation (Legacy/Compliance)

Sometimes, legacy servers still require "IP-based allow-listing." You can achieve this for remote users using **IP Pools**.[134] [135]

- **Gateway IP Pools:**
  - **Path:** `Configuration > Mobile Users > GlobalProtect > Gateways > Agent > Client Settings`.
  - **Strategy:** Create different "Client Settings" configs for different user groups.
    - *Config A:* `Match Criteria: "IT-Admins"` → `IP Pool: 10.100.1.0/24`.
    - *Config B:* `Match Criteria: "Contractors"` → `IP Pool: 10.100.2.0/24`.
  - **Result:** Admin users always get an IP in the `.1.x` range, allowing you to create a "Source IP" rule on your backend Data Center firewall.

3. Traffic Steering (Service Connection Segmentation)

Once the user is in the cloud (Prisma), how do you keep their traffic separate when it goes back to your Data Center?[136] [137]

- **Dedicated Service Connections:**
  - **Scenario:** You have a "PCI-DSS" environment that must be isolated.
  - **Config:**
    1. Create a **Service Connection** specifically for the PCI zone.
    2. Use **Traffic Steering** rules to force traffic from "PCI-Users" to *only* use that specific Service Connection tunnel.
  - **Benefit:** This physically isolates the traffic path, satisfying strict compliance audits.

4. Dynamic Micro-Segmentation (Tags & HIP)

For the most granular control (e.g., preventing an infected laptop from attacking a server), use **Tags**.[138]

- **HIP-Based Segmentation:**
  - **Workflow:** If a user's GlobalProtect agent reports "Antivirus Disabled," the firewall tags their IP as `Tag: Risky-Device`.
  - **Policy:** A deny rule at the top of your policy set blocks `Source Tag: Risky-Device` from accessing critical segments. This is automated containment.

Summary Checklist for NSP Exam

- **Primary Method:** Use **User-ID** for user-to-application segmentation (e.g., HR user to HR app).
- **Legacy/Server Method:** Use **IP Pools** in Gateway Client Settings for user-to-IP segmentation (e.g., Admin IP to Firewall Mgmt IP).
- **Isolation Method:** Use **Traffic Steering** with dedicated Service Connections to keep sensitive traffic flows physically separate.

⁂

Maintain connectivity and security of remote users security policy tunning

To **tune security policies** for remote users (Prisma Access) effectively, you should focus on minimizing the attack surface while preventing "false positive" blocks that kill productivity. In **Strata Cloud Manager (SCM)**, the primary tool for this is the **Policy Optimizer**.

This domain is critical for the NSP exam because it moves you from "making it work" to "making it secure."

1. Identify and Remove Stale Rules (Hygiene)

Over time, temporary rules ("Allow-All for Testing") get forgotten.

- **Tool: Policy Optimizer > No App Specified** or **Unused Apps**.[147] [148]
- **Workflow:**
  1. Go to `Policies > Security > Policy Optimizer`.
  2. Select **Unused Apps**.
  3. Sort by **Days with No New Apps** (e.g., > 90 days).
  4. **Action:** If a rule allows `App-ID: Any` but has only seen `ssl` and `google-base` in the last 3 months, click **Migrate** to replace "Any" with just those two apps. This instantly tightens the policy without breaking verified traffic.
- **Hit Counts:** Use the "Reset Hit Count" feature during troubleshooting sessions, but rely on "Last Hit Date" for long-term cleanup.[149]

2. Transition from Port-Based to App-ID (Hardening)

Remote users on home Wi-Fi are high-risk. A rule allowing `Port 443` allows *any* evasive malware using SSL.

- **Tool: Policy Optimizer > No App Specified**.[150]
- **Goal:** Reach **100% App-ID adoption**.
- **Workflow:**
  - Identify rules with `Service: application-default` or `Service: 443`.
  - The Optimizer will list all applications actually seen on that rule (e.g., `facebook`, `bittorrent`, `office365`).
  - **Action:** Create a new rule allowing only the *business* apps (Office365) and explicitly blocking the *risk* apps (Bittorrent), then delete the port-based rule.

