SAMPLE REPORT — generated with the same engine as your live audit — auditxa.com

AuditXA — Palo Alto PA-3220 Security Report

File: pa3220-running-config.xml · Generated: 5 Jun 2025, 14:30 · Score: 59/100 (F)

59
/ 100

Palo Alto PA-3220 — Grade F

Analysed 30 controls against NSA, CIS, and vendor best practices · Palo Alto PA-3220 (PAN-OS 11.1.2)

Generated: 5 Jun 2025, 14:30

1 Critical | 2 High | 5 Medium | 22 Passed

AUDIT SUMMARY

RESULTS BY CATEGORY · WEAKEST FIRST

Authentication	0%	0/2 passed
WildFire	0%	0/2 passed
DNS Security	0%	0/1 passed
HA	0%	0/1 passed
Management	71%	5/7 passed
Policies	100%	3/3 passed
Threat Prevention	100%	2/2 passed
URL Filtering	100%	1/1 passed
Decryption	100%	3/3 passed
Logging	100%	1/1 passed
Updates	100%	2/2 passed
Zone Protection	100%	4/4 passed

Geo-Blocking		100%	1/1 passed

MFA configured for admin login

CRITICAL Authentication

Multi-factor authentication is required for all PAN-OS administrative access.

```
set mgt-config users admin mfa-enable yes
```

PAN-OS Hardening – Admin MFA

WildFire analysis profile applied to security rules

HIGH WildFire

WildFire is your last line of defence against unknown malware and zero-days. Without a WildFire profile attached to security rules, suspicious files are allowed without sandbox analysis.

```
set profiles wildfire-analysis <name> rules any application any file-type
any direction both analysis public-cloud
```

AuditXA Hardening Checklist

DNS Security enabled on Anti-Spyware profile

HIGH DNS Security

DNS Security blocks C2 callbacks and malware downloads at the DNS layer — before any connection is established. It is one of the highest-ROI controls available on PAN-OS.

```
set profiles spyware <name> dns-security dns-security-categories malware
action sinkhole
```

AuditXA Hardening Checklist

SAML/RADIUS authentication profile defined

MEDIUM Authentication

Centralised identity integration via SAML or RADIUS enables SSO, MFA, and auditing.

```
set authentication-profile SAML-Auth method saml idp-profile <profile>
```

PAN-OS Authentication Profile Guide

Certificate-based HTTPS for management

MEDIUM Management

A custom TLS service profile with a valid internal CA certificate should secure the management UI.

```
set deviceconfig system ssl-tls-service-profile <profile>
```

PAN-OS TLS Management Best Practices

WildFire real-time analysis enabled

MEDIUM WildFire

Real-time WildFire analysis reduces verdict time from 5 minutes to under 1 second for known file hashes, dramatically reducing exposure window.

```
set deviceconfig setting wildfire file-size-limit real-time enable yes
```

AuditXA Hardening Checklist

High Availability configured or documented exception

MEDIUM HA

A single firewall with no HA is a single point of failure for your entire network. Configure active-passive HA or document the exception with business justification.

```
set deviceconfig high-availability enabled yes
```

AuditXA Hardening Checklist

Panorama management server configured

MEDIUM Management

Without Panorama, firewall configuration changes have no centralised audit trail, no version control and no policy consistency enforcement across devices.

```
set deviceconfig system panorama-server <panorama-ip>
```

AuditXA Hardening Checklist

Restrict management to permitted-ip list

OK Management

Management plane must only accept connections from a dedicated OOB management subnet.

```
set deviceconfig system permitted-ip <mgmt-subnet>
```

PAN-OS Admin Guide – Management Interface Security

Disable Telnet and HTTP on management interface

OK Management

Telnet and HTTP transmit credentials in cleartext. Only SSH and HTTPS should be enabled — both must be explicitly disabled, not just one.

```
set deviceconfig system service disable-telnet yes
set deviceconfig system service disable-http yes
```

CIS PAN-OS Benchmark – 1.1.1

Admin account lockout after failed attempts

OK Management

Account lockout prevents brute-force attacks on the management interface.

```
set mgt-config users admin failed-attempts 5
set mgt-config users admin lockout-time 30
```

PAN-OS Security Baseline – Section 2

No any/any/any allow rules

OK Policies

Catch-all allow rules negate App-ID and expose the network to all applications. Note: an attribute PAN-OS lets you omit (from/to/source/destination/application) defaults to any, so a rule can be any/any/any without ever spelling out the word "any" for every field.

```
Replace any/any/any with App-ID based least-privilege rules per zone pair.
```

PAN-OS Best Practices – Security Policy Design

Implicit deny rule has logging enabled

OK Policies

The implicit deny must log dropped traffic to enable threat detection and forensics.

```
set rulebase security rules DenyAll action deny log-end yes log-setting
<profile>
```

Palo Alto BPA – Policy Recommendations

Threat Prevention profile on all internet rules

OK Threat Prevention

Vulnerability protection, AV, and WildFire profiles must be attached to internet-bound rules.

```
set rulebase security rules <n> profile-setting group <security-group>
```

PANW Best Practices – Security Profile Groups

DNS Security / Anti-Spyware sinkhole configured

OK Threat Prevention

DNS Security blocks C2 callbacks and DGA domains in real time.

```
set profiles spyware <n> botnet-domains action sinkhole
set profiles spyware <n> dns-security enabled yes
```

PANW DNS Security Deployment Guide

URL Filtering blocks high-risk categories

OK URL Filtering

Malware, phishing, and C2 URL categories must be blocked at minimum.

```
set profiles url-filtering <n> action block categories [malware phishing
command-and-control]
```

