

Firewall rule review

Device	HQ-FGT
Platform	FortiGate
Tracked as	Head office firewall
Firmware	FortiOS 6.4.12
Rules reviewed	6 (hit counts for 5)
Generated	13 Oct 2026, 16:31
Prepared by	Example IT Services Ltd - it.manager@example.com
Report ID	SAMPLE
Standards shown	NIST SP 800-53 Rev. 5; ISO/IEC 27001:2022 Annex A; UK Cyber Essentials

F

0 / 100

8

High findings

8

Medium findings

15

Low findings

Summary

The automated review found 8 high, 8 medium and 15 low-severity issues across 6 rules, giving a score of 0/100 (grade F). The firmware is affected by 2 vulnerabilities that attackers are known to exploit; upgrading is the first priority. Fix the high-severity items first: they expose services to untrusted networks, leave intended blocks ineffective, or weaken how the firewall itself is managed. 1 finding was accepted as a risk by the organisation and left out of the score; see "Accepted risks".

This report was produced from a built-in example configuration, not a real device.

Top priorities

1. RDP open to any source (internet-facing) - Rule "RDP to admin PC" (wan1 -> internal)
2. Intended block never happens (shadowed by an allow) - Rule "Block bad actor" (deny) is completely covered by earlier rule "LAN out" (accept).
3. FortiOS 6.4.12 on FG100F is end of support and no longer gets security fixes.
4. Admin access (https, ssh) is open on internet-facing port wan1.
5. Telnet admin access is on for internal.
6. Default SNMP community "public" is in use.
7. FortiOS 6.4.12 is affected by known-exploited CVE-2024-21762: SSL-VPN out-of-bounds write (remote code execution) - Vulnerable and the affected feature is exposed. SSL-VPN is enabled on an internet-facing interface. Listed in CISA's Known Exploited Vulnerabilities catalog, so attackers are using it.
8. FortiOS 6.4.12 is affected by known-exploited CVE-2023-27997: SSL-VPN heap overflow before login (remote code execution) - Vulnerable and the affected feature is exposed. SSL-VPN is enabled on an internet-facing interface. Listed in CISA's Known Exploited Vulnerabilities catalog, so attackers are using it.

Findings

Severity	Finding	Fix	Controls
High	RDP open to any source (internet-facing) Rule "RDP to admin PC" (wan1 -> internal)	Never expose remote-admin, file-sharing or database services to the internet. Put them behind a VPN or restrict the source to known addresses. (see Remediation commands)	800-53: SC-7, AC-17, CM-7 ISO: 8.20 CE: Firewalls
High	Intended block never happens (shadowed by an allow) Rule "Block bad actor" (deny) is completely covered by earlier rule "LAN out" (accept).	Move this block above the broader allow rule, then confirm the traffic is dropped. (see Remediation commands)	800-53: CM-6, AC-4 ISO: 8.9 CE: Firewalls
High	FortiOS 6.4.12 on FG100F is end of support and no longer gets security fixes.	Upgrade to a supported FortiOS release following Fortinet's upgrade path tool. (see Remediation commands)	800-53: SI-2, SA-22 ISO: 8.8 CE: Security update management
High	Admin access (https, ssh) is open on internet-facing port wan1.	Manage the firewall over VPN or a dedicated management port. If WAN access is unavoidable, add trusted hosts and a local-in policy. (see Remediation commands)	800-53: AC-17, SC-7 ISO: 8.2, 8.20 CE: Firewalls
High	Telnet admin access is on for internal.	Remove "telnet" from allowaccess and use SSH or HTTPS. (see Remediation commands)	800-53: SC-8, CM-7, AC-17 ISO: 8.5, 8.20 CE: Secure configuration
High	Default SNMP community "public" is in use.	Change it to a long random string, or move to SNMPv3. (see Remediation commands)	800-53: IA-5, CM-6 ISO: 5.17, 8.9 CE: Secure configuration
High	FortiOS 6.4.12 is affected by known-exploited CVE-2024-21762: SSL-VPN out-of-bounds write (remote code execution) Vulnerable and the affected feature is exposed. SSL-VPN is enabled on an internet-facing interface. Listed in CISA's Known Exploited Vulnerabilities catalog, so attackers are using it. FG-IR-24-015, CISA KEV	Upgrade to 6.4.15 or later (the latest patch on your branch is best). Disable SSL-VPN until upgraded (turning off web mode alone is not enough). (see Remediation commands)	800-53: SI-2, RA-5 ISO: 8.8 CE: Security update management
High	FortiOS 6.4.12 is affected by known-exploited CVE-2023-27997: SSL-VPN heap overflow before login (remote code execution) Vulnerable and the affected feature is exposed. SSL-VPN is enabled on an internet-facing interface. Listed in CISA's Known Exploited Vulnerabilities catalog, so attackers are using it. FG-IR-23-097, CISA KEV	Upgrade to 6.4.13 or later (the latest patch on your branch is best). Disable SSL-VPN until upgraded. (see Remediation commands)	800-53: SI-2, RA-5 ISO: 8.8 CE: Security update management
Medium	Rule allows every port and protocol Rule "LAN out" (internal -> wan1)	Limit the service to the ports this traffic needs. (see Remediation commands)	800-53: CM-7, SC-7(5) ISO: 8.20 CE: Firewalls
Medium	Admin "admin" can log in from any address (no trusted hosts).	Set trusthost entries on each admin to your management networks. (see Remediation commands)	800-53: AC-17, AC-3 ISO: 8.2, 8.5 CE: Firewalls
Medium	1 admin account without two-factor authentication (admin).	Turn on FortiToken, email or SMS two-factor for every administrator. (see Remediation commands)	800-53: IA-2(1) ISO: 8.5 CE: User access control
Medium	Unencrypted HTTP admin access is on for internal.	Remove "http" from allowaccess; use HTTPS only. (see Remediation commands)	800-53: SC-8, AC-17 ISO: 8.5 CE: Secure configuration
Medium	No remote logging (syslog, FortiAnalyzer or FortiGuard) is turned on.	Send logs off the box so they survive a reboot and can be reviewed centrally. (see Remediation commands)	800-53: AU-6, AU-9 ISO: 8.15
Medium	1 VPN proposal uses weak encryption or key exchange IKE "to-branch": 3DES, SHA-1, DH group 2	Use AES-256 (or AES-GCM), SHA-256 or better, and DH group 14, 19, 20 or 21. Change both ends of each tunnel in the same window. (see Remediation commands)	800-53: SC-8, SC-13, AC-17 ISO: 8.24 CE: Secure configuration

