SecureLAN Consulting Services, Inc.

CIS Firewall Assessment

Audit Report

Firewall: DEMO-PA-440

Assessment Date: March 29, 2026

Prepared by: SecureLAN Consulting

Table of Contents

Rule Analysis — Findings & Recommendations

Executive Findings

The firewall rule compliance score of 11.1% represents a critically deficient posture across the 45 rules analysed on device DEMO-PA-440 (PA-440, PAN-OS 11.2.4). One rule was classified as Critical risk and one as High risk, while the remaining 43 rules carry Low risk ratings. However, the pervasive presence of overly permissive configurations across the rule base — including unrestricted destination and service definitions — significantly elevates the aggregate exposure of the organisation.

The dominant risk factors identified include the use of ANY for both destination and service fields, the absence of logging configurations, and the lack of security profile attachments on multiple rules. Remote access service rules were also found without logging or security profiles, presenting an elevated threat vector for undetected lateral movement or data exfiltration. VPN reduction techniques were applied to several rules, masking the true scope of permissiveness.

The absence of logging on a substantial proportion of rules means that security events traversing these policies are not recorded, severely undermining the organisation's ability to detect, investigate, and respond to incidents. Immediate remediation of Critical and High risk rules, combined with a systematic review of ALL-scoped service and destination definitions, is strongly recommended to restore an acceptable security baseline.

Remediation Recommendations

Priority	Action Item	Risk	Recommended Action
Critical	**Restrict Critical-Risk Permissive Rules**	The single Critical-rated rule permits unrestricted destination and service access without logging or security profiles, creating an unmonitored and broadly exploitable attack surface.	Immediately review and restrict the Critical-rated rule by replacing ANY destination and service definitions with explicit, least-privilege values. Attach appropriate security profiles and enable session-end logging as an urgent priority.
High	**Remediate High-Risk Firewall Rule**	The High-rated rule leverages VPN reduction alongside ANY destination and service scopes with no logging, allowing broad unmonitored access through the VPN perimeter.	Replace the ANY destination and service definitions in the High-rated rule with specific, authorised network objects and port definitions. Enable logging at session end and apply threat prevention and URL filtering security profiles.
High	**Enable Logging on All Security Rules**	Rules without logging configured produce no audit trail for traffic matches, preventing detection of malicious activity and violating forensic and compliance requirements.	Audit all 45 firewall rules and enable at minimum session-end logging on each rule. Configure log forwarding to a centralised SIEM or syslog server to ensure log availability and integrity.
High	**Attach Security Profiles to All Permissive Rules**	Rules lacking security profiles provide no threat prevention, antivirus, or URL filtering inspection, allowing malicious payloads to traverse the firewall undetected.	Assign a Security Profile Group — encompassing antivirus, anti-spyware, vulnerability protection, and URL filtering — to all rules that permit outbound or inbound traffic, prioritising those with ANY destination or service definitions.

Priority	Action Item	Risk	Recommended Action
High	**Replace ANY Service Definitions with Explicit Ports**	Rules permitting ANY service allow all TCP and UDP ports, far exceeding the access required by business functions and significantly expanding the exploitable attack surface.	Conduct a traffic analysis to determine the specific ports required by each rule and replace ALL ANY service objects with explicit application or port-based service definitions. Leverage App-ID where possible to enforce application-level control.
High	**Restrict ANY Destination Definitions**	Rules configured with ANY destination permit traffic to all network segments, including sensitive infrastructure, increasing the blast radius of any compromise.	Replace ANY destination objects with specific, named address objects or address groups representing only the authorised target networks. Implement zone-based segmentation to enforce traffic boundaries.
High	**Secure Remote Access Service Rules**	Remote access service rules without logging or security profiles allow unmonitored remote connectivity, which could facilitate credential theft, unauthorised access, or persistent threats.	Apply dedicated security profiles to all remote access rules, enable logging, and restrict source and destination to explicitly authorised address ranges. Consider implementing multi-factor authentication at the policy enforcement point.
Medium	**Audit VPN Reduction Rule Scope**	VPN reduction applied alongside broad ANY service and destination definitions may inadvertently grant excessive access to VPN-connected users or sites.	Review all VPN-reduction-affected rules to confirm that the resulting effective access scope aligns with documented business requirements, and narrow service and destination definitions accordingly.
Low	**Document and Validate Low-Risk Rules**	Although rated Low, rules with even minor permissiveness misconfigurations can contribute to cumulative risk when combined with other weaknesses in the rule base.	Schedule a periodic rule review cycle to validate that all 43 Low-rated rules remain fit for purpose, removing or tightening any rules that are no longer required or that have drifted from their original intent.
Low	**Implement Rule Cleanup and Shadow Rule Analysis**	Unreviewed or shadowed rules may allow traffic that is believed to be blocked, or conversely block traffic that administrators assume is permitted, leading to security gaps or operational disruption.	Perform a full shadow rule analysis using the firewall's built-in policy optimiser or a third-party tool, and remove or reorder any shadowed, redundant, or unused rules identified during the review.

