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

AuditXA — FortiGate 200F Security Report

File: fortigate-200f.conf · Generated: 5 Jun 2025, 14:30 · Score: 59/100 (F)

59
/ 100

FortiGate 200F — Grade F

Analysed 25 controls against NSA, CIS, and vendor best practices · FortiGate 200F (FortiOS 7.4.2)

Generated: 5 Jun 2025, 14:30

1 Critical | 2 High | 1 Medium | 21 Passed

AUDIT SUMMARY

RESULTS BY CATEGORY · WEAKEST FIRST

Interface	0%	0/1 passed
System Hardening	67%	2/3 passed
Management	80%	4/5 passed
SSL VPN	80%	4/5 passed
Authentication	100%	2/2 passed
IPsec VPN	100%	2/2 passed
Firewall Policies	100%	1/1 passed
Security Profiles	100%	3/3 passed
Logging	100%	1/1 passed
Updates	100%	1/1 passed
Geo-Blocking	100%	1/1 passed

WAN interfaces do not allow SSH/HTTPS/HTTP/Telnet via allowaccess

CRITICAL Interface

FortiGate WAN/external interfaces must have HTTPS, HTTP, SSH and Telnet removed from allowaccess. Management services on internet-facing interfaces expose the firewall directly to attack. Admin access must only be available on the internal or dedicated management interface.

```
config system interface
  edit "wan1"
    set allowaccess ping
    # Remove https, http, ssh, telnet from allowaccess
  next
end
```

AuditXA Hardening Checklist

Admin idle timeout configured (≤10 min)

HIGH Management

Admin sessions must time out after inactivity.

```
config system global
    set admintimeout 10
end
```

CIS FortiGate Benchmark 1.3

SSL VPN restricted via local-in policy

HIGH SSL VPN

Local-in policies restrict SSL VPN access before traffic reaches the VPN daemon.

```
config firewall local-in-policy
    edit 1
        set intf <wan-iface>
        set srcaddr <trusted-group>
        set action accept
    next
end
```

Fortinet SSL VPN Hardening Guide

NTP authentication configured

MEDIUM System Hardening

Unauthenticated NTP allows time manipulation affecting MFA and log timestamps.

```
config system ntp
    set ntpsync enable
    set type custom
end
```

CIS FortiGate Benchmark 2.x

strong-crypto enabled (TLS static keys disabled)

OK System Hardening

Strong crypto must be explicitly enabled.

```
config system global
    set strong-crypto enable
    set ssl-static-key-ciphers disable
    set dh-params 8192
end
```

Fortinet Best Practices 7.6 – Hardening; CIS FortiGate Benchmark

Admin access restricted to trusted hosts only

OK Management

Administrator accounts must be restricted to specific trusted host IP ranges.

```
config system admin
    edit admin
        set trusthost1 <mgmt-subnet>/<mask>
    next
end
```

Fortinet Best Practices 7.6; CIS FortiGate 1.1

HTTPS admin access only — HTTP disabled

OK Management

HTTP admin access transmits credentials in cleartext.

```
config system interface
    edit <mgmt-iface>
        set allowaccess https ssh
    next
end
```

CIS FortiGate Benchmark 1.2

SSH v2 only — SSHv1 disabled

OK Management

Enabling strong-crypto automatically disables SSHv1.

```
config system global
    set strong-crypto enable
end
```

Fortinet Hardening Best Practices

Two-factor / MFA enabled for admin accounts

OK Authentication

All FortiGate administrator accounts must use MFA.

```
config system admin
    edit admin
        set two-factor fortitoken-cloud
    next
end
```

Fortinet Best Practices – MFA for Admins; CIS FortiGate 1.5

LDAPS / RADSEC used for remote auth

OK Authentication

LDAP and RADIUS transmit credentials in cleartext. LDAPS or RADSEC must be used.

```
config user ldap
    edit CORP-LDAP
        set secure ldaps
        set port 636
    next
end
```

Fortinet SSL VPN Security Best Practices 7.6.2

SSL VPN login attempt limit and block time configured

OK SSL VPN

Without login rate limiting, SSL VPN is vulnerable to brute force attacks.

```
config vpn ssl settings
    set login-attempt-limit 3
    set login-block-time 60
end
```

Fortinet SSL VPN Security Best Practices 7.6.2

SSL VPN TLS version restricted to TLS 1.2+

OK SSL VPN

TLS 1.0 and TLS 1.1 have known exploitable vulnerabilities.

```
config vpn ssl settings
    set ssl-min-proto-ver tls1-2
end
```

