Firewall and router review

ACME-RTR01

Cisco IOS

Client	Device type	Firmware	Reviewed on
Acme Ltd (sample data)	Router	15.4	6 November 2026

! The short version

9 things need fixing on this router, and 7 more are worth checking.

0 checks look good. Working through everything listed should take about 3.8 hours. 3 openings to the internet were found.



! Action needed	9
? Worth checking	7
✓ Looks good	0

Areas checked

Admin access — ! Action needed

3 items to fix

Passwords and accounts — ! Action needed

2 items to fix

What the internet can reach — ! Action needed

3 items to fix

Services and settings — ! Action needed

1 item to fix

Firmware and updates — ? Worth checking

1 item to check

Fix these first

1. **The admin login can be reached from the internet.** Reachable from any internet address: HTTP (Web admin page (unencrypted)); HTTPS (Web admin page); Telnet (Comman...
2. **Telnet is switched on.** Telnet admin access is enabled (Command line (unencrypted)).
3. **Nothing stops password guessing on the internet-facing login.** No account lockout or login throttling was found, and the login can be reached from the internet.
4. **A well-known default password is in use.** The password for enable, admin, line vty 0 4 is a well-known default or the same as the account name. (The passw...

and 5 more, listed later in this report

BLACKDOWN DIGITAL · SAMPLE DATA

What the internet can reach

Every port forward and inbound rule found, in plain English. Cyber Essentials asks for each one to have a documented business reason, approved by someone at the right level, and for anything no longer needed to be removed. Fill in the last column with the client, then keep this page as the record.

Type	From	To (inside)	Service	Risk	Business reason
Port forward	Anyone	192.168.10.20: 3389	Remote Desktop (RDP) (3389)	! Action needed	
Port forward	Anyone	192.168.10.30: 443	Web (HTTPS) (443)	? Worth checking	
Port forward	Anyone	192.168.10.40: 5000	NAS admin page (e.g. Synology) (5000)	! Action needed	

Who can manage the device

Service	Reachable from	Details	
HTTP	Anywhere on the internet	Web admin page (unencrypted)	! Action needed
HTTPS	Anywhere on the internet	Web admin page	! Action needed
Telnet	Anywhere on the internet	Command line (unencrypted)	! Action needed
SSH	Anywhere on the internet	Command line	! Action needed

Accounts

Account	Level	How the password is stored	Password	Notes
enable	15	Plain text (readable)	A well-known default	Enable password
admin	15	Scrambled, but reversible	A well-known default	
support	15	Old hash (weak)		
line vty 0 4		Scrambled, but reversible	A well-known default	Line password

Passwords are never shown. Where the file holds a readable or reversible password, only its length, and whether it is a well-known default, are reported.

BLACKDOWN DIGITAL · SAMPLE DATA

What to do next

Start with the items marked **Action needed**. Each one explains what was found in the configuration, why it matters for Cyber Essentials, and what to do. The configuration lines are shown with passwords and keys hidden.

1 The admin login can be reached from the internet

! Action needed

Admin access · Firewalls · About 20 minutes

What we found

Reachable from any internet address: HTTP (Web admin page (unencrypted)); HTTPS (Web admin page); Telnet (Command line (unencrypted)); SSH (Command line).

```
line 43ip http server
line 44ip http secure-server
line 69transport input telnet ssh
```

Why it matters

Cyber Essentials does not allow the admin interface of a firewall or router to be open to the internet unless there is a business need, and then it must be protected by multi-factor authentication or limited to known addresses. Admin logins open to the internet are scanned and attacked constantly.

What to do

Turn off admin access on the internet side, or limit it to your own fixed addresses, and manage the device from inside the network or over the VPN. Remove "0.0.0.0 0.0.0.0 outside" from the http/ssh/telnet lines (ASA), or add an inbound access list or zone-based firewall on the internet interface and "access-class" on the vty lines (IOS).

2 Telnet is switched on

! Action needed

Admin access · Firewalls · About 10 minutes

What we found

Telnet admin access is enabled (Command line (unencrypted)).

```
line 69transport input telnet ssh
```

Why it matters

Telnet sends the admin username and password across the network unencrypted, where they can be read.

What to do

Turn Telnet off and use SSH. Use "transport input ssh" on the vty lines and "no ip telnet server" where supported.

3 Nothing stops password guessing on the internet-facing login

! Action needed

Admin access · Firewalls · About 10 minutes

What we found

No account lockout or login throttling was found, and the login can be reached from the internet.

Why it matters

Cyber Essentials requires protection against brute-force password guessing (locking after no more than 10 attempts, or throttling) for logins on the internet.

