Troubleshoot tunnel health

This guide helps you diagnose and resolve common tunnel health issues with Cloudflare WAN. Tunnel health checks monitor your GRE and IPsec tunnel endpoints (also called connectors in the Cloudflare dashboard) and steer traffic to the best available routes.

Quick diagnostic checklist

Use the following table to match your symptom to the most likely cause and first action:

Symptom	Most likely cause	First action
Tunnel shows Down, never becomes healthy	Configuration mismatch or firewall blocking IKE	Check IPsec parameters and firewall rules. Refer to IPsec tunnel establishment failures.
Dashboard shows "100% degraded" for some colos	Normal — this is a state indicator, not packet loss	Check if affected colos carry your traffic. Refer to Understanding degraded status.
Tunnel flaps between healthy and unhealthy	Anti-replay protection or rekey disruption	Disable anti-replay protection on your router. Refer to IPsec tunnel instability.
Health checks fail but traffic flows normally	Stateful firewall dropping health check probes	Change health check type from *Reply* to *Request*. Refer to Tunnel shows Down but traffic is flowing.
Health checks fail on policy-based VPN tunnels	Reply health checks fall outside tunnel traffic selectors	Use Request-style health checks with a loopback target. Refer to

		Policy-based VPN health check failures.
All tunnels degraded or down in a specific region	Network path issue between that region and your network	Check ISP connectivity. Use traceroute or MTR from your tunnel endpoint toward Cloudflare.
All tunnels degraded or down globally	Issue at your network edge	Check your tunnel endpoint router and upstream connectivity.

What you can check

- **Dashboard**: Tunnel health status per data center and traffic volume per tunnel (Go to **Insights** > **Network health** > **Network health**)
- **API**: Tunnel health status via the Cloudflare WAN tunnel health API
- **Network Analytics**: Traffic volume, packet counts, and protocol distribution through Network Analytics
- **From your network**: Traceroute and MTR from your tunnel endpoint toward Cloudflare. Since Cloudflare endpoints use anycast, this tests the path to the nearest data center only. To test specific regions, use the Cloudflare Traceroute API to run traceroutes from specific Cloudflare locations to your network.

What you cannot check (current limitations)

- Correlation between tunnel health events and Cloudflare network incidents
- Per-packet forwarding decisions (which data center forwarded which packet through which tunnel)
- Historical health check probe data beyond the dashboard retention period

Common fixes checklist

If you are experiencing tunnel health issues, check these items first:

1. **Health check type**: If using a stateful firewall (such as Palo Alto Networks, Check Point, Cisco, or Fortinet), change health check type from *Reply* to *Request*.
2. **Anti-replay protection**: Disable anti-replay protection on your router, or set the replay window to `0`.
3. **MTU settings**: Verify MTU is set correctly (typically `1476` for GRE, `1400`-`1450` for IPsec).
4. **IPsec parameters**: Confirm your cryptographic parameters match Cloudflare's supported configuration.
5. **Health check direction**: Cloudflare WAN defaults to *Bidirectional*.
6. **Cloudflare Network Firewall rules (less common)**: Ensure ICMP traffic from Cloudflare IP addresses ↗ is allowed.

Tunnel health states

The Network health ↗ page in the Cloudflare dashboard displays three tunnel health states:

State	Dashboard display	Technical threshold
Healthy	More than 80% of health checks pass	Less than 0.1% failure rate
Degraded	Between 40% and 80% of health checks pass	At least 0.1% failures in last five minutes (minimum two failures)
Down	Less than 40% of health checks pass	All health checks failed (at least three samples in last second)

The dashboard shows tunnel health as measured from each Cloudflare data center where your traffic lands. It is normal to see some locations reporting degraded status due to Internet path issues. Focus on locations that show traffic in the **Traffic volume (1h)** column.

Understanding degraded status in the dashboard

The tunnel health dashboard reports health state per data center per tunnel. Each Cloudflare data center independently tracks the health of each tunnel.

A common source of confusion is seeing "100% degraded" in the dashboard and misinterpreting it as 100% packet loss. Note that these are different.

How degraded state is triggered:

When a health check probe fails, Cloudflare sends two additional probes. If some probes succeed and some fail, the tunnel enters degraded state for that data center. A few seconds of intermittent packet loss is enough to trigger this transition.

What to check:

Focus on data centers that show traffic in the **Traffic volume (1h)** column. A data center showing degraded status with zero or minimal traffic is informational — it indicates a path issue between that specific Cloudflare data center and your network, but it does not affect your traffic if no traffic routes through that data center.