1. Palo Alto Rule Analysis

Firewall Name	Rule ID	Rule Name	Source Zones	Destination Zones	Source Object	Destination Object	Service Object	Application	Action	Log Setting	Security Profiles	Permissiveness Level	Risk Factors (Full)
DEMO-PA-440	1	Universal-Block-Rule	nas-zone, trust, wifi-zone	untrust	LAN-Network, NAS-Network, WiFi-Net	panw-highrisk-ip-list, panw-known-ip-list	application-default	any	deny	False	False	Low	
DEMO-PA-440	2	Social-Media Daily Block	wifi-zone	untrust	Keith_Phone, KH-iPad	any	any	facebook, instagram, tiktok, twitter, youtube-base, youtube-livechat-posting, youtube-posting, youtube-uploading	deny	False	False	Low	
DEMO-PA-440	3	Danni Box	trust	untrust	Danni-Box	any	any	any	allow	False	True	Low	Destination ANY/ALL, Service ANY/ALL, No Logging Configured
DEMO-PA-440	4	Rasberry_Pi3 Outbound	trust	untrust	Xenno_Pi3	any	any	dns, dns-base, ntp, ntp-base, ssl	allow	False	True	Low	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured
DEMO-PA-440	5	Danni Box to WiFi Network	trust	wifi-zone	Danni-Box	WiFi-Net	any	any	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	6	TEK-AD Outbound Rule	trust	untrust	Lab-FTG 40F-1	any	any	any	allow	False	False	Low	Destination ANY/ALL, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	7	Rasberry_Pi3 Management	wifi-zone	trust	WiFi-Net	Xenno_Pi3	any	ssh, ssl	allow	False	True	Low	VPN Reduction Applied, Service ANY/ALL, No Logging Configured
DEMO-PA-440	8	Rasberry_Pi3 DNS	wifi-zone	trust	WiFi-Net	Xenno_Pi3	any	dns, dns-base	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	9	LAN App-Rule	trust	untrust	LAN-Network	any	any	google-base, ping, quic, rtcp, rtp, ssl, traceroute	allow	False	True	High	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured
DEMO-PA-440	10	LAN Internet Access	trust	untrust	LAN-Network	any	dns-udp, service-http, service-https	any	allow	False	True	Critical	Destination ANY/ALL, No Logging Configured
DEMO-PA-440	11	Cisco ASA TFTP Rule	trust	wifi-zone	Cisco-ASA_Lab-1, Cisco-ASA_Lab-2, Cisco-ASA_Lab-TEMP	Keith_Laptop-1	application-default	tftp	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	12	LAN Shared-Drive	trust	trust	LAN-Network	Shared_Drive	application-default	ms-ds-smb	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	13	Juniper-Test-FW-Management	wifi-zone	trust	WiFi-Net	XennoSec-JP-FW	ssh	any	allow	False	False	Low	Remote Access Services, No Logging Configured, No Security Profiles
DEMO-PA-440	14	WiFi-Shared-Drive	wifi-zone	trust	WiFi-Net	Cisco-ASA_Lab-1, Cisco-ASA_Lab-2, Cisco-ASA_Lab-TEMP, Lab-Net_Drive-1, LAB-Net_Drive-2, XennoSec-JP-FW	application-default	ms-ds-smb, ssh, web-browsing	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	15	PA-MGMT Internet Access	trust	untrust	PA-MGMT	any	ntp	ntp	allow	False	True	Low	Destination ANY/ALL, No Logging Configured
DEMO-PA-440	16	AD LDAP Rule	trust	nas-zone	FW-LAN-IF	FW-NAS-IF	application-default	ldap	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	17	AD Monitor Rule	trust	nas-zone	FW-LAN-IF	FW-NAS-IF	application-default	ms-ds-smb-base, msrpc-base, netbios-ss	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	18	Shodan Tool Access	wifi-zone	untrust	WiFi-Net	any	application-default	shodan	allow	False	True	Low	Destination ANY/ALL, Service ANY/ALL, No Logging Configured
DEMO-PA-440	19	Danni iPad	wifi-zone	untrust	Danni-iPad, Danni-iPad-2	any	dns-udp, service-http, service-https	any	allow	False	True	Low	Destination ANY/ALL, No Logging Configured
DEMO-PA-440	20	iRobot Rule	wifi-zone	untrust	iRobot-1, iRobot_2	any	any	aws-iot, dns, ntp, ssl	allow	False	False	Low	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	21	Keith-Devices WiFi Internet Access	wifi-zone	untrust	Keith_Laptop-1, KH-iPad	any	any	ssl, web-browsing	allow	False	True	Low	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured
DEMO-PA-440	22	Keith-Devices WiFi Block Quic	wifi-zone	untrust	Keith_Laptop-1, KH-iPad	any	any	quic	deny	False	False	Low	
DEMO-PA-440	23	WiFi Internet Access	wifi-zone	untrust	WiFi-Net	any	any	any	allow	False	False	Low	Destination ANY/ALL, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	24	Tek_AD RDP and LDAP Inbound Access	wifi-zone	trust	WiFi-Net	TEK-AD-Svr	application-default	ldap, ms-rdp	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	25	Tek_AD CA Inbound Access	wifi-zone	trust	WiFi-Net	TEK-AD-Svr	service-http, service-https	any	allow	False	False	Low	No Logging Configured, No Security Profiles
DEMO-PA-440	26	Xenno-Probe Inbound Spiderfoot OSINT Access	wifi-zone	trust	WiFi-Net	Xenno-Probe	tcp-5000	any	allow	False	False	Low	No Logging Configured, No Security Profiles
DEMO-PA-440	27	Xenno-Probe Inbound RDP Access	wifi-zone	trust	WiFi-Net	Xenno-Probe	application-default	ms-rdp	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	28	Xenno-Probe Inbound Mgmt Access	wifi-zone	trust	WiFi-Net	Xenno-Probe	application-default	ssh, ssh-tunnel	allow	False	False	Low	VPN Reduction Applied, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	29	Xenno-Probe Inbound LDAP Svr Magmt	nas-zone, trust, wifi-zone	trust	any	Xenno-Probe	service-http, service-https	any	allow	False	False	Low	Source ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	30	Xenno-Probe SNMP Outbound	trust	any	Xenno-Probe	any	application-default	snmp	allow	False	False	Low	Destination ANY/ALL, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	31	Xenno-Probe Inbound LDAP Access	wifi-zone	trust	WiFi-Net	Xenno-Probe	application-default	ldap	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	32	DNS Service Rule	wifi-zone	untrust	WiFi-Net	Google DNS Servers, QUAD-9-DNS Servers	application-default	dns	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	33	IKE VPN Access	wifi-zone	untrust	WiFi-Net	any	application-default	ipsec	allow	False	False	Low	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	34	Tek-Probe Mgmt Access	wifi-zone	trust	WiFi-Net	Tek-Probe	application-default	ms-rdp, ssh	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	35	LAN to LAB FTG-40F	wifi-zone	trust	WiFi-Net	Lab-FTG 40F-1	ssh, tcp-10443	any	allow	False	False	Low	Remote Access Services, No Logging Configured, No Security Profiles
DEMO-PA-440	36	LAN to Cisco Switch	wifi-zone	trust	WiFi-Net	Main-SW	service-https, ssh	any	allow	False	False	Low	Remote Access Services, No Logging Configured, No Security Profiles
DEMO-PA-440	37	PA440 MGMT Rule	wifi-zone	trust	WiFi-Net	PA-MGMT	service-https, ssh	ssh, ssl	allow	False	True	Low	VPN Reduction Applied, Remote Access Services, No Logging Configured
DEMO-PA-440	38	PA440 Management Rule	trust	wifi-zone	LAN-Network	WiFi-Net	service-https, ssh	ssh, ssl	allow	False	True	Low	VPN Reduction Applied, Remote Access Services, No Logging Configured
DEMO-PA-440	39	Allow_Inbound_2_Plex	untrust	nas-zone	any	ext-fw-if	tcp-44000	plex, ssl, web-browsing, web-crawler	allow	False	True	Low	VPN Reduction Applied, Source ANY/ALL, No Logging Configured
DEMO-PA-440	40	WiFi to NAS Access	wifi-zone	nas-zone	WiFi-Net	TEK-NAS	any	any	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	41	LAN to NAS Access	trust	nas-zone	LAN-Network	TEK-NAS	any	any	allow	False	True	Low	Service ANY/ALL, No Logging Configured
DEMO-PA-440	42	NAS Internet Access	nas-zone	untrust	TEK-NAS	any	any	bitdefender, brightcloud, dns, dns-over-https, icmp, ms-office365-base, ms-update, ntp, ocsp, ping, sentinelone, soap, solarwinds, ssl, traceroute, web-browsing, windows-azure, windows-push-notifications	allow	False	True	Low	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured
DEMO-PA-440	43	Ping Allow Rule	wifi-zone	trust	WiFi-Net	LAN-Network	application-default	ping	allow	False	False	Low	Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	44	LAN-App-Rule	wifi-zone	untrust	WiFi-Net	any	any	any	allow	False	False	Low	Destination ANY/ALL, Service ANY/ALL, No Logging Configured, No Security Profiles
DEMO-PA-440	45	Clean Up Rule	any	any	any	any	any	any	deny	False	False	Low	