3. Tuning Decryption for Connectivity (Exceptions)

The #1 cause of "Connectivity Issues" for remote users is aggressive SSL Decryption breaking pinned certificates (e.g., Dropbox, Banking apps).[151]

- **Tool: Monitor > Logs > Traffic** (Filter: `session_end_reason eq decrypt-cert-validation`).
- **Tuning Workflow:**
  1. **Identify:** Users complain "Bank of America website is broken."
  2. **Verify:** Check logs for decryption failures.
  3. **Fix:** Do not turn off decryption globally.
  4. **Action:** Add the specific URL (or the predefined "Financial Services" category) to a **"Do Not Decrypt"** policy rule placed *above* your decryption rules.

5. **Best Practice:** Use a "Do Not Decrypt" rule for `Category: Health, Finance, Government` to respect user privacy and avoid technical breaks.

4. Handling SaaS Dynamics (External Dynamic Lists)

SaaS apps (Zoom, Microsoft 365) change IPs weekly. Static rules break connectivity.

- **Tool: External Dynamic Lists (EDLs)**.
- **Configuration:**
  - Instead of manually updating IPs, use the built-in `Palo Alto Networks - Microsoft 365` EDL.
  - **Policy:** `Source: Mobile_Users` → `Destination: EDL-Microsoft-365` → `Action: Allow`.
  - **Benefit:** The firewall automatically updates the IPs in the background. If Microsoft adds a new range, your users stay connected without you touching the config.

Summary Checklist for NSP Exam

- **Cleanup:** Use **Policy Optimizer** to find rules that allow "Any" app but only use a few.
- **Hardening:** Convert all Port-based rules (L4) to App-ID rules (L7).
- **Connectivity:** Use **EDLs** for SaaS apps and **Decryption Exclusions** for pinned certificates/privacy.
- **Shadowing:** SCM alerts you if a new rule is "shadowed" (blocked) by a broader rule above it. Fix these immediately to avoid confusion.[147]

⁂

Maintain connectivity and security of remote users monitoring and logging

For the **Network Security Professional (NSP)** exam and daily operations, monitoring remote users (Prisma Access) in Strata Cloud Manager (SCM) focuses on two questions: "Is the user connected?" and "Is their experience good?"

You will use **Prisma Access Insights**, **Explore (Logs)**, and **ADEM** to answer these.

1. High-Level Monitoring: Prisma Access Insights

This is your NOC dashboard. It tells you *system* health, not just user health.[162] [163]

- **Path:** `Insights > Activity Insights > Mobile Users`.
- **Key Metrics:**
  - **Current Connected Users:** Real-time count of active VPN sessions.
  - **Location Map:** Visualizes where users are connecting from. If you see 500 users in "Singapore" but you only have an office in "London," this is an anomaly.

- **Connection Failures:** A dedicated widget showing "Top Connection Failures" (e.g., Auth Failure, Certificate Error).

2. Troubleshooting Connectivity (GlobalProtect Logs)

When a user says "I can't connect," you dig into the raw logs. In SCM, GlobalProtect logs are separate from Traffic logs.[164] [165]

- **Path:** `Monitor > Logs > GlobalProtect`.
- **Key Log Types (Subtypes):**
  - **System:** Shows the tunnel setup (Phase 1/Phase 2). Look here for "Gateway Certificate Invalid" or "Authentication Failed."
  - **HIP Match:** Verifies if the user passed the Host Information Profile check. If a user is connected but blocked from the HR app, check here to see if they failed a "Patch Level" check.
  - **Ops:** Detailed debugging (tunnel up/down events).
- **Common Search Query:**
  - `(eventid eq globalprotectgateway-logout-succ)`: Finds normal disconnects.
  - `(user eq 'john.doe') and (stage eq 'login')`: Traces a specific user's login attempt.

3. Troubleshooting Experience (ADEM)

If a user says "My internet is slow," logs won't help. You need **Autonomous Digital Experience Management (ADEM)**.[166] [167]

- **The ADEM Dashboard:** `Insights > ADEM > Mobile Users`.
- **What it reveals:**
  - **Endpoint:** CPU/RAM usage of the user's laptop.
  - **Wi-Fi:** Signal strength (RSSI) and local interference. (Common finding: "User is 3 floors away from their router").
  - **Path:** Hop-by-hop latency through the ISP to the Prisma Access Gateway.
- **NSP Exam Tip:** ADEM is unique because it segments latency into "Device," "Wi-Fi," "ISP," and "Cloud." If the "ISP" segment is red, you can prove it's not a firewall issue.

