perplexity

Application Layer inspection for strata and sase products

Palo Alto Networks utilizes a **Single Pass Parallel Processing (SP3)** architecture to perform application-layer (Layer 7) inspection across both **Strata** (NGFW) and **Prisma SASE** (Prisma Access) products.

This approach ensures that traffic is inspected for application identity (App-ID), content threats (Content-ID), and policy compliance in a single processing stream, minimizing latency.

1. Single Pass Parallel Processing (SP3) Architecture

The core differentiator for Palo Alto Networks is that inspection operations happen effectively "once" per packet, rather than in daisy-chained serial processes used by legacy UTMs.

Feature	**Strata (NGFW Hardware)**	**Prisma SASE (Cloud-Delivered)**
Software Architecture	**Single Pass Software:** Performs networking, policy lookup, App-ID, and Content-ID in one pass.	**Single Pass Software:** Runs the same core PAN-OS security stack in cloud-native containers.
Hardware/Compute	**Parallel Processing Hardware:** Uses dedicated ASICs/FPGAs to offload networking, content scanning, and management tasks.	**Cloud-Scale Compute:** Elastic "Security Processing Nodes" scale dynamically to handle compute-intensive inspection without customer hardware sizing.
Dataplane	Local physical dataplane (fast path/slow path on-box).	Cloud-delivered dataplane (traffic tunnels to PoP).

2. App-ID: The Foundation of Layer 7 Inspection

App-ID is the first critical step in inspection. It classifies traffic based on the *application identity* rather than the port (e.g., identifying "Facebook-base" vs. "Facebook-chat" on TCP/443).

The 4-Stage Identification Process:

1. **Application Signatures:** The engine looks for unique protocol signatures in the packet stream to identify the application immediately.
2. **SSL/TLS Decryption:** If the traffic is encrypted and matches a decryption policy, the firewall decrypts the flow. **App-ID is then re-applied** to the decrypted stream to identify the inner application.[1] [2]
3. **Protocol Decoders:** If an application is tunneling inside another (e.g., Gmail inside HTTP), decoders parse the outer protocol to expose the inner application context.[2] [3]

4. **Heuristics:** For evasive or unknown applications that lack standard signatures, the system uses behavioral analysis to identify the traffic.[2]

3. Content-ID: Deep Packet Inspection (DPI)

Once App-ID classifies the traffic and a Security Policy **allows** it, the traffic undergoes Content-ID inspection for threats. This happens in the same "single pass."

- **Threat Prevention (IPS/Vulnerability):** Scans for exploit attempts (buffer overflows, SQL injection) against the identified application.
- **Anti-Virus / Anti-Spyware:** Stream-based scanning for malware payloads and C2 (Command & Control) traffic.
- **URL Filtering:** Classifies web requests (including those inside SSL) to block malicious or non-compliant categories.
- **Data Filtering (DLP):** Inspects for sensitive patterns (Credit Card #, SSN) or file properties (Real-Time decoding of file types).

Advanced Threat Prevention (ATP) & Inline Deep Learning

In modern Strata (PAN-OS 10.2+) and Prisma SASE deployments, **Advanced Threat Prevention** adds an **Inline Deep Learning** engine.

- **Mechanism:** It analyzes live traffic patterns in real-time (not just static signatures) to detect zero-day C2 and evasive malware.[4] [5]
- **Strata vs SASE:**
  - **Strata:** High-end appliances (e.g., PA-5400) can perform *Local Deep Learning* on-box. Other models may rely on cloud-based inline analysis.[6]
  - **Prisma SASE:** Natively uses cloud-scale compute for Inline Deep Learning without performance degradation.

4. Decryption: The Key Enabler

Layer 7 inspection is blind to encrypted traffic without decryption.