Severity	Finding	Fix	Controls
Medium	1 VPN gateway uses IKEv1 aggressive mode "to-branch"	Aggressive mode exposes a hash of the pre-shared key that can be cracked offline. Use main mode, or better, IKEv2. (see Remediation commands)	800-53: SC-13, IA-5, AC-17 ISO: 8.24, 8.5 CE: Secure configuration
Medium	Old TLS allowed on SSL-VPN: minimum TLS version is TLS 1.1	Require TLS 1.2 or later. TLS 1.0 and 1.1 are deprecated (RFC 8996) and fail PCI DSS. (see Remediation commands)	800-53: SC-8, SC-13 ISO: 8.24 CE: Secure configuration
Low	Very broad source in an allow rule Rule "Corp to DMZ apps": source includes 10.0.0.0/8.	Use the smallest subnets or host groups that need access. (see Remediation commands)	800-53: AC-4, SC-7 ISO: 8.22 CE: Firewalls
Low	Wide port range allowed Rule "Corp to DMZ apps": tcp 8000-9999.	List the specific ports the application uses instead of a large range. (see Remediation commands)	800-53: CM-7 ISO: 8.20 CE: Firewalls
Low	The default "admin" account is still in use.	Create named admin accounts, then rename or remove "admin". (see Remediation commands)	800-53: IA-5, AC-2 ISO: 5.17 CE: Secure configuration
Low	SSL-VPN is enabled on internet-facing interface wan1.	SSL-VPN has been the most-exploited part of FortiGate for years, and Fortinet is moving customers to IPsec VPN. Keep firmware current, require MFA for VPN users, and limit source countries or addresses. (see Remediation commands)	800-53: AC-17, SC-7 ISO: 8.20 CE: Firewalls
Low	1 VPN proposal uses SHA-1 IPsec "to-branch-p2": SHA-1	Use AES-256 (or AES-GCM), SHA-256 or better, and DH group 14, 19, 20 or 21. Change both ends of each tunnel in the same window. (see Remediation commands)	800-53: SC-8, SC-13, AC-17 ISO: 8.24 CE: Secure configuration
Low	1 VPN uses IKEv1 "to-branch"	IKEv1 is deprecated (RFC 9395). Move tunnels to IKEv2 when the other end supports it. (see Remediation commands)	800-53: SC-13, AC-17 ISO: 8.24
Low	1 IPsec tunnel without perfect forward secrecy "to-branch-p2"	Turn on PFS with DH group 14 or higher, so one stolen key can't decrypt earlier traffic. (see Remediation commands)	800-53: SC-8, SC-13 ISO: 8.24
Low	1 disabled rule left in the rulebase "Temp test"	Delete rules that are no longer needed, and record why in your change log. (see Remediation commands)	800-53: CM-6 ISO: 8.9 CE: Firewalls
Low	1 allow rule doesn't log traffic "RDP to admin PC"	Turn on logging for allow rules, at least for traffic crossing the internet edge. (see Remediation commands)	800-53: AU-2, AU-12 ISO: 8.15
Low	No explicit deny-all rule at the end Rules from wan1, internal end without a logged deny-all, so they rely on the implicit default.	Add a final "deny any any" rule with logging so dropped traffic is visible. (see Remediation commands)	800-53: SC-7(5), AU-2 ISO: 8.20 CE: Firewalls
Low	2 unused objects Addresses/groups: "WEB-01-copy", "OLD-PRINTER".	Remove objects nothing references; they make reviews slower and hide mistakes. (see Remediation commands)	800-53: CM-6 ISO: 8.9
Low	1 address value is defined more than once "WEB-01" = "WEB-01-copy".	Keep one object per address and update rules to use it.	800-53: CM-6 ISO: 8.9
Low	1 internet-bound allow rule has no security profiles "LAN out"	Attach antivirus, web filter and IPS profiles to outbound internet rules. (see Remediation commands)	800-53: SI-3, SI-4 ISO: 8.7, 8.16 CE: Malware protection
Low	2 allow rules had no hits in the last 90 days "RDP to admin PC", "Corp to DMZ apps"	Unused allow rules are open doors nobody needs. Confirm with the owner, disable for a few weeks, then delete. (see Remediation commands)	800-53: CM-7, AC-4 ISO: 8.9, 8.20 CE: Firewalls
Low	1 block rule had no hits in the last 90 days	Unused block rules usually mean the	800-53: CM-7, AC-4

