Platform & Sizing

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

CONTEXT DRIVES ENFORCEMENT

- **App-ID** — Application
- **User-ID** — User
- **Device-ID** — Device
- **Policy** — Enforce

01 NGFW architecture and solution design

Application visibility and policy

- **App-ID** identifies applications through protocol decoding, signatures and heuristics, including applications using nonstandard ports. A port number alone does not establish application identity.
- **Security policy** combines zones, addresses, users, applications and services. Rules are evaluated in order; the first matching rule applies. App-ID augments network controls rather than opening every port.
- **application-default** restricts permitted applications to their defined default ports. Use explicit services when a justified application deployment needs other ports, and account for application dependencies.
- Default **interzone** policy denies traffic; default **intrazone** policy allows it. Define explicit segmentation rules and logging for the required trust boundaries.

Single-pass processing

- **Single Pass Architecture (SPA)** combines classification, policy and content inspection while avoiding repeated decoding and separate scans for each security function. **SP3** pairs this software approach with parallel processing hardware.
- The **stream-based signature engine** checks decoded traffic for multiple threat and content patterns. Networking, security and content processing have distinct responsibilities; management functions use the management plane.
- A packet matching an established **session** uses the fast path for session handling. Required content inspection still runs; fast-path processing does not mean the session bypasses security.
- Single-pass processing reduces duplicated work when services are enabled. Validate the intended feature mix and encrypted workload during sizing; an architecture benefit is not an unlimited-capacity guarantee.

Sizing and business outcomes

- Size for **threat-prevention throughput**, concurrent sessions, new connections per second, interfaces and growth. Raw firewall throughput alone is insufficient for an inspected workload.
- Include **TLS decryption**, packet and application mix, VPN traffic, logging, session duration and failover load. The surviving HA peer must handle the required production demand.

Platform & Sizing / Threat Prevention

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

CONTEXT DRIVES ENFORCEMENT

- **App-ID** — Application
- **User-ID** — User
- **Device-ID** — Device
- **Policy** — Enforce

- Use the **Product Comparison tool** and relevant datasheets to shortlist firewalls. Validate the shortlist with representative traffic and enabled protections during a proof of concept.
- Position the platform around **visibility, prevention and operational efficiency**: consistent application and identity controls, shared intelligence, consolidated management and faster response. Tie each benefit to measurable customer requirements.

Zero Trust and the protect surface

- **Zero Trust** removes implicit trust based on network location. Authenticate users, assess devices, permit only required applications and inspect activity throughout access.
- Define the **protect surface** by identifying critical **data, applications, assets and services (DAAS)**. Classify sensitivity and business importance before selecting controls.
- The five-step sequence is **define the protect surface**, **map transaction flows**, **architect the network**, **create policy**, then **monitor and maintain**. Transaction flows establish required communication; policy specifies permitted access.
- **User-ID** supplies user context, **Device-ID** supplies device context and **App-ID** supplies application context. Combine these signals with segmentation and least privilege to reduce lateral movement.

02 Threat prevention and cloud-delivered services

Choose the enforcement control

- **Antivirus** detects malicious content; **Anti-Spyware** detects spyware and command-and-control traffic; **Vulnerability Protection** detects exploit attempts and supported brute-force patterns.
- **File Blocking** controls transfers by recognized file type, application and direction. It can restrict risky downloads while general web browsing remains allowed.
- Attach **Security profiles** or a profile group to the allow rules that carry the traffic. A configured profile provides no inspection unless the matching traffic uses it.
- **Zone Protection** applies to an ingress zone and addresses reconnaissance, floods and packet-based attacks. **DoS Protection** can protect selected resources; these controls have different scopes from content profiles.
- Keep **dynamic content updates** automatic and frequent enough for the protection objective. Monitor installation success and subscription health; distinguish update availability from the configured download-and-install schedule.

Threat Prevention

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

LAYER THE PREVENTION CONTROLS

- **WildFire** — Unknown files
- **Threat profiles** — Exploits & C2
- **URL Filtering** — Web access
- **DNS Security** — Domains

Command-and-control and rate detection

- For **C2** signatures, select prevention actions such as drop or the appropriate reset action. **Alert** records detection without blocking; **allow** permits traffic. Understand the selected signature action rather than relying on a profile name.
- **Brute-force signatures** in Vulnerability Protection detect repeated attempts against supported services. Apply the profile to the relevant allowed traffic and keep content current.
- **Custom combination signatures** can trigger on a frequency threshold within a time window. Define the event, count, interval and tracking scope carefully; this is distinct from general log correlation.
- Layer controls across **delivery, exploitation, C2, lateral movement and exfiltration**. A blocked download, a sinkholed domain and a restricted application interrupt different parts of an attack.