4. User Activity Reporting

To see *what* users are doing (Security):

- **Path:** `Monitor > Logs > Traffic` (or `Explore`).
- **Focus:** Use the **User-ID** column.
  - *Filter:* `source_user eq 'acme\alice'`
- **User Activity Report (UAR):** You can generate a PDF report for HR/Management showing exactly which websites and applications a specific user accessed over the last 30 days.

Summary Checklist for NSP Exam

- **Connectivity Issue:** Check **GlobalProtect Logs** (Auth/Cert errors).
- **Performance Issue:** Check **ADEM** (Wi-Fi/ISP latency).
- **Capacity Issue:** Check **Prisma Access Insights** (License counts/Gateway load).
- **Security Issue:** Check **Traffic Logs** (Blocked apps/Threats).

⁂

Maintain connectivity and security of remote users certificates

For **Network Security Professional (NSP)** candidates, managing certificates for remote users (Prisma Access/GlobalProtect) is distinct from standard firewall certificate management because it involves **two directions of trust**: authenticating the *User to the Cloud* (Client Certs) and authenticating the *Cloud to the User* (Decryption Certs).

1. User Authentication (Client Certificates)

To implement Zero Trust, you often require a "Machine Certificate" in addition to a password/MFA to prove the device is corporate-issued.[177] [178]

- **Configuration Workflow:**
  1. **Certificate Profile:** Create a profile in SCM (`Configuration > Objects > Certificate Profile`) that references your Root CA.
     - *Critical Setting:* Set the "Username Field" to `Subject-Alt` (Email) or `Subject` (CN) so the firewall knows *who* the certificate belongs to.[179]
  2. **Portal/Gateway Auth:** In your GlobalProtect Portal/Gateway Authentication tab, add this Certificate Profile.
  3. **Behavior:** Set "Allow Authentication with User Credentials OR Client Certificate" to **No** (meaning *AND*). This enforces 2-Factor Auth (Password + Certificate).[177]

2. Transparent Decryption (Deploying Root CA)

To inspect SSL traffic from remote users without browser warnings, they must trust your "Forward Trust" certificate.

- **The GlobalProtect "Trojan Horse" Method:**
  - Instead of using GPO/Intune, you can use the GlobalProtect app itself to install the certificate.[180]
  - **Path:** `Configuration > Mobile Users > GlobalProtect > Portal > Agent > Trusted Root CA`.
  - **Action:** Add your Forward Trust Root CA here and check **"Install in Local Root Certificate Store"**.

- **Result:** When the user connects to VPN, the app silently installs the certificate. This is perfect for BYOD or non-domain machines.

3. Certificate Lifecycle Management (SCEP)

Manually installing client certs on 5,000 laptops is impossible. Use **SCEP (Simple Certificate Enrollment Protocol)**.[181]

- **Concept:** The GlobalProtect Portal acts as a middleman. When a user logs in, the Portal asks your internal PKI "Please mint a fresh cert for this user," then pushes it to the app.
- **SCM Config:**
  - Define a SCEP Profile pointing to your CA (e.g., Microsoft NDES).
  - Assign this profile in the **Portal Agent Config**.
  - *Benefit:* Certificates are auto-renewed without admin intervention.

4. Troubleshooting Certificate Errors

Common error: "Required client certificate is not found" or "Server certificate verification failed".[182]

- **Check 1 (Client Side):** Open the GlobalProtect App > Settings > Troubleshooting > Logs. Look for `PanGPS.log`. It will say "Certificate with thumbprint X not found in store".[183]
- **Check 2 (Server Side):** In SCM, check the **System Logs**. If you see "Certificate Valid: No", it means the firewall cannot verify the CRL (Certificate Revocation List). Ensure the firewall/Prisma Access can reach your CRL URL (usually HTTP port 80).

Summary Checklist for NSP Exam

- **Authentication:** Use **Certificate Profiles** to enforce "Machine Auth."
- **Distribution:** Use the **Portal Agent Config** to transparently push Root CAs to endpoints.
- **Automation:** Use **SCEP** for automated client certificate issuance and renewal.
- **Validation:** Ensure your **CRL** is accessible; otherwise, strict validation will fail and block all users.