- **Strata:** Relies on hardware offloading (dedicated crypto hardware) to handle the heavy CPU load of SSL Forward Proxy. Performance varies by model.
- **Prisma SASE:** Decryption is handled by the cloud node. This is advantageous because the "performance penalty" of decryption is absorbed by the cloud provider's scalable infrastructure rather than a fixed-capacity appliance.[7]

Exam Notes: Key Differentiators & Terminology

> **For Certification (PCNSE / NET-SEC Pro):**
>
> - **Sequence: App-ID** always happens *before* **Content-ID**. You cannot inspect the content for threats until you know *what* the application is.
> - **Implicit Dependency:** If you use an **Application Override** policy, you **bypass** App-ID and Content-ID (Deep Inspection) for that traffic. It essentially turns the NGFW into a L4 firewall for that flow.[8]
> - **Encrypted Traffic:** Without a decryption policy, App-ID can only identify applications based on the **Server Name Indication (SNI)** and certificate Common Name (CN), which is less granular and prone to spoofing.
> - **Management:** While Strata is often managed by **Panorama**, Prisma SASE is increasingly managed by **Strata Cloud Manager (SCM)**, which unifies policy across both form factors.[9] [10]

Summary Comparison Table

Inspection Layer	Strata (NGFW)	SASE (Prisma Access)
Classification	**App-ID** (Local Database + Updates)	**App-ID** (Cloud Database + Instant Updates)
Threat Engine	**Content-ID** (IPS/AV/Spyware)	**Content-ID** (IPS/AV/Spyware)
Zero-Day Logic	**WildFire** (Sandboxing) + **ATP** (Inline Deep Learning - Hardware dependent)	**WildFire** + **ATP** (Inline Deep Learning - Cloud Native)
Throughput	Limited by **Appliance Datasheet** (verify "Threat Prevention" throughput)	Limited by **License/Bandwidth Tier** (elastic scale)

⁂

ips

In the Palo Alto Networks ecosystem, **Intrusion Prevention (IPS)** is not a standalone module. It is primarily delivered through **Content-ID** using two key Security Profiles: **Vulnerability Protection** and **Anti-Spyware**.

1. The Core Components of "IPS"

To enable full IPS functionality, you must attach both of these profiles to your Security Policy rules.

- **Vulnerability Protection Profile:** Focuses on **Exploits**.
    - **Target:** System flaws, buffer overflows, code execution vulnerabilities, and SQL injection.
    - **Function:** It stops attacks from *entering* your network or moving laterally between zones.

    - **Mechanism:** Uses signature-based detection on the application payload (after App-ID has classified it).[31] [32]
- **Anti-Spyware Profile:** Focuses on **C2 (Command & Control)**.
    - **Target:** Infected hosts attempting to "phone home," beaconing, and botnet traffic.
    - **Function:** It stops malware from *communicating out* of your network.
    - **Mechanism:** Detects C2 traffic patterns (even inside SSL if decrypted) and blocks access to malicious domains via DNS signatures.[33] [34]

> **Exam Tip:** If a question asks about "preventing exploits against a web server," use **Vulnerability Protection**. If it asks about "detecting infected hosts beaconing out," use **Anti-Spyware**.

2. Advanced Threat Prevention (ATP) & Deep Learning

Modern IPS in Strata and SASE has evolved beyond static signatures into **Advanced Threat Prevention (ATP)**.

- **Inline Deep Learning:** Instead of waiting for a signature update, the firewall (or SASE cloud node) analyzes live traffic streams using deep learning models to block **zero-day** attacks in real-time.
- **Key Capabilities:**
    - **SQL/Command Injection:** Detects unknown injection attacks by analyzing the syntax of the traffic inline.[35] [36]
    - **Evasive C2:** Identifies "malleable" C2 (like Cobalt Strike) that changes its signature frequently to evade traditional IPS.[37] [35]

3. Critical Configuration Concepts

When configuring these profiles, understanding the **Action** and **Exceptions** is critical for both real-world operations and exams.