2. Critical & High Risk Rules

Firewall Name	Firewall Model	Rule ID	Rule Name	Risk Level	Score	Traffic Direction	Primary Risk Factors (Full)	Source Addresses (Full)	Destination Addresses (Full)	VPN Associated	Status	Log Setting	Security Profiles	CIS Benchmark Violations (Full)	CIS Benchmark Action (Full)
DEMO-PA-440	PA 440	10	LAN Internet Access	Critical	95	outbound	Destination ANY/ALL, No Logging Configured	172.16.4.0/24	any	No	enabled		virus:default, spyware:default, vulnerability:default, url-filtering:default, file-blocking:basic file blocking	CIS_2_2_1, CIS_2_2_1, CIS_2_2_2, CIS_2_1_1, CIS_3_1_1, CIS_2_2_3, CIS_8_1_1, CIS_3_1_1	CIS 2.2.1: Apply principle of least privilege; CIS 2.2.1: Restrict destination to required hosts; CIS 3.1.1: Enable comprehensive logging
DEMO-PA-440	PA 440	9	LAN App-Rule	High	85	outbound	VPN Reduction Applied, Destination ANY/ALL, Service ANY/ALL, No Logging Configured	172.16.4.0/24	any	Yes	enabled		virus:default, spyware:default, vulnerability:default, file-blocking:basic file blocking	CIS_2_2_1, CIS_2_2_1, CIS_2_2_2, CIS_2_2_3, CIS_5_1_1, CIS_3_1_1	CIS 2.2.1: Restrict destination to required hosts; CIS 2.2.1: Limit to specific required ports; CIS 3.1.1: Enable comprehensive logging

CIS System Configuration — Findings & Recommendations

Executive Findings

The system configuration compliance score of 91.7% reflects a generally sound configuration baseline for device DEMO-PA-440; however, four configuration checks have failed, two of which are rated High severity. These failures introduce tangible risks related to intra-zone traffic control and overly broad service definitions at the policy level, which collectively undermine the firewall's ability to enforce a least-privilege security posture.