⁂

1. https://gregjorg.com/posts/prisma-access-network-design-and-planning
2. https://gregjorg.com/posts/prisma-access-planning-and-design
3. https://docs.paloaltonetworks.com/strata-cloud-manager
4. https://www.paloguard.com/strata-cloud-manager.asp
5. https://datacipher.net/palo-alto-networks-netsec-professional-certification-guide/
6. https://datacipher.net/palo-alto-network-security-professional-certification-guide-2025/
7. https://www.youtube.com/watch?v=YgeR0OZF3gY
8. https://www.youtube.com/watch?v=9UGOMhy6wu4

9. https://info.menlosecurity.com/rs/281-OWV-899/images/Menlo-Palo-Alto-Integration-Guide-Prisma-Access-Cloud-Managed.pdf
10. https://www.youtube.com/watch?v=hnYRDyXh8jM
11. https://docs.paloaltonetworks.com/prisma-access
12. https://www.paloaltonetworks.com/services/education/palo-alto-networks-netsec-professional
13. https://www.paloaltonetworks.co.uk/network-security/strata-cloud-manager
14. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-overview/how-to-manage-prisma-access
15. https://www.scribd.com/document/912838016/Strata-Cloud-Manager-Getting-Started
16. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started
17. https://www.youtube.com/watch?v=PH5iGgUqkfg
18. https://www.youtube.com/watch?v=V7u6BXiVljU
19. https://www.scribd.com/document/935794353/Strata-Cloud-Manager-Getting-Started
20. https://pan.dev/scm/docs/home/
21. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-setup/configure-the-prisma-access-service-infrastructure
22. https://www.youtube.com/watch?v=CW7aTIMkpic
23. https://www.youtube.com/watch?v=KVEBpdGZxrc
24. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/overview/get-started
25. https://www.paloaltonetworks.com.br/network-security/strata-cloud-manager
26. https://www.youtube.com/watch?v=ClDQmabhEzc
27. https://techdocs.broadcom.com/gr/el/vmware-sde/velocloud-sase/vmware-velocloud-sd-wan/5-3/palo-alto-networks-strata-cloud-manager-configuration.html
28. https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn/define-cryptographic-profiles/define-ike-crypto-profiles
29. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-ike-crypto
30. https://www.youtube.com/watch?v=pX3e8vlu7hg
31. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PORsCAO
32. https://www.reddit.com/r/Zscaler/comments/1cf0ibu/palo_alto_ipsec_tunnel_configuration/
33. https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn/define-cryptographic-profiles/define-ike-crypto-profiles-prisma-access-cloud-management
34. https://www.reddit.com/r/networking/comments/8l3see/palo_alto_vpn_tunnel_question/
35. https://www.reddit.com/r/paloaltonetworks/comments/xowy37/ikev2_and_ipsec/
36. https://github.com/cdot65/pan-scm-ansible
37. https://summalai.com/?p=4449
38. https://www.analysisman.com/2021/11/ipsec-encryption.html
39. https://www.reddit.com/r/paloaltonetworks/comments/1jvz8ar/current_ike_ipsec_best_practices_for_s2s_vpn/
40. https://palo-alto.fandom.com/wiki/IPsec_VPN