Actions

- **Default:** Uses the action recommended by Palo Alto Networks researchers for that specific threat.
- **Strict:** Automatically upgrades the action for Critical, High, and Medium severity threats to **Block**, regardless of the default.[33]
- **Block IP:** Blocks the *source* or *destination* IP for a set duration (e.g., 3600 seconds). This is a "nuclear" option—use with caution as it can block legitimate traffic from the same IP.[38]

Exceptions vs. IP Exemptions (Crucial Distinction)

There is a common trap in how exceptions are configured:

- **Signature Exception:** You change the action for a specific signature (e.g., Threat ID 12345) from *Block* to *Alert* for **all** traffic matching the profile.
- **IP Address Exemption:** You add an IP address to the "IP Address Exemptions" column of a signature exception.
    - **The Trap:** The modified action (e.g., *Alert*) applies **ONLY** to the IPs listed. All *other* traffic continues to use the original action (e.g., *Block*).[39] [40]
    - *Common Misconception:* Users often think the IP list is "exempt from the block." In reality, the IP list "receives the exception action," while everyone else gets the standard profile action.

4. Strata vs. SASE Implementation

Feature	Strata (NGFW)	SASE (Prisma Access)
Throughput	Dependent on **Hardware Datasheet** (Threat Prevention throughput).	Elastic/Cloud-Native (scales with license).
ATP Compute	High-end models (PA-5400+) run Deep Learning **on-box**. Smaller models may rely on cloud assist.	Runs natively in the cloud for all traffic.
Management	Managed via **Panorama** or local UI.	Managed via **Strata Cloud Manager (SCM)** or Panorama.

Summary for Study Notes

- **IPS = Vulnerability Protection + Anti-Spyware.**
- **Vulnerability Protection** = Stops **Exploits** (Inbound/Lateral).
- **Anti-Spyware** = Stops **C2/Beacons** (Outbound).
- **ATP** = Adds **Inline Deep Learning** for zero-day Injection/C2.
- **IP Exemption Logic:** The IP gets the *exception action*; everyone else gets the *profile action*.

⁂

slow path and fast path for packet inspection

In Palo Alto Networks architecture (PAN-OS), the distinction between **Slow Path** and **Fast Path** refers to how the firewall processes packets based on whether a session already exists.

The firewall does not inspect every packet from scratch. Instead, it expends heavy resources on the *first* packet to establish a "contract" (session), allowing subsequent packets to flow through an optimized path.

1. Slow Path (Session Setup)

The **Slow Path** is the processing route for the **first packet** of a new connection (typically a TCP SYN). It is "slow" because the firewall must perform all the logical lookups to decide if the connection is allowed.

- **Trigger:** Packet arrives, and **Flow Lookup** finds **no existing session** match.
- **Key Operations:**
  - **Forwarding Lookup:** Determines the destination interface and zone.
  - **NAT Policy Lookup:** Checks if Network Address Translation is required.
  - **Security Policy Lookup:** Checks the "pre-NAT" and "post-NAT" zones/IPs against the rulebase to see if the traffic is allowed.
  - **Session Creation:** If allowed, the firewall allocates a **Session ID**, creates an entry in the session table, and installs "flow keys" (6-tuple hash) for fast lookup.
- **Outcome:** The packet is forwarded, and the session state moves to the Fast Path.

2. Fast Path (Session Processing)

The **Fast Path** handles all **subsequent packets** for an established session. Since the "allowed" decision was already made in the Slow Path, these packets skip the policy/routing lookups and go directly to processing.

- **Trigger:** Packet arrives, and **Flow Lookup** finds a **matching Session ID**.
- **Key Operations:**
  - **TCP/Network Processing:** Validates sequence numbers and checksums.
  - **NAT/Decryption:** Applies the translation or decryption defined during setup.
  - **App-ID (Layer 7):** The "Single Pass" software scans the payload to identify the application (e.g., identifying `facebook-base` inside `ssl`).
  - **Content-ID (Layer 7):** If the session is actively being inspected, the stream is scanned for threats (IPS, Virus, Spyware) in this path.
- **Performance:** This runs on the Dataplane CPU cores (MIPS/Cavium) and is highly optimized using the **Single Pass Parallel Processing (SP3)** architecture.

3. Hardware Offload (The "Fastest" Path)

There is a third state called **Offload**. Once the firewall determines that a session no longer needs deep software inspection (App-ID is final and no Content-ID is required), it "offloads" the session to dedicated hardware (FPGA or Flow Engine).

