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

AuditXA — Cisco ASA 5525-X Security Report

File: asa5525x-running-config.txt · Generated: 5 Jun 2025, 14:30 · Score: 59/100 (F)

59
/ 100

Cisco ASA 5525-X — Grade F

Analysed 24 controls against NSA, CIS, and vendor best practices · Cisco ASA 5525-X (ASA 9.18(4))

Generated: 5 Jun 2025, 14:30

1 Critical | 2 High | 0 Medium | 21 Passed

AUDIT SUMMARY

RESULTS BY CATEGORY · WEAKEST FIRST

Encryption	67%	2/3 passed
AnyConnect	80%	4/5 passed
Firewall	80%	4/5 passed
Management	100%	6/6 passed
Logging	100%	3/3 passed
Geo-Blocking	100%	1/1 passed
Interface	100%	1/1 passed

TLS 1.2 minimum — legacy protocols disabled

CRITICAL Encryption

SSLv3, TLS 1.0, 3DES, and RC4 are cryptographically broken.

```
ssl server-version tlsv1.2
ssl client-version tlsv1.2
```

NIST SP 800-52r2; Cisco ASA TLS Hardening Guide

AnyConnect certificate validation enforced

HIGH AnyConnect

Without certificate validation, AnyConnect clients cannot verify they are connecting to a legitimate server — enabling MITM attacks against remote workers.

```
webvpn
 certificate-validation <trustpoint>
```

AuditXA Hardening Checklist

Botnet traffic filtering enabled

HIGH Firewall

The ASA botnet traffic filter blocks known C2 and botnet destinations. It is a built-in, no-cost control that requires only a subscription to enable.

```
dynamic-filter enable interface outside
dynamic-filter use-database
```

AuditXA Hardening Checklist

AnyConnect MFA via RADIUS / SAML

OK AnyConnect

AnyConnect must authenticate via RADIUS+MFA.

```
aaa-server RADIUS (inside) host <radius-ip>
 key <shared-secret>
```

Cisco AnyConnect Hardening Guide – Section 3

VPN idle timeout and session limits configured

OK AnyConnect

Idle sessions must time out after 30 min.

```
group-policy <n> attributes
 vpn-idle-timeout 30
 vpn-session-timeout 480
```

NIST 800-46r2 – VPN Session Management

Split tunnel policy reviewed and restricted

OK AnyConnect

Only approved subnets should bypass the tunnel.

```
group-policy <n> attributes
 split-tunnel-policy tunnelspecified
```

Cisco AnyConnect Split Tunnel Best Practices

Internal DNS pushed to AnyConnect clients

OK AnyConnect

Internal DNS servers must be pushed to prevent DNS leaks.

```
group-policy <n> attributes
 dns-server value <internal-dns1>
```

Cisco Split DNS Deployment Guide

Threat Detection enabled

OK Firewall

Threat Detection monitors for port scans, DoS attacks, and service abuse.

```
threat-detection basic-threat
threat-detection statistics access-list
threat-detection scanning-threat shun
```

Cisco ASA Threat Detection Guide

Global inspection service policy configured

OK Firewall

A global service policy applying Layer 7 inspection prevents protocol abuse.

```
policy-map global_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect http
service-policy global_policy global
```

Cisco ASA MPF Configuration Guide

AAA for SSH/HTTPS management access

OK Management

All management access must authenticate via centralised AAA (TACACS+).

```
aaa authentication ssh console TACACS+ LOCAL
aaa authentication http console TACACS+ LOCAL
```

CIS ASA Benchmark – Management Plane

Management access restricted to known hosts

OK Management

HTTP/HTTPS and SSH access must be restricted to specific management host IP ranges.

```
http <mgmt-subnet> <mask> management
ssh <mgmt-subnet> <mask> management
```

CIS ASA Benchmark 1.1

Syslog configured with informational level

OK Logging

All events must be forwarded to SIEM.

```
logging enable
logging host <interface> <siem-ip>
logging trap informational
```