WildFire analysis and deployment

- **WildFire** analyzes unknown files and supported links, produces verdicts and distributes protections. It complements exploit prevention by detecting malicious content that lacks an existing signature.
- A **WildFire Analysis profile** selects files for submission and the analysis destination. **Antivirus** applies file protections; submission for analysis and inline prevention are separate decisions.
- **Public cloud** analysis uses the shared analysis service. **Private cloud** keeps submitted samples within the private deployment. **Hybrid** designs select destinations by file or policy requirements.
- Subscription features include broader **file-type analysis**, API capabilities and faster protection delivery than basic submission capabilities. File formats, size limits and private-appliance support must match the deployed capabilities.
- Relevant formats include **PE**, **ELF**, documents, archives, macOS files and scripts. Treat supported formats and configured maximum sizes separately; a recognized format is not automatically eligible for every submission path.
- Supported **HTTP and HTTPS links** extracted from email can be submitted for analysis. Recognize **benign**, **malicious**, **grayware** and link-related **phishing** verdict concepts; response depends on the object and verdict.

Inline machine learning and validation

- **WildFire inline ML** evaluates supported content on the firewall to prevent unknown malicious files during transfer. It complements cloud analysis rather than removing the need for it.
- Configure applicable inline ML models and actions in the **Antivirus profile**, then attach that profile to the relevant Security rules. Model support varies by file type and platform.

Threat Prevention

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

LAYER THE PREVENTION CONTROLS

- **WildFire** — Unknown files
- **Threat profiles** — Exploits & C2
- **URL Filtering** — Web access
- **DNS Security** — Domains

- **show mlav cloud-status** checks connectivity to the inline ML service. A connected status establishes service reachability, not proof that a particular download was inspected or blocked.
- During validation, confirm the **matched rule**, attached profile, enabled model and action. Inspect **Threat logs** for inline ML detections, including the **ml-virus** threat type, and use a suitable approved test sample.

DNS Security and sinkholing

- **DNS Security** detects malicious domains, including threats using **domain generation algorithms (DGAs)**. Category actions can address malware, C2 and other risky domain classes.
- In the PAN-OS configuration model using **Anti-Spyware DNS policies**, enable the DNS service and apply the profile to allowed DNS traffic. DNS inspection, URL filtering and file analysis inspect different objects.
- **Sinkholing** replaces a malicious DNS answer with a controlled sinkhole address. The client connects toward that address instead of the malicious destination; subsequent **Traffic logs** help identify the originating host behind an internal resolver.
- A sinkhole does not become the client's DNS resolver or automatically repair the endpoint. Correlate the domain detection with the source host and follow an incident-response workflow.
- If the **cloud verdict lookup times out**, DNS Security passes the request and responses without that cloud inspection. Monitor service latency and connectivity; a timeout is not a permanent allow decision for the domain.

Web access, phishing and exceptions

- **Advanced URL Filtering** classifies web destinations and uses real-time analysis against malicious pages and phishing. It is especially relevant to users browsing the web, while server protection also needs application and exploit controls.
- **URL Filtering profiles** control categories, credential submission and logging. **Safe Search enforcement** limits supported search results; it serves a different purpose from blocking malware or C2 categories.
- Use a narrow **custom URL category** or the appropriate inline-analysis exception for a validated false positive. Preserve protections for other sites, and verify which engine generated the block.
- When **uncategorized** sites must remain accessible, add layered controls such as File Blocking, threat inspection and a suitable **continue** action. User acknowledgment does not establish that a site is safe.
- **HTTP header logging** can capture fields such as **X-Forwarded-For**, User-Agent and Referer. Encrypted HTTP requires visibility into the decrypted traffic; handle logged identity and browsing data carefully.

Identity & TLS

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

IDENTITY AND INSPECTION

Identify User & device → **Authenticate** Validate access → **Decrypt** Inspect TLS → **Authorize** Least privilege

03 Identity, credentials and encrypted traffic

User-ID and cloud identity

- **IP-to-user mapping** associates network sessions with users. **Group mapping** retrieves user membership so policy can target directory groups; these are separate functions.
- Mapping sources include **directory server monitoring**, GlobalProtect, Authentication Portal and supported syslog or API integrations. Evaluate source reliability, shared IP addresses and mapping timeouts.
- Enable **User-ID** on appropriate trusted zones, restrict included and excluded networks, and use a dedicated account with minimum required permissions. Avoid broad probing and mapping collection from untrusted networks.
- **Cloud Identity Engine Directory Sync** supplies directory user and group information. Its **Cloud Authentication Service** authenticates through supported **SAML 2.0 IdPs**; directory synchronization and authentication solve different needs.