The failure of CIS_1_2, which requires that intra-zone traffic be denied by default, is particularly concerning as it permits unconstrained communication between hosts within the same security zone. This configuration is frequently exploited during lateral movement phases of an attack, where a threat actor moves between systems within a trusted zone without traversing a zone boundary that would otherwise trigger inspection. Similarly, CIS_3_2's failure to restrict the use of ANY service definitions at the configuration level compounds the rule-base permissiveness issues identified in the rules assessment.

The two Low-severity failures — relating to SNMP version configuration (CIS_2_3_1) and the absence of High Availability (CIS_2_5_1) — represent operational and security hygiene concerns. SNMP v1/v2c usage exposes management-plane credentials to interception, while the lack of HA configuration introduces a single point of failure for network availability. These items should be addressed within standard change management cycles.

Remediation Recommendations

Priority	Action Item	Risk	Recommended Action
High	**Deny Intra-Zone Traffic by Default (CIS_1_2)**	Without a default deny posture for intra-zone traffic, hosts within the same zone can communicate freely without firewall inspection, enabling undetected lateral movement by threat actors.	Navigate to Network > Zones and set the intra-zone default action to Deny for all defined security zones. Validate that any legitimate intra-zone traffic flows are explicitly permitted by named rules subject to full logging and security profile inspection.
High	**Eliminate ANY Service in Policies (CIS_3_2)**	Policies permitting ANY service allow all ports and protocols, violating the principle of least privilege and substantially increasing the attack surface exposed to both internal and external threats.	Conduct a comprehensive audit of all security policies and replace every instance of the ANY service object with explicit, named service objects defining only the required ports and protocols. Use application-based controls via App-ID where applicable to enforce more granular restrictions.
Low	**Upgrade SNMP to Version 3 (CIS_2_3_1)**	SNMP v1 and v2c transmit community strings in cleartext, allowing an attacker with network access to capture credentials and gain read or write access to device management data.	Disable SNMP v1 and v2c on the management interface and configure SNMP v3 with both authentication (SHA) and privacy (AES) parameters. Restrict SNMP access to authorised management hosts via access control lists on the management profile.

Priority	Action Item	Risk	Recommended Action
Low	**Configure High Availability (CIS_2_5_1)**	The absence of a High Availability configuration creates a single point of failure, meaning any hardware fault or software issue on DEMO-PA-440 will result in complete loss of network security enforcement and potential service outage.	Assess the availability of a compatible secondary PA-440 unit and configure an Active/Passive or Active/Active HA pair in accordance with Palo Alto Networks HA best practices. Validate failover behaviour through scheduled testing following deployment.