Cisco ASA Logging Best Practices

ICMP restricted on external interface

OK Logging

Unrestricted ICMP on external interfaces enables network reconnaissance.

```
icmp deny any outside
```

Cisco ASA Hardening Guide

SSH version 2 only — SSHv1 disabled

OK Encryption

SSHv1 has known cryptographic weaknesses and must not be used. Many ASAs ship with SSHv1 enabled by default. Restrict SSH to version 2 only.

```
ssh version 2
```

AuditXA Hardening Checklist

Console and VTY exec timeout configured

OK Management

Without exec timeout, an unattended management session remains open indefinitely — a physical or remote attacker can use it without needing credentials.

```
console timeout 5
ssh timeout 30
```

AuditXA Hardening Checklist

Inbound any/any permit rule not present

OK Firewall

An inbound permit ip any any rule allows all traffic from the internet to all internal hosts. This completely defeats the purpose of the firewall.

```
Replace permit ip any any with explicit rules for required services only.
```

AuditXA Hardening Checklist

AES-256 or AES-128 only for IKEv2 proposals

OK Encryption

3DES and single DES are cryptographically broken and must not be used in VPN proposals. Use AES-256 with SHA-256 and DH group 14 minimum.

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 14
```

AuditXA Hardening Checklist

SNMP v3 with authentication — SNMPv1/v2 disabled

OK Management

SNMPv1 and SNMPv2 community strings are sent in cleartext and default strings like "public" are well-known. Disable them and use SNMPv3 with authentication and encryption.

```
no snmp-server community public
snmp-server group MGMT v3 priv
```

AuditXA Hardening Checklist

Log buffer size and log file rotation configured

OK Logging

Without logging buffer configuration, ASA logs are lost on reboot and unavailable for incident response. Configure buffer and ASDM logging at informational level.

```
logging enable
logging buffered informational
logging asdm informational
```

AuditXA Hardening Checklist

Password encryption service enabled

OK Management

Without password encryption, all local account passwords are stored as plaintext MD5 hashes in the running config. AES encryption protects them from offline cracking if the config is exposed.

```
password encryption aes
```

AuditXA Hardening Checklist

ICMP unreachable rate limiting configured

OK Firewall

Without ICMP unreachable rate limiting, an attacker can use ICMP scanning to map your network topology at high speed. Rate limiting defeats this reconnaissance technique.

```
icmp unreachable rate-limit 1 burst-size 50
```

AuditXA Hardening Checklist

Embargo and sanctioned countries blocked via ACL

OK Geo-Blocking

Cisco ASA does not have native geo-blocking. Sanctioned country IP ranges (Cuba, Iran, North Korea, Russia, Syria) must be denied via extended ACL on the outside interface. This is required for ITAR, PCI-DSS and HIPAA compliance.

```
# Block OFAC/EU sanctioned country prefix ranges inbound on outside
interface
access-list OUTSIDE_IN extended deny ip <country-prefix-list> any log
# Maintain updated ACL or use Cisco TALOS reputation feed
```

AuditXA Hardening Checklist

SSH and HTTPS management not accessible from outside interface

OK Interface

SSH and HTTPS access configured for 0.0.0.0/0 or any on the outside interface exposes the ASA management plane to the entire internet. Restrict SSH and HTTPS to the management interface only, locked to specific administrator IP addresses.

```
no http 0.0.0.0 0.0.0.0 outside
no ssh 0.0.0.0 0.0.0.0 outside
# Replace with specific management host:
ssh <mgmt-host> 255.255.255.255 management
http <mgmt-host> 255.255.255.255 management
```

AuditXA Hardening Checklist

Management access restricted to /32 hosts not broad subnets

OK Management

SSH and HTTPS management entries with broad subnet masks allow too many hosts to reach the management plane. Restrict to /32 individual administrator IP addresses wherever possible.

```
# Replace broad subnet SSH/HTTP entries with specific /32 hosts:
ssh <admin-ip> 255.255.255.255 management
http <admin-ip> 255.255.255.255 management
```

AuditXA Hardening Checklist