41. https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/set-up-site-to-site-vpn/define-cryptographic-profiles/define-ipsec-crypto-profiles
42. https://www.youtube.com/watch?v=CnAXJ770yHs
43. https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices/zero-trust-best-practices/the-five-step-methodology
44. https://www.youtube.com/watch?v=vU74Sy23qSg
45. https://docs.paloaltonetworks.com/ngfw/getting-started/initial-setup-configuration-ngfws/segment-your-network/configure-interfaces-and-zones
46. https://origin-docs.paloaltonetworks.com/network-security/security-policy/administration/objects/tags/create-and-apply-tags/create-and-apply-tags-cloud-management
47. https://zeronetworks.com/blog/palo-alto-networks-zero-networks-deliver-unified-zero-trust-solution
48. https://www.startupdefense.io/blog/palo-alto-networks-and-zero-networks-integration-how-microsegmentation-and-ngfws-work-together
49. https://www.youtube.com/watch?v=fmxLfukF-Zg
50. https://www.youtube.com/watch?v=gGwFvi8rvqU
51. https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices
52. https://www.reddit.com/r/networking/comments/n2r2me/network_segmentation_with_zero_trust_approach/
53. https://www.paloaltonetworks.co.uk/resources/guides/sase-segmentation-solution-guide
54. https://www.linkedin.com/pulse/zero-trust-architecture-palo-alto-practical-implementation-7sqxc
55. https://www.reddit.com/r/paloaltonetworks/comments/1dcm58c/strata_cloud_manager_zones/
56. https://www.paloaltonetworks.com/resources/guides/sase-segmentation-solution-guide
57. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/system-settings/system-settings-folder-management
58. https://dependencyhell.net/2024/introduction-to-strata-cloud-manager-part-i
59. https://www.mbtechtalker.com/mastering-policy-flexibility-understanding-configuration-scope-in-strata-cloud-manager-scm/
60. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/maintain-security-policy-best-practices
61. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/network-policies/qos
62. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/network-policies/policy-based-forwarding
63. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/policy-optimizer-best-practices
64. https://www.test-inside.com/blog/comprehensive-guide-to-palo-alto-network-security-administrator-certification-excellence/
65. https://www.youtube.com/watch?v=KVEBpdGZxrc
66. https://www.reddit.com/r/paloaltonetworks/comments/1hws13i/scm_folder_and_snippet_structure/
67. https://datacipher.net/palo-alto-network-security-professional-certification-guide-2025/
68. https://www.reddit.com/r/paloaltonetworks/comments/1dtlzqv/inheritance_on_strata_manage_prisma_access_ngfw/

69. https://datacipher.net/palo-alto-networks-netsec-professional-certification-guide/
70. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/workflows/workflows-ngfw-setup/folder-management
71. https://docs.cloud.google.com/resource-manager/docs/organization-policy/understanding-hierarchy
72. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/insights-scm
73. https://www.paloguard.com/strata-cloud-manager.asp
74. https://subscription.packtpub.com/book/web-development/9781801077446/5/ch05lvl1sec29/configuring-cortex-data-lake
75. https://docs.paloaltonetworks.com/network-security/security-policy/administration/objects/log-forwarding/configure-a-log-forwarding-profile-cm
76. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/configure-log-forwarding/configure-log-forwarding-scm
77. https://www.youtube.com/watch?v=wDlg4KtlmPY
78. https://www.reddit.com/r/paloaltonetworks/comments/1mn25nm/strata_cloud_manager_log_viewer_90_days_option/
79. https://www.paloguard.com.au/datasheets/strata-cloud-manager.pdf
80. https://www.prepaway.com/certification/palo-alto-pcnsa-chapter-11-monitoring-and-reporting-part-2/
81. https://www.youtube.com/watch?v=ClDQmabhEzc
82. https://datacipher.net/palo-alto-networks-secops-professional-certification-guide/
83. https://www.youtube.com/watch?v=nuANbdW-n14
84. https://datacipher.net/palo-alto-network-security-professional-certification-guide-2025/
85. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/monitor
86. https://www.youtube.com/watch?v=YgeR0OZF3gY
87. https://docs.paloaltonetworks.com/network-security/decryption/administration/enabling-decryption/configure-ssl-forward-proxy
88. https://ruatelo.com/palo-alto-ssl-inspection/
89. https://www.youtube.com/watch?v=nZsqKe4MqOY
90. https://www.youtube.com/watch?v=i8da6l4o7pM
91. https://live.paloaltonetworks.com/t5/next-generation-firewall/ssl-inspection/td-p/582039
92. https://live.paloaltonetworks.com/t5/vm-series-in-the-private-cloud/deploying-ssl-decryption-cert-using-global-protect-client/td-p/493739
93. https://www.reddit.com/r/paloaltonetworks/comments/1ndboz1/panorama_migration_to_strata_cloud_manager_scm/
94. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/decryption/prepare-to-deploy-decryption/develop-a-pki-rollout-plan
95. https://faatech.be/palo-alto-ssl-forward-proxy-anti-virus/
96. https://docs.paloaltonetworks.com/network-security/decryption/administration/decryption-overview/ssl-forward-proxy
97. https://www.youtube.com/watch?v=WlkjXBG_J08
98. https://www.youtube.com/watch?v=m2-bJfHDocI
99. https://www.youtube.com/watch?v=KVEBpdGZxrc