- **Trigger:** App-ID is identified + No Content-ID is needed (or traffic is encrypted/trusted and not being decrypted).
- **Mechanism:** The session keys are pushed to the hardware chip.

- **Result:** Packets move from Ingress Chip → Offload Chip → Egress Chip. They **never touch the main CPU**, resulting in near wire-speed throughput and zero CPU load.
- **Visual Indicator:** In the CLI (`show session id <id>`), you will see `offload=yes`.

Summary Comparison Table

Feature	**Slow Path**	**Fast Path**	**Offload**
Packet Type	First Packet (New Flow)	Subsequent Packets (Established)	Trusted/Encrypted Packets
Primary Task	**Policy & Route Lookup**	**App-ID & Content Inspection**	**Pure Forwarding**
Component	Dataplane CPU (Control Logic)	Dataplane CPU (SP3 Software)	FPGA / Flow Engine (Hardware)
Latency	High (Setup Overhead)	Medium (Inspection Overhead)	Lowest (Wire Speed)
CLI State	`state: opening`	`state: active`	`offload: yes`

⁂

decryption on Strata and SASE

Decryption (SSL/TLS inspection) is the most critical configuration for effective Layer 7 inspection on both platforms, but the *enforcement point* and *management scale* differ.

The fundamental concept is identical: **App-ID** identifies the traffic as SSL/TLS, and a **Decryption Policy** intercepts the handshake to inspect the inner payload.

1. Architectural & Implementation Differences

Feature	**Strata (NGFW Hardware)**	**Prisma SASE (Cloud-Delivered)**
Enforcement Point	**On-Box:** Decryption happens on the local appliance. Performance is tied to the hardware model's specific "SSL Decrypt" throughput.	**Cloud Node:** Decryption happens in the cloud PoP. Performance scales elastically without you managing the hardware "ceiling."
Certificate Mgmt	**Manual/HSM:** You generate/import the Forward Trust CA manually. Distribution to clients via GPO/MDM is entirely your responsibility.	**Cloud PKI / Default:** Can use a "Palo Alto Networks" default CA (rapid PoC) or import your Enterprise CA via Cloud Management.
Resource Impact	**High CPU Load:** Decryption is computationally expensive. Enabling it on an undersized box can spike Dataplane CPU and latency.	**Offloaded:** The compute burden is absorbed by the cloud provider's infrastructure, removing the "should I decrypt?" performance fear.
Proxy Modes	Supports **Forward Proxy** (outbound), **Inbound Inspection** (internal servers), and **SSH Proxy**.	Primarily **Forward Proxy** (outbound). **Inbound Inspection** is supported but less common (traffic must route *in* through the cloud to your servers).

2. Supported Decryption Modes

- **SSL Forward Proxy (Outbound):**
  - *Scenario:* Users accessing the Internet (e.g., stopping malware download from HTTPS site).
  - *Mechanism:* The firewall acts as a "Man-in-the-Middle" (MitM). It presents a generated certificate (signed by your **Forward Trust CA**) to the client. The client *must* trust this CA, or they get browser warnings.
  - *Strata & SASE:* Both support this fully.
- **SSL Inbound Inspection (Inbound):**
  - *Scenario:* External users accessing *your* internal DMZ web server.
  - *Mechanism:* You import the **real server certificate + private key** onto the firewall. The firewall passively decrypts traffic without proxying or modifying the certificate.
  - *Key Constraint:* Perfect Forward Secrecy (PFS) ciphers (e.g., DHE, ECDHE) prevent passive decryption. If your server uses PFS, you generally cannot use Inbound Inspection; you must use **SSL Forward Proxy** (targeting the server) or terminate SSL on a load balancer.
- **SSH Proxy:**
  - *Scenario:* Inspecting SSH tunnels to ensure they aren't hiding other apps.
  - *Note:* SSH Proxy is **not supported** in Strata Cloud Manager (SCM) as of late 2025/early 2026, though supported in Panorama-managed NGFWs.[61]