Severity	Finding	Fix	Controls
	"Block bad actor"	traffic is already stopped elsewhere. Check the order, then tidy them up. (see Remediation commands)	ISO: 8.9, 8.20 CE: Firewalls
Info	Hit counts matched 5 of 6 rules. Rules without a counter weren't judged.		

Accepted risks

Severity	Finding	Reason	Review by
Low	3 rules have no comment or description	Business reasons are recorded in the change tickets for each rule (example). Accepted by it.manager@example.com	2027-04-30

Score history

Date	Grade	Score	High	Medium	Low
13/10/2026	F	0	8	8	15
13/07/2026	F	0	11	9	16

NIST SP 800-53 Rev. 5

16 fail 5 partial 2 pass 0 not assessed

Control	Requirement	Status	Findings
AC-2	Account Management	partial	1
AC-3	Access Enforcement	fail	1
AC-4	Information Flow Enforcement	fail	4
AC-17	Remote Access	fail	10
AU-2	Event Logging	partial	2
AU-6	Audit Record Review, Analysis, and Reporting	fail	1
AU-8	Time Stamps	pass	
AU-9	Protection of Audit Information	fail	1
AU-12	Audit Record Generation	partial	1
CM-6	Configuration Settings	fail	5
CM-7	Least Functionality	fail	6
IA-2(1)	Multi-factor Authentication to Privileged Accounts	fail	1
IA-5	Authenticator Management	fail	3
SA-22	Unsupported System Components	fail	1
SC-7	Boundary Protection	fail	4
SC-7(5)	Deny by Default - Allow by Exception	fail	2
SC-8	Transmission Confidentiality and Integrity	fail	6
SC-13	Cryptographic Protection	fail	6
SC-45	System Time Synchronization	pass	
RA-5	Vulnerability Monitoring and Scanning	fail	2
SI-2	Flaw Remediation	fail	3
SI-3	Malicious Code Protection	partial	1
SI-4	System Monitoring	partial	1

"Pass" means none of the related automated checks found a problem in this configuration. It is not evidence of compliance on its own. "Not assessed" controls need evidence from outside the firewall configuration. Control references are for orientation; confirm them against the current edition of the standard.

ISO/IEC 27001:2022 Annex A

8 fail 3 partial 1 pass 0 not assessed

Control	Requirement	Status	Findings
5.17	Authentication information	fail	2
8.2	Privileged access rights	fail	2
8.5	Secure authentication	fail	5
8.7	Protection against malware	partial	1
8.8	Management of technical vulnerabilities	fail	3
8.9	Configuration management	fail	7
8.15	Logging	fail	2
8.16	Monitoring activities	partial	1
8.17	Clock synchronization	pass	
8.20	Networks security	fail	9
8.22	Segregation of networks	partial	1
8.24	Use of cryptography	fail	6

"Pass" means none of the related automated checks found a problem in this configuration. It is not evidence of compliance on its own. "Not assessed" controls need evidence from outside the firewall configuration. Control references are for orientation; confirm them against the current edition of the standard.