100. https://www.youtube.com/watch?v=Rp9_Ez7hfXU
101. https://www.youtube.com/watch?v=UuKcjfQicNw
102. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/device-settings/cheat-sheet-global-protect-for-cloud-management-of-ngfws
103. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/manage-configuration-ngfw-and-prisma-access/device-settings/cheat-sheet-global-protect-for-cloud-management-of-ngfws
104. https://docs.paloaltonetworks.com/prisma-access/administration/privileged-remote-access/configure-split-tunneling-for-privileged-remote-access-traffic
105. https://docs.paloaltonetworks.com/globalprotect/administration/host-information/host-information-profile-hip-in-security-policy-enforcement/configure-hip-based-policy-enforcement
106. https://paloaltofirewallconfiguration.blogspot.com/2019/04/global-protect-and-hip-configuration-we.html
107. https://www.youtube.com/watch?v=GlXkEVdJlZo
108. https://www.paloaltonetworks.com/blog/sase/prisma-sase-adem-simplify-network-troubleshooting-for-the-hybrid-workforce/
109. https://www.reddit.com/r/paloaltonetworks/comments/1j0i2uk/prisma_access_cloud_globalprotect_authentication/
110. https://www.youtube.com/watch?v=Dj-rjuX9I_E
111. https://www.reddit.com/r/paloaltonetworks/comments/q28×97/globalprotectprisma_access_different_agent/
112. https://www.youtube.com/watch?v=2VES4GECQdc
113. https://www.youtube.com/watch?v=9j2cuT0snWY
114. https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-quick-configs/globalprotect-for-internal-hip-checking-and-user-based-access
115. https://www.reddit.com/r/paloaltonetworks/comments/buu6mk/globalprotect_remote_users_network_conflicts_with/
116. https://www.youtube.com/watch?v=A3b8u8RkUhM
117. https://docs.paloaltonetworks.com/whats-new/new-features/november-2024/privileged-remote-access
118. https://docs.paloaltonetworks.com/prisma-access/administration/privileged-remote-access/set-up-privileged-remote-access-profiles
119. https://docs.paloaltonetworks.com/prisma-access-browser
120. https://live.paloaltonetworks.com/t5/community-blogs/prisma-access-4-0-adds-explicit-proxy-support-to-globalprotect/ba-p/543150
121. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-explicit-proxy/agent-based-proxy-globalprotect-proxy-mode
122. https://datacipher.net/palo-alto-network-security-professional-certification-guide-2025/
123. https://www.reddit.com/r/paloaltonetworks/comments/u3f6pv/rdp_to_clientless_vpn_through_prisma/
124. https://datacipher.net/palo-alto-networks-netsec-professional-certification-guide/
125. https://www.pomerium.com/blog/palo-alto-clientless-vpn
126. https://www.youtube.com/watch?v=PH5iGgUqkfg

127. https://www.reddit.com/r/paloaltonetworks/comments/ykrj4o/globalprotect_vs_prisma_access_mobil_users_and/
128. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/configure-clientless-vpn-prisma-access
129. https://www.reddit.com/r/paloaltonetworks/comments/1hxh4fo/anyone_using_prisma_access_browser_how_is_your/
130. https://www.reddit.com/r/paloaltonetworks/comments/fu0b4m/global_protect_vs_prisma_access/
131. https://www.youtube.com/watch?v=6B5eRknlxNo
132. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-user-based-policy/retrieve-user-id-information
133. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/zone-protection-and-dos-protection/network-segmentation-using-zones
134. https://www.reddit.com/r/paloaltonetworks/comments/x8dng9/is_there_a_way_to_assign_a_user_connecting_to/
135. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/ip-address-pools-for-a-globalprotect-mobile-users-deployment
136. 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
137. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/service-connection-advanced-deployments/use-traffic-forwarding-rules-with-service-connections/traffic-steering
138. https://www.youtube.com/watch?v=vU74Sy23qSg
139. https://www.youtube.com/watch?v=n8h592fuZqA
140. https://www.youtube.com/watch?v=QYy-5XTUlCo
141. https://www.youtube.com/watch?v=ezOOZP7xQic
142. https://www.reddit.com/r/paloaltonetworks/comments/1kcb9xl/prisma_access_userid_issue/
143. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/configuration-scm/manage-configuration-ngfw-and-prisma-access/device-settings/cheat-sheet-global-protect-for-cloud-management-of-ngfws
144. https://docs.paloaltonetworks.com/best-practices
145. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/userid-to-usergroup-mapping
146. https://www.reddit.com/r/paloaltonetworks/comments/qrk66w/prisma_access_user_id_redistribution_possibility/
147. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/policy-optimizer-best-practices
148. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/security-policy-rule-optimization
149. https://www.reddit.com/r/paloaltonetworks/comments/wzv295/is_it_okay_to_reset_rule_hit_count_for/
150. https://www.youtube.com/watch?v=z9GUTxHCFXk
151. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000LCkoCAG
152. https://www.youtube.com/watch?v=HfGVUjV8kWQ
153. https://www.youtube.com/watch?v=w7wI0Q64Tno