3. Decryption Policy & Profiles (Exam Critical)

- **Decryption Policy (The "Who"):** Matches traffic to decrypt (Source Zone, User, URL Category).
  - *Best Practice:* Do NOT decrypt "Financial/Health" categories (legal privacy) or "Pinned Certificate" sites (technical breakage).
  - *pinned-certificate-exceptions:* A predefined list of sites (like Windows Update, Apple iCloud) that break if decrypted.
- **Decryption Profile (The "How"):** Controls the security of the decrypted session.
  - **Unsupported Modes:** Action to take if the site uses old TLS (1.0/1.1) or weak ciphers. (Block/Strip).
  - **Failure Checks:** If the firewall cannot decrypt (e.g., HSM down, resource limit), do you **Fail Open** (allow traffic) or **Fail Close** (drop it)?
  - **TLS 1.3:** Both platforms support TLS 1.3 inspection. However, TLS 1.3 *enforces* Perfect Forward Secrecy, so passive **Inbound Inspection** is impossible for TLS 1.3 traffic (must use Proxy mode).[62]

4. Special SASE Feature: Explicit Proxy / Cloud SWG

Prisma Access offers an **Explicit Proxy** (SWG) mode where users point their browser proxy settings to the cloud (PAC file) rather than using a VPN agent.

- **Decryption:** Handled similarly, but you must ensure the "Forward Trust CA" is installed on the endpoint.
- **Authentication:** Explicit Proxy requires specific authentication flows (often "Cookie-based" or "IP-based") to map the user for policy before decryption can occur.[63] [64]

Summary Checklist

- **Strata:** Watch your hardware sizing. Use Hardware Security Modules (HSM) for high-volume key storage.
- **Prisma SASE:** Use the cloud scalability. Easier certificate management via SCM.
- **Both:** Avoid decrypting Finance/Health. Beware of TLS 1.3 + Inbound Inspection (PFS issue).
- **Golden Rule: "Decrypt Known, Bypass Unknown."** (Only decrypt traffic you strictly need to inspect, or you risk breaking applications).

⁂

network hardening methods for enhanced security on strata and sase

Network hardening on Palo Alto Networks Strata and SASE involves securing not just the device's management plane, but also the "dataplane" (traffic processing) to prevent abuse, reconnaissance, and Denial-of-Service (DoS) attacks.

The following methods target the **Network/Dataplane** specifically, distinct from general "device administration" hardening.

1. Management Plane Hardening (Network Layer)

Even before touching the traffic policies, you must lock down how the device itself is accessed on the network.

- **Dedicated Management Interface:** Always use the dedicated MGT port (out-of-band). Never mix management traffic with data traffic unless absolutely necessary.
- **Permitted IP Lists:**
  - **Strata (NGFW):** Configure "Permitted IP Addresses" in `Device > Setup > Management`. This restricts *which* IPs can even reach the login page or SSH service.
  - **Interface Management Profiles:** If you *must* manage a firewall via a dataplane interface (e.g., inside a branch), attach a strict **Interface Management Profile** that permits only HTTPS/SSH and **restricts source IPs** to your admin subnets.[76] [77]

- **Prisma Access:**
  - **IP Restrictions:** In Cloud Management, configure "IP Restrictions" to limit access to the Prisma Access console/API to only your corporate public IPs.[78]

2. Zone Protection Profiles (The "Shield")

Zone Protection Profiles are your first line of defense against flood and reconnaissance attacks. They apply **before** the security policy lookup (pre-session), saving resources.

- **Flood Protection:** Set thresholds (CPS - Connections Per Second) for SYN, UDP, and ICMP floods.
  - *Action:* Use "SYN Cookies" (activation threshold) rather than "Drop" to protect legitimate users during a spoofed attack.[79] [80]
- **Reconnaissance Protection:** Enable detection for TCP Port Scans and Host Sweeps to identify internal infected hosts trying to map your network.
  - *Best Practice:* Set the action to **Block** (not just Alert) for internal zones to stop lateral movement attempts.
- **Packet Based Attacks:** Drop malformed packets, "IP fragments," and "TCP non-SYN first" packets (unless using asymmetric routing) to prevent bypass techniques.