PAN-OS URL Filtering Best Practices

SSL/TLS decryption policy configured

OK Decryption

Without SSL decryption ~80% of threats are invisible.

```
set rulebase decryption rules DecryptOutbound action decrypt
set rulebase decryption rules DecryptOutbound type ssl-forward-proxy
```

PAN-OS Decryption Best Practices

TLS minimum version 1.2 enforced

OK Decryption

TLS 1.0 and 1.1 have known vulnerabilities (POODLE, BEAST). Minimum TLS 1.2.

```
set ssl-decryption min-version TLSv1-2
```

NIST SP 800-52r2 – TLS Guidance

Syslog or Panorama forwarding configured

OK Logging

All traffic, threat, and system logs must be forwarded to a centralised SIEM or Panorama.

```
set deviceconfig system panorama-server <ip>
set shared log-settings syslog <n> server <ip>
```

PAN-OS Logging Best Practices

Auto content update schedule configured

OK Updates

AV/threat signatures and App-ID updates should refresh automatically at least daily.

```
set deviceconfig system update-schedule av recurring daily at 04:00
```

PANW Content Update Best Practices

Zone protection profile applied to all zones

OK Zone Protection

Without zone protection profiles, zones are vulnerable to reconnaissance scans, DoS floods and packet-based attacks. Apply a zone protection profile to every zone.

```
set zone <name> network zone-protection-profile <profile>
```

AuditXA Hardening Checklist

Intrazone blocking enabled on untrust zone

OK Zone Protection

Intrazone traffic is permitted by default on Palo Alto. Hosts in the untrust zone can communicate laterally without hitting security policy — enable intrazone blocking on untrust.

```
set zone untrust enable-intrazone yes
```

AuditXA Hardening Checklist

Decryption exclusions list reviewed and restricted

OK Decryption

Overly broad decryption exclusions silently punch holes in your SSL inspection policy. Every exclusion should be documented and justified.

```
Review and document all SSL decryption exclusions. Remove any not strictly
required.
```

AuditXA Hardening Checklist

Threat content updates within 24 hours

OK Updates

Threat content older than 24 hours misses new malware signatures. Configure automatic recurring downloads and installs for anti-virus and threat content.

```
set deviceconfig system update-schedule threats recurring every-30-mins
action download-and-install
```

AuditXA Hardening Checklist

Service objects used — no application-default overrides to any

OK Policies

Using service:any on allow rules bypasses App-ID enforcement and allows traffic on non-standard ports, defeating the purpose of next-generation firewall policy.

```
Replace service any on allow rules with application-default or specific port
objects.
```

AuditXA Hardening Checklist

Embargo and sanctioned countries blocked (OFAC/EU)

OK Geo-Blocking

Traffic from OFAC-sanctioned and EU-embargoed countries (Cuba, Iran, North Korea, Russia, Syria and others) should be blocked inbound at the perimeter. Many compliance frameworks (PCI-DSS, HIPAA, ITAR) require this. Configure geo-based block rules or use an EDL with embargo country codes.

```
set rulebase security rules BlockEmbargo from untrust to any source [ AF CN
CU IR KP RU SY ] action deny log-end yes
# Or use an External Dynamic List with country codes
```

AuditXA Hardening Checklist

Zone protection profile applied to outside/untrust interface

OK Zone Protection

A zone protection profile on the outside/untrust zone is the first line of defence against flood attacks, port scans and packet-based exploits before traffic hits any security policy. Without it your firewall is directly exposed to internet-scale attacks with no flood thresholds or scan detection.

```
set zone untrust network zone-protection-profile ZP-Outside
# ZP-Outside should include: SYN flood, ICMP flood, UDP flood,
reconnaissance protection, packet-based attack protection
```

AuditXA Hardening Checklist

Reconnaissance protection enabled on outside zone protection profile

OK Zone Protection

Without reconnaissance protection enabled in the zone protection profile, attackers can freely port-scan and host-sweep your network perimeter without triggering any alert or block. Enable TCP port scan, UDP port scan, host sweep and SYN-FIN detection with block-ip action.

```
set profiles zone-protection ZP-Outside scan-white-list
set profiles zone-protection ZP-Outside recon-protection syn-fin action
block-ip duration 300
set profiles zone-protection ZP-Outside recon-protection tcp-fin-scan action
block-ip duration 300
```

AuditXA Hardening Checklist

Management interface permitted-ip locked to specific admin hosts

OK Management

A permitted-ip configured as a broad subnet (e.g. 10.0.0.0) or missing entirely leaves the management interface reachable from too many hosts. Restrict to specific administrator IP addresses (/32) or a dedicated management VLAN with the narrowest possible prefix.

```
set deviceconfig system permitted-ip <specific-admin-ip-or-/32>
# Remove any broad subnets — use /32 host entries or a narrow /29 management
subnet only
```

AuditXA Hardening Checklist

Data-plane interfaces deny SSH/HTTPS/Telnet — no management profile on external interfaces

OK Management

Data-plane interfaces facing the internet must never allow SSH, HTTPS or Telnet in their interface management profile. These services on external interfaces expose your firewall to brute-force,

exploitation and credential-stuffing from the entire internet. Only the dedicated management interface (MGT port) should allow admin access, locked to permitted-ip addresses. An interface management profile on external interfaces should allow ping only if ICMP monitoring is required, and nothing else.

```
set network interface-management-profile External-Facing
  set https no
  set ssh no
  set telnet no
  set ping yes   ← only if needed
# Apply this profile to all internet-facing/untrust zone interfaces
set network interface ethernet1/1 layer3 interface-management-profile
External-Facing
```

AuditXA Hardening Checklist