154. https://docs.paloaltonetworks.com/cloud-ngfw-aws/administration/protect/strata-cloud-manager-policy-management
155. https://www.reddit.com/r/paloaltonetworks/comments/10nj7wd/prisma_access_explicit_proxy_authentication_issues/
156. https://www.youtube.com/watch?v=kIOMbtLJg-E
157. https://www.youtube.com/watch?v=h7fzNyWzAxs
158. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices
159. https://www.youtube.com/watch?v=c2d6FWnYRfQ
160. https://xsoar.pan.dev/docs/reference/packs/policy-optimizer
161. https://www.youtube.com/watch?v=PH5iGgUqkfg
162. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-globalprotect/monitor-globalprotect-mobile-users
163. https://www.youtube.com/watch?v=0-80tNMxcpA
164. https://www.youtube.com/watch?v=Ik1rXsVdxI4
165. https://www.youtube.com/watch?v=YjnO8d9-wHI
166. https://docs.paloaltonetworks.com/autonomous-dem/china-administration/first-look-at-adem-in-pa/remote-sites-dashboard
167. https://www.thenetworkdna.com/2025/10/prisma-sase-enable-adem.html
168. https://live.paloaltonetworks.com/t5/general-topics/globalprotect-amp-sccm/td-p/333928
169. https://www.reddit.com/r/paloaltonetworks/comments/1c7ymh5/prisma_with_strata_cloud_manager_and_syslog/
170. https://www.reddit.com/r/paloaltonetworks/comments/ftrd55/investigating_globalprotect_connectivity/
171. https://xsoar.pan.dev/docs/reference/integrations/prisma-access
172. https://www.reddit.com/r/paloaltonetworks/comments/jcwqmm/global_protect_ip_pool_logs/
173. https://www.youtube.com/watch?v=9CkpAO3DQbs
174. https://thwack.solarwinds.com/discussion/104663/strata-cloud-manger-monitoring
175. https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/monitor
176. https://www.reddit.com/r/paloaltonetworks/comments/x4pt88/globalprotect_logs_forwarded_to_panorama_are_only/
177. https://blog.reversethrottle.com/palo-alto-networks/globalprotect-deployment/globalprotect-client-certificate-authentication
178. https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-certificate-profile
179. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/enable-mobile-users-to-authenticate-to-prisma-access
180. https://live.paloaltonetworks.com/t5/vm-series-in-the-private-cloud/deploying-ssl-decryption-cert-using-global-protect-client/td-p/493739
181. https://blog.reversethrottle.com/palo-alto-networks/globalprotect-deployment
182. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClkBCAS
183. https://www.reddit.com/r/paloaltonetworks/comments/w8mu6l/globalprotect_certificate_issue/
184. https://www.youtube.com/watch?v=fmxLfukF-Zg

185. https://www.youtube.com/watch?v=gGwFvi8rvqU
186. https://www.youtube.com/watch?v=hldjFFxzZhc
187. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000g1tPCAQ&lang=en_US
188. https://www.nwexam.com/blog/ultimate-guide-palo-alto-certification-path
189. https://www.youtube.com/watch?v=QYy-5XTUlCo
190. https://docs.paloaltonetworks.com/prisma-access/administration/ztna-connector-in-prisma-access/ztna-connector-requirements-and-guidelines/certificate-management
191. https://www.youtube.com/watch?v=qeLSaDqROak