What to do

Turn on login lockout or throttling, and ideally remove the login from the internet altogether.

BLACKDOWN DIGITAL · SAMPLE DATA

4 A well-known default password is in use

! Action needed

Passwords and accounts · User access control · About 10 minutes

What we found

The password for enable, admin, line vty 0 4 is a well-known default or the same as the account name. (The password itself is not shown.)

```
line 17enable password [hidden]
line 27username admin privilege 15 password [hidden]
line 67password [hidden]
```

Why it matters

Cyber Essentials requires default passwords to be changed. Default passwords are the first thing attackers try.

What to do

Change it to a long, unique password (at least 12 characters) and keep it in a password manager.

5 Passwords are stored in a readable form

! Action needed

Passwords and accounts · User access control · About 20 minutes

What we found

enable (plain text), admin (reversible scrambling, e.g. Cisco type 7), line vty 0 4 (reversible scrambling, e.g. Cisco type 7). Anyone with a copy of this file can recover them.

```
line 17enable password [hidden]
line 27username admin privilege 15 password [hidden]
line 67password [hidden]
```

Why it matters

Configuration backups get copied, emailed and stored in many places; readable passwords in them give away the keys to the network.

What to do

Store passwords with a strong one-way hash (for Cisco: "enable secret" / "username ... secret" with algorithm-type scrypt; elsewhere the "hash" or "irreversible" option), then change the passwords, as the old ones are now known.

6 Remote Desktop (RDP) (3389) is open to the internet

! Action needed

What the internet can reach · Firewalls · About 20 minutes

What we found

Anyone on the internet can reach 192.168.10.20:3389 on Remote Desktop (RDP) (3389) (port forward).

```
line 47ip nat inside source static tcp 192.168.10.20 3389 interface GigabitEthernet0/0
3389
```

Why it matters

Services like this are scanned for and attacked within minutes of being exposed. Cyber Essentials only allows inbound access that has a documented business need, and services that are not protected by a login must not be exposed at all.

What to do

Remove the rule. If remote access is needed, use a VPN with multi-factor authentication, or limit the rule to known source addresses.

BLACKDOWN DIGITAL · SAMPLE DATA

7 NAS admin page (e.g. Synology) (5000) is open to the internet

! Action needed

What the internet can reach · Firewalls · About 20 minutes

What we found

Anyone on the internet can reach 192.168.10.40:5000 on NAS admin page (e.g. Synology) (5000) (port forward).

```
line 49ip nat inside source static tcp 192.168.10.40 5000 interface GigabitEthernet0/0
5000
```

Why it matters

Services like this are scanned for and attacked within minutes of being exposed. Cyber Essentials only allows inbound access that has a documented business need, and services that are not protected by a login must not be exposed at all.

What to do

Remove the rule. If remote access is needed, use a VPN with multi-factor authentication, or limit the rule to known source addresses.

8 SNMP uses a default or writable community

! Action needed

Services and settings · Secure configuration · About 10 minutes

What we found

SNMP with a default community name (such as "public"); with write access is configured. (Community names are hidden in this report.)

```
line 54snmp-server community [hidden] RO
line 55snmp-server community [hidden] RW
```

Why it matters

SNMP communities act like passwords. Default ones are guessed instantly, and write access lets someone change the device's settings.

What to do

Remove default and write communities. Use SNMP version 3 with authentication and encryption, or turn SNMP off if nothing uses it. Remove the community ("no snmp-server community <name>") and use SNMP version 3 with authentication and encryption, or turn SNMP off if nothing uses it.

9 No firewall rules on the internet connection

! Action needed

What the internet can reach · Firewalls · About 15 minutes

What we found

The internet-facing interface (GigabitEthernet0/0) has no inbound access list and the router does not use the zone-based firewall.

Why it matters

Cyber Essentials needs a firewall that blocks unrequested connections from the internet. Address translation (NAT) on its own is not a firewall, and the router's own services (web admin, SSH) are open to the internet.

What to do

Configure the IOS zone-based firewall, or an inbound access list on the internet interface that permits only return traffic and the services you have a documented reason for.

BLACKDOWN DIGITAL · SAMPLE DATA

10 The admin page also works without encryption

? Worth checking

Admin access · Firewalls · About 10 minutes

What we found HTTP admin access is enabled (Web admin page (unencrypted)).

```
line 43ip http server
```

Why it matters Over plain HTTP or FTP the admin password crosses the network unencrypted.

What to do Use HTTPS only (or let HTTP just redirect to HTTPS). Use "no ip http server" and keep "ip http secure-server".