Tags and automatic access changes

- **Dynamic User Groups (DUGs)** select users through tag expressions. Policies can restrict risky users or grant temporary access while retaining user identity in logs.
- Add or remove **user-to-tag mappings** through supported firewall or Panorama interfaces and the XML API. Use mapping expiration and automation to remove temporary contractor access when the approved period ends.
- **Dynamic Address Groups (DAGs)** select IP-address members through tags, including tags supplied by virtual infrastructure and automation. They follow workload addresses rather than user accounts.
- **External Dynamic Lists (EDLs)** retrieve external lists of IP addresses, domains or URLs for supported policy uses. They do not replace a dynamic user group or an identity directory.

Corporate credential protection

- **Credential phishing prevention** detects corporate credential submission to restricted web categories. Configure detection in a **URL Filtering profile** and apply it to the web allow rules; decrypt applicable HTTPS to inspect submissions.
- **Group Mapping** checks submitted usernames against directory membership. **IP-User Mapping** checks the username against the session's IP-to-user mapping. These methods detect usernames rather than verifying corporate passwords.

Identity & TLS / Network & HA

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

IDENTITY AND INSPECTION

Identify User & device → **Authenticate** Validate access → **Decrypt** Inspect TLS → **Authorize** Least privilege

- **Domain Credential Filter** checks username-and-password submissions using a Bloom filter supplied by the **Windows User-ID agent credential service**, together with IP-to-user mapping. Protect the supporting identity infrastructure.
- **MFA** limits abuse of a stolen password. Combine it with phishing prevention, threat analysis and least privilege; detecting a phishing page and challenging an authentication attempt are complementary controls.

TLS inspection and certificate roles

- **SSL Forward Proxy** inspects outbound client TLS by creating separate client-to-firewall and firewall-to-server connections. Managed clients must trust the CA used for substitute server certificates.
- The **Forward Trust** certificate signs substitute certificates for trusted destinations. **Forward Untrust** marks untrusted server certificates so clients receive an appropriate warning; avoid making that certificate a trusted client root.
- The forward-proxy signing CA can be **enterprise CA-signed** or **self-signed** with its trust distributed to clients. Certificate authority, signing key and client trust are separate configuration requirements.
- **SSL Inbound Inspection** requires the protected server's certificate and corresponding private key for supported TLS sessions. It serves inbound applications rather than impersonating arbitrary internet servers.
- Plan **decryption exclusions** for privacy requirements and incompatible traffic such as certificate pinning or unsupported mutual authentication. Roll out in stages, test applications and size for encrypted throughput.
- **Decryption Broker / Network Packet Broker** capabilities can send inspected or decrypted traffic to third-party security tools on supported deployments. Decrypting once can reduce duplicate decryption across the inspection chain.

04 Deployment, routing and resilience

Interfaces and routing decisions

- **Tap mode** observes a SPAN or mirror feed for assessment and visibility; it cannot enforce inline blocking. **Virtual wire** inserts inspection transparently without requiring routed IP addressing on its paired interfaces.
- **Layer 2** interfaces switch traffic within VLANs; **Layer 3** interfaces participate in routing. A routed **VLAN interface** and a **loopback interface** can belong to a virtual router; a Layer 2 port is not itself a routed interface.
- Routing uses **longest-prefix match** first. For the same prefix, **administrative distance** ranks route sources, then applicable **metrics** rank routes within the routing protocol or route type.
- **Policy-Based Forwarding (PBF)** can steer selected flows outside the normal route choice. Design both directions of stateful traffic and verify the failover behavior of any path-monitoring policy.

Network & HA

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

RESILIENCE HAS SEPARATE LAYERS

- **HA1** — Control
- **HA2** — State sync
- **HA3** — Active/active packets
- **SD-WAN** — Path quality

High availability and split brain

- **Active/passive HA** has one traffic-processing peer and a standby. **Active/active HA** allows both peers to process traffic and supports designs with asymmetric forwarding when session handling is configured correctly.
- **HA1** carries control, hello messages and configuration synchronization. **HA2** synchronizes session and other runtime state. **HA3** forwards packets between peers in active/active deployments.
- **Split brain** occurs when peers lose control communication and both believe they should be active. Provide an independent **HA1 backup** and supported **heartbeat backup**; test control-link failure scenarios.
- Use **link and path monitoring** to detect failures beyond the local device. Preemption controls return to a preferred active peer; it does not replace reliable HA control connectivity.
- Keep both directions of a session visible to the inspection design. **Non-SYN first-packet** handling is an advanced accommodation for some asymmetric cases, with reduced validation; evaluate the security trade-off before enabling it.