3. CIS System Configuration

Firewall Name	Check ID	Check Name	Level	Section	Check Status	Severity	Scored	Description (Full)	Finding (Full)	Recommendation (Full)	Priority	Compliance Impact
DEMO-PA-440	CIS_1_1	Ensure DNS server is configured	Level 1	Basic Configuration	PASS	LOW	Yes	DNS servers must be configured for proper name resolution	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_1_3	Ensure management interface access is restricted	Level 1	Basic Configuration	PASS	LOW	Yes	Management interface should only allow access from trusted networks	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_1	Ensure login banner is configured	Level 1	System Configuration	PASS	LOW	Yes	Login banner should warn about unauthorized access	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_2	Ensure acknowledgment of login banner	Level 1	System Configuration	PASS	LOW	Yes	Users must acknowledge login banner before proceeding	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_4	Ensure NTP servers are configured	Level 1	System Configuration	PASS	LOW	Yes	NTP synchronization is critical for log correlation	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_5	Ensure hostname is set	Level 1	System Configuration	PASS	LOW	Yes	Hostname should be properly configured for identification	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_6	Disable telnet service	Level 1	System Configuration	PASS	LOW	Yes	Telnet transmits credentials in clear text and should be disabled	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_7	Disable HTTP service	Level 1	System Configuration	PASS	LOW	Yes	HTTP management interface should be disabled in favor of HTTPS	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_8	Ensure SSL/TLS service profile is configured	Level 1	System Configuration	PASS	LOW	Yes	SSL/TLS service profile ensures encrypted management communications	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_9	Ensure minimum TLS version (TLS 1.2 or higher)	Level 1	System Configuration	PASS	LOW	Yes	Minimum TLS 1.2 or higher should be enforced for security	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_2_1	Ensure password complexity is enabled	Level 1	Authentication	PASS	LOW	Yes	Password complexity requirements enhance security	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_2_2	Ensure minimum password length	Level 1	Authentication	PASS	LOW	Yes	Minimum password length should be at least 8 characters	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_4_1	Ensure administrator access is from trusted networks only	Level 1	Access Control	PASS	LOW	Yes	Administrative access should be restricted to specific networks	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_4_2	Ensure local user database has strong passwords	Level 1	Access Control	PASS	LOW	Yes	Local user passwords should use strong hashing algorithms	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_3_1	Ensure default deny rule exists	Level 1	Security Policies	PASS	LOW	Yes	Default deny rule should be the last rule in security policies	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_3_3	Ensure security profiles are applied	Level 1	Security Policies	PASS	LOW	Yes	Security profiles provide threat protection	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_4_1	Ensure antivirus profile is configured	Level 1	Security Profiles	PASS	LOW	Yes	Antivirus profiles protect against malware	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_4_2	Ensure anti-spyware profile is configured	Level 1	Security Profiles	PASS	LOW	Yes	Anti-spyware profiles detect and block spyware	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_4_3	Ensure vulnerability protection is configured	Level 1	Security Profiles	PASS	LOW	Yes	Vulnerability protection prevents exploitation attempts	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_7_1	Ensure system logging is configured	Level 1	Logging	PASS	LOW	Yes	System logging is essential for security monitoring	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_7_2	Ensure configuration logging is configured	Level 1	Logging	PASS	LOW	Yes	Configuration logging tracks administrative changes	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_7_3	Ensure traffic logging is enabled	Level 1	Logging	PASS	LOW	Yes	Traffic logging provides security visibility	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_1_2	Ensure intra-zone traffic is denied by default	Level 1	Basic Configuration	FAIL	HIGH	Yes	Intra-zone traffic should be denied by default for security	Configuration does not meet CIS benchmark requirement	Set intra-zone default action to deny	CRITICAL	Negative - Reduces overall compliance score
DEMO-PA-440	CIS_3_2	Check policies do not use service ANY	Level 1	Security Policies	FAIL	HIGH	Yes	Policies should specify explicit services rather than ANY	Configuration does not meet CIS benchmark requirement	Replace ANY service with specific port definitions	CRITICAL	Negative - Reduces overall compliance score
DEMO-PA-440	CIS_2_1_3	Ensure timezone is properly configured	Level 2	System Configuration	PASS	LOW	No	Proper timezone ensures accurate logging timestamps	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_1_10	Ensure certificate is configured for management	Level 2	System Configuration	PASS	LOW	No	Management interface should use valid certificates	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_5_2	Ensure update schedule is configured	Level 2	System Maintenance	PASS	LOW	No	Automated updates ensure latest security patches	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_4_4	Ensure URL filtering is configured	Level 2	Security Profiles	PASS	LOW	No	URL filtering blocks access to malicious websites	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_4_5	Ensure file blocking is configured	Level 2	Security Profiles	PASS	LOW	No	File blocking prevents dangerous file types	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_5_1	Ensure zone protection profiles are configured	Level 2	Zone Protection	PASS	LOW	No	Zone protection profiles provide DoS and flood protection	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_5_2	Ensure flood protection is enabled	Level 2	Zone Protection	PASS	LOW	No	Flood protection prevents DoS attacks	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_8_1	Ensure certificate management is configured	Level 2	Certificate Management	PASS	LOW	No	Proper certificate management ensures encrypted communications	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_8_2	Ensure SSL decryption is configured	Level 2	Certificate Management	PASS	LOW	No	SSL decryption enables inspection of encrypted traffic	Configuration complies with CIS benchmark requirement	Configuration is compliant - maintain current settings	LOW	Positive - Meets CIS Benchmark requirement
DEMO-PA-440	CIS_2_3_1	Ensure SNMP is properly configured (check for v3)	Level 2	Monitoring	FAIL	LOW	No	SNMP v3 provides authentication and encryption	Configuration does not meet CIS benchmark requirement	Configure SNMP v3 with authentication and encryption	MEDIUM	Negative - Best practice not implemented
DEMO-PA-440	CIS_2_5_1	Check for High Availability configuration	Level 2	High Availability	FAIL	LOW	No	High Availability ensures system resilience	Configuration does not meet CIS benchmark requirement	Configure High Availability for redundancy	MEDIUM	Negative - Best practice not implemented

CIS Benchmark Compliance — Findings & Recommendations

Executive Findings

A total of 15 CIS benchmark controls were evaluated against device DEMO-PA-440, of which 7 controls recorded active violations, accounting for 82 individual violation instances. The two most critical controls — 2.2.1 (Least Privilege Security Policies, 36 violations) and 2.2.2 (Deny-All Default Policy, 34 violations) — together represent 85% of all recorded violations and indicate systemic deficiencies in the fundamental security policy architecture of this device. These findings are consistent with and directly correlated to the critically low rule compliance score of 11.1%.

Controls relating to administrative access restriction (1.1.1, 5 violations), security event logging (3.1.1, 3 violations), VPN authentication strength (5.1.2, 2 violations), and VPN encryption standards (5.1.1, 1 violation) represent additional areas requiring structured remediation. The logging deficiency in control 3.1.1 is of particular concern as it limits the organisation's ability to detect, alert on, and investigate security incidents in real time. Unnecessary services remaining enabled (2.1.1, 1 violation) further expand the management-plane attack surface unnecessarily.

Eight controls recorded zero violations and are currently meeting their benchmark requirements, indicating that foundational areas such as PAN-OS version currency, secure management protocols, IPS enablement, and application identification are well maintained. These compliant controls should be preserved through change management discipline and periodic re-assessment. The overall benchmark compliance posture requires a prioritised remediation programme addressing the Critical and Immediate-priority controls before the next assessment cycle.