3. DoS Protection Policies (Granular Defense)

While Zone Protection protects the *zone/aggregate*, DoS Protection Policies protect specific *critical assets* (e.g., a web server or database).

- **Classified vs. Aggregate:**
  - **Aggregate:** Limits the *total* CPS to a server from *everyone* combined (good for protecting server hardware limits).
  - **Classified:** Limits the CPS *per source IP*. This is critical for stopping a single infected host from overwhelming a server while letting others connect.[81] [79]
- **Hardening Tip:** Apply a "Classified" DoS policy to your public-facing VIPs to prevent one user from exhausting your session table.

4. SASE (Prisma Access) Specific Hardening

Since the infrastructure is cloud-managed, hardening focuses on "who can enter" and "who can leave."

- **Source IP Allow-Listing:**
  - Prisma Access uses dynamic public IPs for egress. To harden SaaS apps (like Salesforce/O365) to *only* accept your users, you must automate the retrieval of Prisma Access egress IPs (via API) and update your SaaS allow-lists.[82] [83]
- **Service Connection Security:**

    - Treat the "Service Connection" (link to your DC) as a **Trusted but Verified** zone. Do not allow "Any/Any" from the cloud to your DC.
    - Harden the BGP peering on Service Connections using MD5 auth to prevent route injection.
- **GlobalProtect Hardening:**
    - **HIP Checks (Host Information Profile):** Enforce that endpoints must have encryption, AV, and patches *before* allowed full access.
    - **Split Tunneling:** "No split tunneling" is most secure, but if split tunneling is needed, use "Exclude Video/High Bandwidth" rather than "Allow only Corp".

5. Routing & Interface Hardening

- **Passive Interfaces:** On Layer 2 deployments, ensure interfaces are in "Virtual Wire" or "Layer 2" mode with strict VLAN filtering to prevent VLAN hopping.
- **Bogon Blocking:** Create a top-down security rule blocking "Bogon" (reserved/private) IP ranges on your *Internet* zone ingress to prevent spoofing.
- **Zone Isolation:** Ensure no rule allows traffic from `Untrust` to `Trust` without strict application + threat inspection (never "Any Application").

Summary Checklist

Area	Feature	Hardening Action
Mgmt	**Permitted IPs**	Restrict Admin Login to IT Subnets only.
Flood	**Zone Protection**	Enable SYN Cookies and Reconnaissance Block on all zones.
Server	**DoS Policy**	Apply "Classified" profile (limit per Source IP) to VIPs.
SASE	**Egress IP**	Automate API fetch of Prisma IPs to lock down SaaS apps.
Routing	**Bogons**	Block RFC1918/Reserved IPs entering from the Internet.

⁂

1. https://media.paloaltonetworks.com/documents/App_ID_tech.pdf
2. https://www.paloguard.com/App-ID.asp
3. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClloPCAS
4. https://www.paloaltonetworks.com/network-security/advanced-threat-prevention
5. https://www.brighttalk.com/resource/core/394058/next-gen-security-services-with-inline-ai-inference---transcript_846530.pdf
6. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/configure-inline-cloud-analysis
7. https://docs.paloaltonetworks.com/prisma-access/administration
8. https://docs.paloaltonetworks.com/ngfw/administration/app-id/app-id-overview