UK Cyber Essentials

4 fail 1 partial 0 pass 0 not assessed

Control	Requirement	Status	Findings
Firewalls	Firewalls (boundary firewalls and internet gateways)	fail	12
Secure configuration	Secure configuration	fail	8
Security update management	Security update management	fail	3
User access control	User access control	fail	1
Malware protection	Malware protection	partial	1

"Pass" means none of the related automated checks found a problem in this configuration. It is not evidence of compliance on its own. "Not assessed" controls need evidence from outside the firewall configuration. Control references are for orientation; confirm them against the current edition of the standard.

Appendix: rules reviewed

#	Rule	From -> To	Source	Destination	Service	Action	Hits	Flags
1	Web in	wan1 -> dmz	all	VIP-WEB	HTTPS	allow	48211	
2	RDP to admin PC	wan1 -> internal	all	ADMIN-PC	RDP	allow	0	no log, exposed, no hits
3	LAN out	internal -> wan1	INSIDE-LAN	all	ALL	allow	1290033	all services
4	Block bad actor	internal -> wan1	INSIDE-LAN	BAD-ACTOR	ALL	deny	0	shadowed, no hits
5	Corp to DMZ apps	internal -> dmz	CORP-WIDE	DMZ-SERVERS	APP-RANGE	allow	0	broad, wide ports, no hits
6	Temp test (disabled)	internal -> dmz	all	all	ALL	allow	-	disabled

Review record

Reviewed and signed off by	it.manager@example.com
Date	13 Oct 2026, 16:31
Result at sign-off	Grade F, score 0/100; 8 high, 8 medium, 15 low
Next review due	13 Apr 2027
Notes	Example sign-off: remediation tracked in change CHG-0001.
Supports	PCI DSS v4.0.1 1.2.7 (review network security control configurations at least every six months); ISO/IEC 27001:2022 A.8.9; NIST SP 800-41 Rev. 1 section 5; CIS Controls v8.1 4.2

Appendix: remediation commands

Suggested FortiOS CLI changes for each finding. Replace values in <angle brackets>, check each change against your environment and apply it in a maintenance window. Back up the configuration first.

HIGH RDP open to any source (internet-facing)

```
config firewall policy
  edit 2
    set srcaddr "<source-address>"
  next
end
```

HIGH Intended block never happens (shadowed by an allow)

```
config firewall policy
  move 4 before 3
end
```

HIGH FortiOS 6.4.12 on FG100F is end of support and no longer gets security fixes.

```
# Upgrade from System > Firmware & Registration, following the upgrade path at
# https://docs.fortinet.com/upgrade-tool (back up the config first)
execute backup config tftp <file-name> <tftp-server-ip>
execute restore image tftp <firmware-image.out> <tftp-server-ip>
```

HIGH Admin access (https, ssh) is open on internet-facing port wan1.

```
config system interface
  edit "wan1"
    unselect allowaccess https ssh
  next
end
# If you must manage over the WAN, restrict it instead:
config firewall local-in-policy
  edit 0
    set intf "wan1"
    set srcaddr "<trusted-admin-addresses>"
    set dstaddr "all"
    set service "HTTPS" "SSH"
    set schedule "always"
    set action accept
  next
end
```

HIGH Telnet admin access is on for internal.

```
config system interface
  edit "internal"
    unselect allowaccess telnet
  next
end
```

HIGH Default SNMP community "public" is in use.

```
config system snmp community
  edit 1
    set name "<long-random-community>"
  next
end
```

HIGH FortiOS 6.4.12 is affected by known-exploited CVE-2024-21762: SSL-VPN out-of-bounds write (remote code execution)

```
# Fix: upgrade to 6.4.15 or later (System > Firmware & Registration)
execute restore image tftp <firmware-image.out> <tftp-server-ip>
# Mitigation until you can upgrade:
config vpn ssl settings
  unset source-interface
end
```

HIGH FortiOS 6.4.12 is affected by known-exploited CVE-2023-27997: SSL-VPN heap overflow before login (remote code execution)

```
# Fix: upgrade to 6.4.13 or later (System > Firmware & Registration)
execute restore image tftp <firmware-image.out> <tftp-server-ip>
# Mitigation until you can upgrade:
config vpn ssl settings
  unset source-interface
end
```

MEDIUM Rule allows every port and protocol

```
config firewall policy
  edit 3
    set service "<needed-service>"
  next
end
```