Remediation Recommendations

Priority	Action Item	Risk	Recommended Action
Critical	**Enforce Least Privilege Across All Security Policies (2.2.1)**	With 36 violations, the pervasive failure to enforce least privilege in security policies represents the single largest contributor to the organisation's risk exposure, permitting far broader access than is operationally necessary.	Initiate a full security policy review programme, examining each of the 45 rules for excessive source, destination, service, and application permissions. Replace all overly broad definitions with the minimum required access and document the business justification for each rule.
Critical	**Implement Deny-All Default Policy (2.2.2)**	The absence of a deny-all default rule at the end of the policy base means that traffic not explicitly matched by an existing rule may be permitted, fundamentally undermining the firewall's role as a security enforcement point.	Create an explicit deny-all rule as the final entry in the security policy, configured to log all matches for visibility. Ensure the rule covers all zones and traffic types and validate through testing that only explicitly permitted traffic traverses the firewall.
High	**Restrict Administrative Access to Authorised Users (1.1.1)**	Five violations against this control indicate that administrative access is not sufficiently restricted, increasing the risk of unauthorised configuration changes or exploitation of administrative credentials.	Audit all administrator accounts, remove or disable any that are not actively required, enforce role-based access control with the principle of least privilege, and implement multi-factor authentication for all administrative access methods including the web UI and SSH.

Priority	Action Item	Risk	Recommended Action
High	**Enable Comprehensive Security Event Logging (3.1.1)**	Three violations of the security event logging control mean that policy matches, authentication events, and administrative activities are not being consistently recorded, creating blind spots for incident detection and forensic investigation.	Enable logging at session end on all security policies, activate authentication and system log forwarding, and configure log profiles to forward all security-relevant events to a centralised SIEM platform with defined retention periods meeting compliance requirements.
High	**Disable Unnecessary Services (2.1.1)**	At least one unnecessary service remains enabled on the device, expanding the management-plane attack surface and providing potential entry points for exploitation.	Review all enabled services on the management interface and data plane, disable any protocols not explicitly required (such as HTTP, Telnet, or unused API access), and document approved services in the organisation's firewall hardening standard.
High	**Strengthen VPN Authentication Configuration (5.1.2)**	Two violations against VPN authentication controls indicate that VPN connections may rely on insufficiently strong authentication methods, increasing the risk of credential-based compromise of remote access tunnels.	Replace pre-shared key authentication with certificate-based authentication for all VPN tunnels where technically feasible, and enforce multi-factor authentication for remote access VPN user connections through integration with an identity provider.
High	**Enforce Strong VPN Encryption Standards (5.1.1)**	One violation of the VPN encryption control indicates at least one tunnel is configured with a cipher suite weaker than AES-256, exposing encrypted VPN traffic to potential decryption by a sufficiently resourced adversary.	Audit all IKE and IPsec crypto profiles configured on the device, remove any profiles utilising DES, 3DES, or AES-128, and enforce AES-256-GCM with SHA-256 or stronger for both IKE phase 1 and phase 2 negotiations.
Medium	**Configure Administrative Session Timeouts (1.1.2)**	Without defined idle timeout values, administrative sessions left unattended remain active indefinitely, providing an opportunity for unauthorised access if a workstation is left unattended.	Set the idle timeout for all administrative session types (web UI, SSH, and CLI) to a maximum of 10 minutes in accordance with CIS benchmark guidance and the organisation's access control policy.
Medium	**Verify and Enforce Log Retention Policy (3.1.2)**	Without a formally configured log retention period, logs may be overwritten prematurely, preventing historical forensic analysis and potentially violating regulatory compliance requirements.	Configure the on-device log retention settings to align with organisational and regulatory requirements, and implement log forwarding to an external repository or SIEM to ensure long-term retention independent of device storage constraints.
Low	**Automate and Secure Configuration Backups (4.1.2)**	Without automated configuration backups, a device failure or misconfiguration event could result in prolonged recovery times and potential loss of the security policy baseline.	Configure automated scheduled configuration exports via the device scheduler or Panorama, encrypt backup files at rest, and store them in a geographically separate, access-controlled repository with version history retained for a minimum of 90 days.