NIST SP 800-52r2; Fortinet SSL VPN Best Practices

One SSL VPN session per user enforced

OK SSL VPN

Limiting users to one concurrent session prevents credential sharing.

```
config vpn ssl web portal
    edit <portal-name>
        set limit-user-logins enable
    next
end
```

Fortinet SSL VPN Security Best Practices 7.6.2

SSL VPN split tunnel policy audited — not unrestricted

OK SSL VPN

Split tunneling without a routing address list permits all traffic to bypass the tunnel.

```
config vpn ssl web portal
    edit <portal>
        set split-tunneling-routing-address <allowed-subnets>
    next
end
```

Fortinet SSL VPN Best Practices

IKEv2 used — IKEv1 Aggressive Mode disabled

OK IPsec VPN

IKEv1 Aggressive Mode leaks the pre-shared key hash.

```
config vpn ipsec phase1-interface
    edit <tunnel>
        set ike-version 2
    next
end
```

NIST SP 800-77r1; Fortinet IPsec Best Practices

Strong IPsec encryption — AES-256 / SHA-256 minimum

OK IPsec VPN

DES, 3DES, and DH groups 1 and 2 are cryptographically broken.

```
config vpn ipsec phase1-interface
    edit <tunnel>
        set encrypt aes256
        set authby sha256
        set dhgrp 20 19 14
    next
end
```

NIST SP 800-77r1; Fortinet IPsec Best Practices 7.6

No any/any accept policy without UTM profile

OK Firewall Policies

Any-to-any allow rules without security profiles provide no threat inspection.

```
Edit overly permissive policies:
set utm-status enable
set av-profile default
set ips-sensor default
```

Fortinet Best Practices – Policy Design

IPS sensor applied to internet-facing policies

OK Security Profiles

An IPS sensor must be attached to all policies permitting internet-bound traffic.

```
config firewall policy
    edit <internet-rule-id>
        set ips-sensor "default"
        set utm-status enable
    next
end
```

CIS FortiGate Benchmark

Web filter profile applied on outbound policies

OK Security Profiles

Web filtering blocks malware download URLs, phishing sites, and C2 categories.

```
config firewall policy
    edit <outbound-rule-id>
        set webfilter-profile "default"
        set utm-status enable
    next
end
```

Fortinet Web Filter Best Practices

AntiVirus profile applied on internet traffic

OK Security Profiles

AV profiles inspect HTTP, HTTPS, SMTP, FTP, and IMAP for malware.

```
config firewall policy
    edit <internet-rule-id>
        set av-profile "default"
        set utm-status enable
    next
end
```

Fortinet AV Profile Guide

FortiAnalyzer or syslog server configured

OK Logging

All traffic, UTM, and system events must be forwarded to FortiAnalyzer or SIEM.

```
config log syslogd setting
    set status enable
    set server <siem-ip>
    set port 514
end
```

Fortinet Logging Best Practices

FortiGuard auto-update enabled for AV, IPS, Web Filter

OK Updates

FortiGuard signatures must update automatically at least daily.

```
config system autoupdate schedule
    set status enable
    set frequency daily
    set time 04:00
end
```

Fortinet Hardening Best Practices 7.6

USB auto-install disabled

OK System Hardening

USB auto-install allows anyone with physical access to load malicious firmware.

```
config system auto-install
    set auto-install-config disable
    set auto-install-image disable
end
```

Fortinet Hardening Best Practices 7.6

Embargo and sanctioned countries blocked via geography address object

OK Geo-Blocking

FortiGate supports geography-based address objects natively. Create a geography address covering OFAC/EU embargoed countries (Russia, North Korea, Iran, Syria, Cuba, Belarus) and deny inbound on all WAN interfaces. Required for PCI-DSS, HIPAA and ITAR compliance.

```
config firewall address
  edit "Sanctioned-Countries"
    set type geography
    set country "RU KP IR SY CU BY"
  next
end
config firewall policy
  edit 0
    set name "Block-Sanctioned"
    set srcintf "wan1"
    set dstintf "any"
    set srcaddr "Sanctioned-Countries"
    set action deny
    set logtraffic all
  next
end
```

AuditXA Hardening Checklist

Admin trusted-hosts locked to specific IPs — not 0.0.0.0/0

OK Management

FortiGate admin accounts without trusted-hosts (or set to 0.0.0.0/0) can be accessed from any IP. Every admin account must have trusted-hosts configured to specific administrator IPs or a narrow management subnet. This is one of the highest-impact hardening controls on FortiGate.

```
config system admin
  edit "admin"
    set trusthost1 <admin-ip> 255.255.255.255
    set trusthost2 <backup-admin-ip> 255.255.255.255
  next
end
```

AuditXA Hardening Checklist