9. https://www.linkedin.com/pulse/when-strata-cloud-manager-scm-replace-panorama-complex-joe-brunner-bpyhe
10. https://docs.paloaltonetworks.com/compatibility-matrix/reference/feature-parity
11. https://www.paloaltonetworks.com/resources/whitepapers/single-pass-parallel-processing-architecture
12. https://www.paloguard.com/sp3-architecture.asp
13. https://www.firewall.cx/security/palo-alto-networks/palo-alto-firewall-single-pass-parallel-processing-hardware-architecture.html
14. https://www.paloaltonetworks.com/resources/whitepapers/single-pass-parallel-processing-architecture.viewer.html
15. https://media.paloaltonetworks.com/documents/Single_Pass_Parallel_Processing_Architecture.pdf
16. https://www.youtube.com/watch?v=eA-hpo2_uss
17. https://www.youtube.com/watch?v=7Q5cFmm9Xak
18. https://www.youtube.com/watch?v=xe5Cs7rpDno
19. https://www.cliffsnotes.com/study-notes/5881819
20. https://docs.paloaltonetworks.com/prisma-sd-wan/ion-cli-reference/use-cli-commands/inspect-commands/inspect-flow-detail
21. https://www.linkedin.com/pulse/firewallcx-benefits-palo-alto-networks-firewall-pass-sp3-partsenidis
22. https://docs.paloaltonetworks.com/advanced-threat-prevention
23. https://www.cc.com.pl/pl/prods/paloaltonetworks/pdf/advanced-threat-prevention.pdf
24. https://www.paloaltonetworks.sg/resources/videos/how-to-stop-sophisticated-attacks-using-inline-deep-learning-protection-thai
25. https://www.youtube.com/watch?v=5_FnO7eq1iA
26. https://docs.paloaltonetworks.com/content/techdocs/en_US/saas-security/saas-security-inline/manage-saas-security-inline-policy/app-id-cloud-engine
27. https://www.youtube.com/watch?v=YgeR0OZF3gY
28. https://www.reddit.com/r/paloaltonetworks/comments/p64cgz/strata_vs_prisma_what_did_you_opt_for_and_why/
29. https://www.firewalls.com/palo-alto-networks-pa-1420-advanced-threat-3-years-36-months-term.html
30. https://www.reddit.com/r/paloaltonetworks/comments/1bnfo33/strata_cloud_manager_vs_panorama/
31. https://www.reddit.com/r/paloaltonetworks/comments/w80hwz/anti_virus_policy_vs_spyware_policy_vs/
32. https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Palo-Alto-Networks-whitepaper-STRATA-ips-as-platform.pdf
33. https://docs.paloaltonetworks.com/network-security/security-policy/administration/security-profiles/security-profile-anti-spyware
34. https://www.reddit.com/r/networking/comments/w80h4x/av_policy_vs_spyware_policy_vs_vulnerability/
35. https://www.paloaltonetworks.com/resources/datasheets/advanced-threat-prevention
36. https://www.cc.com.pl/pl/prods/paloaltonetworks/pdf/advanced-threat-prevention.pdf
37. https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/674464005510460
38. https://www.techtarget.com/searchsecurity/feature/How-to-set-up-Palo-Alto-security-profiles
39. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UscCAE

40. https://www.reddit.com/r/paloaltonetworks/comments/xk46wa/vulnerability_signature_exceptions_and_the_ip/
41. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/set-up-antivirus-anti-spyware-and-vulnerability-protection
42. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/take-packet-captures/take-a-custom-packet-capture
43. https://docs.paloaltonetworks.com/ngfw/administration/monitoring/take-packet-captures/take-application-packet-capture
44. https://www.youtube.com/watch?v=HMfBfB0PT-c
45. https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/create-threat-exceptions
46. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClWFCA0
47. https://www.reddit.com/r/Cisco/comments/11pkkh2/software_vs_hardware_processing_for_network/
48. https://portal.nutanix.com/page/documents/details?targetId=AHV-Admin-Guide-v10_3%3Aahv-sriov-no-slow-fast-path-process-ahv-c.html
49. https://stackoverflow.com/questions/68947219/what-is-fast-path-slow-path-hot-path
50. https://www.paloaltonetworks.com/cyberpedia/hardware-firewall-vs-software-firewall
51. https://www.youtube.com/watch?v=Xj7C4qsBf9Q
52. https://www.facebook.com/groups/435258026591146/posts/25695698973453703/
53. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0
54. https://www.youtube.com/shorts/dtfogEaXr3M
55. https://www.scribd.com/document/354027526/Differences-Between-Packets-in-Slow-Path-Fast-Pat
56. https://threatfiltering.com/packet-flow-and-order-of-operations-in-pan-os/
57. https://www.linkedin.com/posts/rajesh-dotaniya-569590a2_paloaltotrobuleshooting-slowpath-fastpath-activity-7365227994946207746-2dRM
58. https://codilime.com/blog/hardware-offloading-sdn/
59. https://www.reddit.com/r/paloaltonetworks/comments/1f3aioj/packet_flow_in_pa_fw/
60. https://www.youtube.com/watch?v=b_rNzkuV-O8
61. https://docs.paloaltonetworks.com/network-security/decryption/administration/decryption-overview/decryption-policy-rules
62. https://docs.paloaltonetworks.com/content/techdocs/en_US/network-security/decryption/administration/decryption-overview/tls-1-3-ssl-decryption
63. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-mobile-users/mobile-users-explicit-proxy/set-up-explicit-proxy
64. https://www.reddit.com/r/paloaltonetworks/comments/10nj7wd/prisma_access_explicit_proxy_authentication_issues/
65. https://docs.paloaltonetworks.com/whats-new/new-features/november-2023/tlsv1-3-support-for-administrative-access-using-ssl-tls-service-profiles
66. https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/decryption/prepare-to-deploy-decryption
67. https://live.paloaltonetworks.com/t5/general-topics/ssl-inspection-issues-with-globalprotect-users/td-p/584535