4. CIS Benchmark Compliance

Firewall Name	Firewall Model	CIS Control ID	Control Title (Full)	Level	Section	Scored	Severity	Total Violations	Critical Risk Rules	High Risk Rules	Compliance Status	Priority	Sample Violating Rules (Full)	Implementation Guidance (Full)
DEMO-PA-440	PA 440	2.2.1	Ensure security policies follow principle of least privilege	Level 1	Network Security	Yes	CRITICAL	36	2	2	NON-COMPLIANT	IMMEDIATE	Danni Box, Rasberry_Pi3 Outbound, Danni Box to WiFi Network, TEK-AD Outbound Rule, Rasberry_Pi3 Management, Rasberry_Pi3 DNS, LAN App-Rule, LAN App-Rule, LAN Internet Access, LAN Internet Access, Cisco ASA TFTP Rule, LAN Shared-Drive, WiFi-Shared-Drive, PA-MGMT Internet Access, AD LDAP Rule, AD Monitor Rule, Shodan Tool Access, Danni iPad, iRobot Rule, Keith-Devices WiFi Internet Access, WiFi Internet Access, Tek_AD RDP and LDAP Inbound Access, Xenno-Probe Inbound RDP Access, Xenno-Probe Inbound Mgmt Access, Xenno-Probe Inbound LDAP Svr Magmt, Xenno-Probe SNMP Outbound, Xenno-Probe Inbound LDAP Access, DNS Service Rule, IKE VPN Access, Tek-Probe Mgmt Access, Allow_Inbound_2 Plex, WiFi to NAS Access, LAN to NAS Access, NAS Internet Access, Ping Allow Rule, LAN-App-Rule	Review all security rules for excessive permissions
DEMO-PA-440	PA 440	2.2.2	Ensure deny-all default policy is configured	Level 1	Network Security	Yes	HIGH	34	1	1	NON-COMPLIANT	IMMEDIATE	Danni Box, Rasberry_Pi3 Outbound, Danni Box to WiFi Network, TEK-AD Outbound Rule, Rasberry_Pi3 Management, Rasberry_Pi3 DNS, LAN App-Rule, LAN Internet Access, Cisco ASA TFTP Rule, LAN Shared-Drive, WiFi-Shared-Drive, PA-MGMT Internet Access, AD LDAP Rule, AD Monitor Rule, Shodan Tool Access, Danni iPad, iRobot Rule, Keith-Devices WiFi Internet Access, WiFi Internet Access, Tek_AD RDP and LDAP Inbound Access, Xenno-Probe Inbound RDP Access, Xenno-Probe Inbound Mgmt Access, Xenno-Probe Inbound LDAP Svr Magmt, Xenno-Probe SNMP Outbound, Xenno-Probe Inbound LDAP Access, DNS Service Rule, IKE VPN Access, Tek-Probe Mgmt Access, Allow_Inbound_2 Plex, WiFi to NAS Access, LAN to NAS Access, NAS Internet Access, Ping Allow Rule, LAN-App-Rule	Ensure last policy denies all traffic not explicitly allowed
DEMO-PA-440	PA 440	1.1.1	Ensure administrative access is restricted to authorized users	Level 1	Access Control	Yes	HIGH	5	0	0	NON-COMPLIANT	MEDIUM	Juniper-Test-FW-Management, LAN to LAB FTG-40F, LAN to Cisco Switch, PA440 MGMT Rule, PA440 Management Rule	Configure strong authentication and limit admin users
DEMO-PA-440	PA 440	3.1.1	Ensure logging is enabled for security events	Level 1	Logging and Monitoring	Yes	HIGH	3	2	1	NON-COMPLIANT	IMMEDIATE	LAN App-Rule, LAN Internet Access, LAN Internet Access	Enable logging for policy matches, authentication, and admin activities
DEMO-PA-440	PA 440	5.1.2	Ensure VPN authentication is properly configured	Level 1	VPN Configuration	Yes	HIGH	2	0	0	NON-COMPLIANT	MEDIUM	PA440 MGMT Rule, PA440 Management Rule	Implement certificate-based or strong authentication
DEMO-PA-440	PA 440	5.1.1	Ensure VPN uses strong encryption	Level 1	VPN Configuration	Yes	HIGH	1	0	1	NON-COMPLIANT	HIGH	LAN App-Rule	Use AES-256 or stronger encryption for VPN tunnels
DEMO-PA-440	PA 440	2.1.1	Ensure unnecessary services are disabled	Level 1	Network Security	Yes	HIGH	1	1	0	NON-COMPLIANT	IMMEDIATE	LAN Internet Access	Review and disable unused services like HTTP, Telnet, etc.
DEMO-PA-440	PA 440	1.1.2	Ensure administrative sessions timeout appropriately	Level 1	Access Control	Yes	MEDIUM	0	0	0	COMPLIANT	MAINTAIN		Set appropriate idle timeout values for admin sessions
DEMO-PA-440	PA 440	1.2.1	Ensure default passwords are changed	Level 1	Access Control	Yes	CRITICAL	0	0	0	COMPLIANT	MAINTAIN		Change all default passwords and use strong password policies
DEMO-PA-440	PA 440	2.1.2	Ensure secure protocols are used for management	Level 1	Network Security	Yes	HIGH	0	0	0	COMPLIANT	MAINTAIN		Disable HTTP and Telnet, enable HTTPS and SSH only
DEMO-PA-440	PA 440	3.1.2	Ensure log retention period is configured	Level 1	Logging and Monitoring	Yes	MEDIUM	0	0	0	COMPLIANT	MAINTAIN		Set log retention to meet compliance requirements
DEMO-PA-440	PA 440	4.1.1	Ensure system is running supported PAN-OS version	Level 1	System Maintenance	Yes	HIGH	0	0	0	COMPLIANT	MAINTAIN		Regularly update to latest stable PAN-OS version
DEMO-PA-440	PA 440	4.1.2	Ensure regular configuration backups are performed	Level 1	System Maintenance	Yes	MEDIUM	0	0	0	COMPLIANT	MAINTAIN		Automate configuration backups and store securely
DEMO-PA-440	PA 440	7.1.2	Ensure IPS is enabled and configured	Level 1	Threat Prevention	Yes	HIGH	0	0	0	COMPLIANT	MAINTAIN		Enable IPS with regularly updated signatures
DEMO-PA-440	PA 440	9.1.1	Ensure application identification is enabled	Level 1	Application Control	Yes	HIGH	0	0	0	COMPLIANT	MAINTAIN		Monitor and control application usage with App-ID
DEMO-PA-440	PA 440	8.1.1	Ensure URL filtering is configured appropriately	Level 2	URL Filtering	Yes	MEDIUM	7	1	0	NON-COMPLIANT	IMMEDIATE	LAN Internet Access, Danni iPad, Tek_AD CA Inbound Access, Xenno-Probe Inbound LDAP Svr Magmt, LAN to Cisco Switch, PA440 MGMT Rule, PA440 Management Rule	Block malicious and inappropriate web content
DEMO-PA-440	PA 440	2.2.3	Ensure security policies are properly documented	Level 2	Network Security	Yes	MEDIUM	2	1	1	NON-COMPLIANT	IMMEDIATE	LAN App-Rule, LAN Internet Access	Use meaningful names and descriptions for all policies
DEMO-PA-440	PA 440	3.2.1	Ensure remote logging is configured	Level 2	Logging and Monitoring	Yes	HIGH	0	0	0	COMPLIANT	MAINTAIN		Configure syslog forwarding to SIEM or log management system
DEMO-PA-440	PA 440	6.1.1	Ensure high availability is properly configured	Level 2	High Availability	No	MEDIUM	0	0	0	COMPLIANT	MAINTAIN		Configure active-passive or active-active HA as appropriate
DEMO-PA-440	PA 440	7.1.1	Ensure antivirus scanning is enabled	Level 2	Threat Prevention	Yes	HIGH	0	0	0	COMPLIANT	MAINTAIN		Enable AV scanning for file transfers and web browsing

