

GSW SYSTEMS

Palo Alto Firewall Audit Checklist

A practical starting point for auditing Palo Alto Networks firewalls

A firewall audit should be systematic. The goal is not simply to find configuration settings that differ from a vendor recommendation, but to understand what the firewall actually allows and whether that behaviour matches the organization's intended security model. Use this checklist as a starting point for a Palo Alto firewall security review.

1. Scope and preparation

- ☐ Confirm the firewalls and virtual systems in scope.
- ☐ Confirm whether Panorama is in scope.
- ☐ Identify the PAN-OS versions being assessed.
- ☐ Record the configuration collection date.
- ☐ Establish the period represented by traffic and hit counters.
- ☐ Identify applicable security and compliance requirements.
- ☐ Establish the rules of engagement.
- ☐ Protect configuration exports and audit evidence.
- ☐ Record tools and versions used during the assessment.

2. Security policy

- ☐ Inventory security rules.
- ☐ Identify broad source or destination scopes.
- ☐ Identify rules using "any" unnecessarily.
- ☐ Identify rules allowing excessive applications or services.
- ☐ Identify shadowed rules.
- ☐ Identify duplicate or redundant rules.
- ☐ Identify disabled rules.
- ☐ Identify stale or unused rules.
- ☐ Review temporary and expiring rules.
- ☐ Confirm important rules have appropriate logging.
- ☐ Review security profile coverage.

- ☐ Review internet-facing allow rules particularly closely.

3. Effective access

- ☐ Build an effective zone-to-zone access model.
- ☐ Account for rule evaluation order.
- ☐ Expand address and service objects.
- ☐ Identify unrestricted paths.
- ☐ Identify paths into sensitive zones.
- ☐ Identify unexpected internal paths.
- ☐ Review paths from untrusted zones.
- ☐ Consider Panorama pre-rules, local rules and post-rules.
- ☐ Validate important paths against the actual configuration.

4. Application and service controls

- ☐ Identify rules using application "any".
- ☐ Identify port-based rules.
- ☐ Review use of application-default.
- ☐ Review custom service objects.
- ☐ Confirm non-standard ports are justified.
- ☐ Identify applications observed on broad rules.
- ☐ Review application overrides.

5. NAT

- ☐ Inventory NAT rules.
- ☐ Review rule ordering.
- ☐ Identify whole-host exposure.
- ☐ Identify orphaned NAT rules.
- ☐ Identify overlapping NAT rules.
- ☐ Cross-reference NAT and security policy.
- ☐ Review internal NAT.
- ☐ Review unrestricted outbound source NAT.
- ☐ Review stale proxy ARP.

- ☐ Review NAT in Panorama-managed environments.

6. Threat prevention

- ☐ Review vulnerability protection.
- ☐ Review anti-spyware and DNS protections.
- ☐ Review antivirus.
- ☐ Review URL filtering.
- ☐ Review file blocking.
- ☐ Review WildFire.
- ☐ Review data filtering where applicable.
- ☐ Identify profiles operating in alert-only mode.
- ☐ Review threat exceptions.
- ☐ Confirm subscriptions are current.
- ☐ Confirm content updates are current.
- ☐ Review zone protection.
- ☐ Review DoS protection for exposed services.

7. Management plane

- ☐ Map the dedicated management interface.
- ☐ Review permitted management source addresses.
- ☐ Review enabled management services.
- ☐ Identify insecure services such as Telnet or HTTP.
- ☐ Inventory interface management profiles.
- ☐ Identify data-plane interfaces accepting management traffic.
- ☐ Review Panorama access.
- ☐ Review API access.
- ☐ Review automation accounts.
- ☐ Review administrator roles.
- ☐ Review authentication.
- ☐ Review local accounts.
- ☐ Review protection of configuration secrets.

8. SSL/TLS decryption

- ☐ Identify decryption types in use.
- ☐ Measure actual decryption coverage where possible.
- ☐ Review decryption policy ordering.
- ☐ Review broad no-decrypt rules.
- ☐ Review custom exclusions.
- ☐ Confirm exclusions are justified.
- ☐ Confirm privacy-sensitive exclusions are deliberate.
- ☐ Review certificate protection.
- ☐ Review forward trust and forward untrust certificates.
- ☐ Review inbound inspection keys.
- ☐ Review access to decrypted data.

9. Logging and monitoring

- ☐ Confirm security logging is enabled where required.
- ☐ Review administrative logging.
- ☐ Review forwarding and retention.
- ☐ Confirm logs are actually arriving at their destination.
- ☐ Confirm timestamps and time synchronisation.
- ☐ Review whether important events can be investigated.

10. High availability and lifecycle

- ☐ Confirm HA mode.
- ☐ Review HA monitoring.
- ☐ Compare configuration between peers.
- ☐ Compare PAN-OS versions.
- ☐ Compare content and licence status.
- ☐ Confirm failover testing.
- ☐ Confirm backups.
- ☐ Confirm restore testing.
- ☐ Review PAN-OS lifecycle status.
- ☐ Review hardware lifecycle.

- ☐ Review expiring licences and certificates.

11. Compliance and reporting

- ☐ Identify applicable frameworks.
- ☐ Record framework versions.
- ☐ Map findings to controls.
- ☐ Distinguish firewall evidence from organization-level evidence.
- ☐ Record exceptions.
- ☐ Validate automated compliance results.
- ☐ Write findings with evidence.
- ☐ Provide specific and verifiable recommendations.
- ☐ Protect the completed audit report.

A checklist is useful for consistency, but a mature audit needs effective-access analysis, evidence and judgement. Read the complete methodology in *Auditing Palo Alto Firewalls: A Practitioner's Guide to PAN-OS Security Reviews* by Gordon Smith, or automate the mechanical analysis with Rampart. — www.gswsystems.com