11 Admin sessions never time out

? Worth checking

Admin access · Firewalls · About 5 minutes

What we found An admin login stays open indefinitely when left unattended.

```
line 65 exec-timeout 0 0
```

Why it matters A session left signed in can be used by anyone with access to that computer.

What to do Set an idle timeout of 10 to 15 minutes.

12 Passwords use an old, weak hashing method

? Worth checking

Passwords and accounts · User access control · About 10 minutes

What we found support use an older hash (such as MD5) that can be cracked quickly if the file is leaked.

```
line 28username support privilege 15 secret [hidden]
```

Why it matters A leaked configuration would let an attacker work out short or common passwords.

What to do Re-enter these passwords so the device stores them with its strongest option (for Cisco: "algorithm-type scrypt", type 9).

13 Each opening to the internet needs a written business reason

? Worth checking

What the internet can reach · Firewalls · About 15 minutes

What we found 1 service is reachable from the internet: Web (HTTPS) (443) to 192.168.10.30:443.

```
line 48ip nat inside source static tcp 192.168.10.30 443 interface GigabitEthernet0/0 443
```

Why it matters Cyber Essentials requires every inbound rule to be documented and approved by someone at the right level, with a business reason, and removed when no longer needed.

What to do Fill in the "Business reason" column in the table "What the internet can reach" and remove anything nobody can justify.

BLACKDOWN DIGITAL · SAMPLE DATA

14 The VPN allows old encryption

? Worth checking

Services and settings · Secure configuration · About 30 minutes

What we found

IPsec VPN uses old encryption (DES/3DES, MD5 or Diffie-Hellman group 1/2).

```
line 58 encr 3des
line 59 hash md5
line 61 group 2
```

Why it matters

Old algorithms make VPN traffic easier to break.

What to do

Use AES with SHA-256 or better and Diffie-Hellman group 14 or higher, on both ends of the VPN.

15 Confirm the firmware is the latest supported version

? Worth checking

Firmware and updates · Security update management · About 20 minutes

What we found

The configuration was saved by 15.4.

Why it matters

Cyber Essentials requires firmware to be supported by the maker and updated within 14 days of a high or critical security fix.

What to do

Check Cisco's website or the device's update page for a newer release, and turn on automatic updates where available.

16 Password encryption service is off

? Worth checking

Passwords and accounts · User access control · About 5 minutes

What we found

"service password-encryption" is not set, so line passwords are kept in plain text.

Why it matters

It at least stops passwords being read over someone's shoulder.

What to do

Add "service password-encryption", and use "secret" rather than "password" for accounts.

Good practice

– Good practice

Logs are only kept on the device

No remote syslog or log server is configured. Consider sending logs to a log server or cloud logging service.

BLACKDOWN DIGITAL · SAMPLE DATA

Help with the firewall questions

Draft answers for the boundary firewall and router questions in the Cyber Essentials self-assessment (section A4), based on this review. The client must check each one and answer for themselves.

Question (in summary)	Status	Draft answer
Has the default password been changed on the router/firewall?	! Not yet	No. A default password is still in use; change it first.
Does the new password meet the password requirements?	? Confirm	Confirm it is at least 12 characters (or 8 with multi-factor authentication).
Can the firewall's admin interface be reached from the internet?	! Not yet	Yes, and it is not protected enough. Remove it from the internet (or add MFA / an address allow-list) first.
Are inbound firewall rules approved and documented with a business reason?	! Not yet	Not yet. Remove the risky openings listed in this report first, then document the rest.
Are rules that are no longer needed removed or disabled promptly?	? Confirm	Yes, once nobody can justify any rule that is left. Review the rules at least once a year.
Is the firewall's software supported and kept up to date?	? Confirm	Confirm it is the latest supported version and that updates are applied within 14 days.

About this review

Device	Cisco IOS
Configuration file	cisco-ios-office-router.txt (2 KB, last changed 6 Nov 2026, 11:32 UTC)
File fingerprint (SHA-256)	`35268d03f3247d8a85e3335fb6b06f06ce2bf125d91c9cf2e8b2303934843bbf`
Reviewed	6 Nov 2026, 19:52 UTC on vm, by the Blackdown Digital Config Review 1.10.0.0

This review was made from the configuration file alone, on this computer: nothing connected to the device or the client's network. Passwords, keys, hashes and SNMP community names are hidden in this report, but the configuration file itself contains them, so store it securely. Settings changed since the file was saved, and settings the maker keeps outside the configuration (for example cloud-managed features), are not covered. This is a readiness aid, not a Cyber Essentials certificate. The fingerprint above identifies the exact file reviewed.

BLACKDOWN DIGITAL · SAMPLE DATA