5. CIS Benchmark Recommendations

Firewall Name	Firewall Model	CIS Control	Level	Priority	Category	Type	Finding (Full)	Risk (Full)	Recommendation (Full)	Timeline	Scored	Implementation (Full)
DEMO-PA-440	PA 440	CIS 2.2.1	Level 1	IMMEDIATE	Network Security - Least Privilege	Policy Violation	1 security rules with Critical permissiveness detected - These rules violate the fundamental principle of least privilege and create significant security exposure	Violation of principle of least privilege represents a fundamental security control failure that could allow unauthorized network access, lateral movement, and potential data exfiltration	Immediately review and restrict these rules to specific source/destination pairs with explicit business justification. Document all exceptions and implement compensating controls where broad access is absolutely required	24 hours	Yes	Use Palo Alto Networks address objects to define specific network segments, implement security zones for network segmentation, and create granular policies with specific source and destination requirements
DEMO-PA-440	PA 440	CIS 1.1.1, 5.1.2	Level 1	HIGH	Access Control - Authentication	Policy Violation	5 security rules allowing remote access services without proper authentication controls and security hardening measures	Unauthorized remote access without proper authentication controls creates significant attack vectors for credential theft, brute force attacks, and unauthorized system access leading to potential compromise	Implement strong multi-factor authentication for all remote access, configure VPN solutions with certificate-based authentication, and restrict remote access to specific source networks with business justification	1 week	Yes	Configure Palo Alto Networks GlobalProtect with certificate-based authentication, implement RADIUS integration for centralized authentication, enable two-factor authentication, and create specific policies for remote access with logging and monitoring
DEMO-PA-440	PA 440	CIS 3.1.1	Level 1	HIGH	Logging and Monitoring	Policy Violation	41 security rules without logging configuration, preventing security event monitoring and incident response capabilities	Absence of security logging prevents detection of security incidents, compliance violations, and forensic analysis capabilities, creating blind spots in security monitoring	Enable comprehensive logging for all security rules, configure log forwarding to SIEM systems, and establish log retention policies meeting compliance requirements	1 week	Yes	Configure log settings for all security policies, set up syslog forwarding to centralized logging systems, enable traffic and threat logs, and implement log filtering for efficient analysis
DEMO-PA-440	PA 440	CIS 7.1.1, 7.1.2	Level 1	HIGH	Threat Prevention	Policy Violation	21 security rules without threat prevention profiles, missing critical security inspection capabilities	Absence of security profiles allows malicious content, viruses, vulnerabilities, and command-and-control traffic to pass undetected through the firewall	Configure comprehensive security profiles including antivirus, anti-spyware, vulnerability protection, URL filtering, and file blocking for all allow rules	2 weeks	Yes	Create security profile groups with antivirus, anti-spyware, vulnerability, URL filtering, file blocking, and data filtering profiles; apply to all allow rules; enable automatic signature updates
DEMO-PA-440	PA 440	CIS_1_2	Level 1	CRITICAL	System Configuration - Basic Configuration	System Configuration	System configuration check failed: Ensure intra-zone traffic is denied by default - Configuration does not meet CIS benchmark requirement	System configuration does not meet CIS baseline requirements which could lead to security weaknesses and compliance violations	Set intra-zone default action to deny	48 hours	Yes	Configure PAN-OS system settings according to CIS benchmark: Set intra-zone default action to deny
DEMO-PA-440	PA 440	CIS_3_2	Level 1	CRITICAL	System Configuration - Security Policies	System Configuration	System configuration check failed: Check policies do not use service ANY - Configuration does not meet CIS benchmark requirement	System configuration does not meet CIS baseline requirements which could lead to security weaknesses and compliance violations	Replace ANY service with specific port definitions	48 hours	Yes	Configure PAN-OS system settings according to CIS benchmark: Replace ANY service with specific port definitions

End of Report

This concludes the CIS Firewall Assessment for DEMO-PA-440.