68. https://www.packtpub.com/en-pt/product/implementing-palo-alto-networks-prisma-access-9781835081006/chapter/chapter-7-securing-web-gateway-9/section/configuring-the-explicit-proxy-ch09lvl1sec41
69. https://www.reddit.com/r/paloaltonetworks/comments/1gwlfvi/understanding_palo_altos_product_tiers/
70. https://docs.taegis.secureworks.com/integration/connectCloud/palo_alto_prisma_access/
71. https://docs.paloaltonetworks.com/network-security/security-policy/administration/all-policy-types
72. https://www.reddit.com/r/paloaltonetworks/comments/p64cgz/strata_vs_prisma_what_did_you_opt_for_and_why/
73. https://live.paloaltonetworks.com/t5/general-topics/strata-prisma-amp-cortex-difference/td-p/543040
74. https://www.reddit.com/r/paloaltonetworks/comments/1osdznp/please_help_me_decode_palo_altos_portfolio_strata/
75. https://docs.paloaltonetworks.com/compatibility-matrix/reference/prisma-access
76. https://www.packtpub.com/en-GR/product/mastering-palo-alto-networks-9781803241418/chapter/setting-up-a-new-device-2/section/hardening-the-management-interface-ch02lvl1sec13
77. https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/configure-interfaces/use-interface-management-profiles-to-restrict-access
78. https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-setup/set-up-prisma-access
79. https://live.paloaltonetworks.com/t5/general-topics/when-to-use-zoneprofile-and-dos-profile/td-p/233035
80. https://www.packtpub.com/en-IN/product/mastering-palo-alto-networks-9781803241418/chapter/advanced-protection-11/section/zone-protection-and-dos-protection-ch11lvl1sec78
81. https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClW6CAK
82. https://www.reddit.com/r/paloaltonetworks/comments/167106p/prisma_access_internet_outbreak/
83. https://www.youtube.com/watch?v=QYy-5XTUICo
84. https://www.reddit.com/r/paloaltonetworks/comments/i0nqtg/whats_your_opinion_of_palos_dos_protections_in/
85. https://www.youtube.com/watch?v=2iAsJUJT4Iw
86. https://berkeley.service-now.com/kb_view.do?sys_kb_id=a3cfc9c41bfd1590f2430ed6624bcbc0&sysparm_class_name=kb_knowledge
87. https://docs.paloaltonetworks.com/best-practices/security-policy-best-practices/security-policy-best-practices/deploy-security-policy-best-practices/security-policy-rule-best-practices
88. https://docs.paloaltonetworks.com/best-practices
89. https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices
90. https://docs.paloaltonetworks.com/ngfw/administration/zone-protection-and-dos-protection