WAN paths and remote access

- **SD-WAN** selects paths using application requirements and link quality such as latency, jitter and packet loss. Multiple WAN links provide path redundancy; an HA pair addresses firewall failure.
- Troubleshoot SD-WAN using **policy-to-interface selection**, path-monitor measurements, event history and session distribution. A healthy physical link can still fail an application quality threshold.
- **GlobalProtect** extends firewall policy to remote users. **Prisma Access** delivers cloud-based security for mobile users and remote networks; **service connections** provide access to private data-center resources.
- Place **service connections** near private resources and user traffic as appropriate. Multiple connections require deliberate route advertisements, symmetric return paths and adequate capacity; geographic placement can change the traffic path.
- **Explicit Proxy** supports web access through a configured proxy, including **PAC files** that select proxy handling. It is a web access deployment choice, while remote-access tunnels cover broader network connectivity.
- **Prisma Cloud** addresses cloud application and workload security. Keep that role distinct from Panorama management, NGFW enforcement and Prisma Access connectivity.

Management & POC

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

FROM REQUIREMENT TO EVIDENCE

- **Assess** — Requirements
- → **Configure** — Policy & profiles
- → **Validate** — Logs & health
- → **Close** — Sanitize equipment

05 Panorama, assessments and proof of concept

Central management and scale

- **Panorama device groups** organize policies and objects. **Templates and template stacks** organize device and network settings. Separate policy inheritance from platform configuration.
- A **commit to Panorama** saves the management configuration; a **push** deploys selected configuration to managed devices. Validate changes and review local overrides and inheritance before pushing.
- **Panorama Interconnect** coordinates management across multiple Panorama servers in large deployments. Size management and logging separately using device count, configuration scale, log rate and query requirements.
- **Zero Touch Provisioning (ZTP)** automates initial firewall onboarding to Panorama through a bootstrap workflow. Plan network reachability, device registration and the intended templates and device groups.
- **Master keys** protect locally stored secrets. Panorama management does not imply that every device shares the same master key; safeguard recorded keys and configuration backups as separate operational tasks.

Logs, correlation and device health

- **Threat logs** show detections and actions; **Traffic logs** show sessions, users, applications and endpoints. **WildFire submissions** add sample verdicts and reports. Correlate sources when identifying a compromised host.
- The **Automated Correlation Engine** combines related log events into higher-level findings. **Botnet reports** highlight suspicious behavior such as malicious destinations and dynamic DNS use; investigate the evidence before concluding compromise.
- **Custom report queries** combine an **attribute**, **operator** and value, joined with logical **connectors**. Choose the appropriate log database; report scheduling and recipients are separate settings.
- **Detailed Device Health** includes **Sessions**, **Interfaces** and **Environmentals** views for applicable hardware. Use session count and throughput, interface errors and drops, and environmental conditions to isolate resource problems.
- **Deviating Devices** identifies metrics outside the expected operating range. Panorama derives baselines from **seven-day averages and standard deviation**; a deviation is a diagnostic signal, not automatically a security incident.
- Size log retention from **logs per second**, average stored log size, retention days, overhead and redundancy. Compare log collectors and cloud logging capacity using a sizing calculator; firewall throughput does not establish storage sufficiency.

Management & POC

Palo Alto Networks System Engineer Professional - Strata

KNOWLEDGE CHEATSHEET

FROM REQUIREMENT TO EVIDENCE

Assess Requirements → **Configure** Policy & profiles → **Validate** Logs & health → **Close** Sanitize equipment

Assess, demonstrate and close out

- **Best Practice Assessment (BPA)** evaluates configuration and feature adoption, including application and user controls, profiles, decryption and management hardening. It differs from a traffic-based **Security Lifecycle Review (SLR)**.
- **Threat-intelligence context** helps determine whether malware is widespread or concentrated in a sector or organization. Tools such as **AutoFocus** organize samples and related activity; a single malware verdict does not prove targeting.
- **Migration planning** maps imported rules to required applications and removes excessive access. Recognize **Expedition** as a migration and policy-conversion tool associated with this workflow; review generated rules before deployment.
- Before a **proof of concept**, define success criteria, reset reused evaluation equipment, select suitable software and updates, and arrange SPAN access for a tap deployment. Agree on the sensitive information that reports may expose.
- Demonstrate **application visibility**, threat actions, identity, decryption and sizing against agreed requirements. Verify matched rules and relevant logs rather than treating a successful download or cloud connection as the complete result.
- At closeout, **clear customer data, logs and configuration** from evaluation equipment using the approved reset procedure. **request system private-data-reset** is the PAN-OS private-data reset command; this is an equipment handoff action.