MEDIUM Admin "admin" can log in from any address (no trusted hosts).

```
config system admin
  edit "admin"
    set trusthost1 <mgmt-network> <netmask>
  next
end
```

MEDIUM 1 admin account without two-factor authentication (admin).

```
config system admin
  edit "admin"
    set two-factor email
    set email-to "<admin-email>"
  next
end
# FortiToken: set two-factor fortitoken, then set fortitoken <serial>
```

MEDIUM Unencrypted HTTP admin access is on for internal.

```
config system interface
  edit "internal"
    unselect allowaccess http
  next
end
```

MEDIUM No remote logging (syslog, FortiAnalyzer or FortiGuard) is turned on.

```
config log syslogd setting
  set status enable
  set server "<syslog-server-ip>"
end
```

MEDIUM 1 VPN proposal uses weak encryption or key exchange

```
config vpn ipsec phase1-interface
  edit "to-branch"
    set proposal aes256-sha256 aes128-sha256
    set dhgrp 20 19 14
  next
end
```

MEDIUM 1 VPN gateway uses IKEv1 aggressive mode

```
config vpn ipsec phase1-interface
  edit "to-branch"
    set mode main
  next
end
```

MEDIUM Old TLS allowed on SSL-VPN: minimum TLS version is TLS 1.1

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

LOW Very broad source in an allow rule

```
config firewall policy
  edit 5
    set srcaddr "<source-address>"
    set dstaddr "<destination-address>"
  next
end
```

LOW Wide port range allowed

```
config firewall policy
  edit 5
    set service "<needed-service>"
  next
end
```

LOW The default "admin" account is still in use.

```
config system admin
  edit "<your-name>"
    set accprofile "super_admin"
    set password <strong-password>
    set trusthost1 <mgmt-network> <netmask>
  next
end
# sign in as the new admin, then:
config system admin
  delete "admin"
end
```

LOW SSL-VPN is enabled on internet-facing interface wan1.

```
config vpn ssl settings
  set source-address "<allowed-countries-or-addresses>"
end
# require two-factor for VPN users:
config user local
  edit "<vpn-user>"
    set two-factor fortitoken
  next
end
```

LOW 1 VPN proposal uses SHA-1

```
config vpn ipsec phase2-interface
  edit "to-branch-p2"
    set proposal aes256gcm aes256-sha256
    set dhgrp 20 19 14
  next
end
```

LOW 1 VPN uses IKEv1

```
config vpn ipsec phase1-interface
  edit "to-branch"
    set ike-version 2
  next
end
```

LOW 1 IPsec tunnel without perfect forward secrecy

```
config vpn ipsec phase2-interface
  edit "to-branch-p2"
    set pfs enable
    set dhgrp 20 14
  next
end
```

LOW 1 disabled rule left in the rulebase

```
config firewall policy
  delete 6
end
```

LOW 1 allow rule doesn't log traffic

```
config firewall policy
  edit 2
    set logtraffic all
  next
end
```

LOW No explicit deny-all rule at the end

```
config log setting
  set fwpolicy-implicit-log enable
end
# or an explicit, logged deny at the bottom of each interface pair:
config firewall policy
  edit 0
    set name "deny-all-log"
    set srcintf "wan1"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "all"
    set service "ALL"
    set schedule "always"
    set action deny
```

```
        set logtraffic all
    next
end
```

LOW 2 unused objects

```
config firewall address
    delete "WEB-01-copy"
    delete "OLD-PRINTER"
end
```

LOW 1 internet-bound allow rule has no security profiles

```
config firewall policy
    edit 3
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set webfilter-profile "default"
        set ips-sensor "default"
        set application-list "default"
    next
end
```

LOW 2 allow rules had no hits in the last 90 days

```
config firewall policy
    delete 2
    delete 5
end
```

LOW 1 block rule had no hits in the last 90 days

```
config firewall policy
    delete 4
end
```

About this report

Known-exploited vulnerability checks use a curated list of CISA KEV entries that can be judged from a configuration export, updated 2026-10-13; check the vendor's advisories for newer issues. Suggested remediation commands are a starting point and must be reviewed before use. This report was produced by automated analysis of a firewall configuration, carried out in the user's web browser. The configuration was not uploaded to or stored by the service provider. Findings reflect the configuration as supplied and cannot account for compensating controls, network context or changes made since export. The report is guidance to help improve security and prepare for assessments. It is not an audit, penetration test, certification or legal advice, and it does not confirm compliance with any standard or regulation. Standard and control names are used for reference only; this report is not endorsed by any standards body or regulator.