Recovery timing:

Tunnels remain in degraded state for at least five minutes, even if health checks start succeeding immediately. Recovery from degraded to healthy requires consistently passing health checks over a sustained period and can take up to 30 minutes. For details on how tunnels transition between states, refer to Recovery behavior below.

Routing priority penalties

When a tunnel becomes unhealthy, Cloudflare applies priority penalties to routes through that tunnel:

- **Degraded**: Adds `500,000` to route priority
- **Down**: Adds `1,000,000` to route priority

These penalties shift traffic to healthier tunnels while maintaining redundancy. Cloudflare never completely removes routes, preserving failover options even when all tunnels are unhealthy.

Recovery behavior

Tunnels transition between states asymmetrically to prevent flapping:

- **Healthy to Degraded/Down**: Transitions quickly when failures are detected. A tunnel can go directly from Healthy to Down if all probe retries fail.
- **Down to Degraded**: Requires three consecutive successful health check probes.
- **Degraded to Healthy**: Requires failure rate below 0.1% over 30 consecutive probes.

For instructions on monitoring tunnel status, refer to Check tunnel health in the dashboard.

Health check types and directions

Health check type:

Type	Behavior	When to use
Reply (default)	Cloudflare sends an ICMP reply packet	Simple networks without stateful firewalls
Request	Cloudflare sends an ICMP echo request	Networks with stateful firewalls (recommended for most deployments)

Health check direction:

Direction	Behavior	Default for
Bidirectional	Probe and response both traverse the tunnel	Cloudflare WAN (formerly Magic WAN)
Unidirectional	Probe traverses tunnel; response returns via Internet	Magic Transit (direct server return)

Resolve common issues

Tunnel shows `Down` but traffic is flowing

Symptoms

- Dashboard shows tunnel as `Down` or `Degraded`
- Actual user traffic passes through the tunnel successfully
- Health check failure rate is 100% despite working connectivity

Cause

Stateful firewalls (such as Palo Alto Networks, Check Point, Cisco, and Fortinet) drop the health check packets. By default, Cloudflare sends ICMP *Reply* packets as health check probes.

Stateful firewalls inspect these packets and look for a matching ICMP *Request* in their session table. When no matching request exists, firewalls drop the reply as "out-of-state".

Solution

Change the health check type from *Reply* to *Request*:

1. Go to the **Connectors** page.

   Go to Connectors ↗

2. In **IPsec/GRE tunnels**, select **Edit** on the affected tunnel.

3. Under **Health check type**, change from *Reply* to *Request*.

4. Select **Update tunnel**.

When you use *Request* style health checks, Cloudflare sends an ICMP echo request. Your firewall's stateful inspection engine recognizes this as a legitimate request and

automatically permits the ICMP reply response.

Health check failures with Cloudflare Network Firewall

Symptoms

- Tunnels were healthy before enabling Cloudflare Network Firewall
- After adding Cloudflare Network Firewall rules, health checks fail
- Blocking ICMP traffic causes immediate health check failures

Cause

Cloudflare Network Firewall processes all traffic, including Cloudflare's health check probes. If you create a rule that blocks ICMP traffic, you also block the health check packets that Cloudflare sends to monitor tunnel status.

Solution

Add an allow rule for ICMP traffic from Cloudflare IP addresses *before* any block rules:

1. Go to the **Firewall policies** page.

   Go to Firewall policies ↗

2. Create a new policy with the following parameters:

Field	Value
Action	Allow
Protocol	ICMP
Source	Cloudflare IP ranges ↗

3. Position this rule *before* any rules that block ICMP traffic.

For more information, refer to Cloudflare Network Firewall rules and endpoint health checks.

IPsec tunnel instability or packet drops

Symptoms

- IPsec tunnel frequently flaps between healthy and down states
- Intermittent packet loss on the tunnel
- Traffic works for a period then stops without configuration changes
- Router logs show packets dropped due to:
  - "replay check failed"
  - "invalid sequence number"
  - "invalid SPI" (Security Parameter Index)

Cause

Anti-replay protection is enabled on your router. IPsec anti-replay protection expects packets to arrive in sequence from a single sender.

Cloudflare's anycast architecture means your tunnel traffic can originate from thousands of servers across hundreds of data centers. Each server maintains its own sequence counter, causing packets to arrive out-of-order from your router's perspective.

Solution

Disable anti-replay protection on your router:

For most routers:

Locate the anti-replay or replay protection setting in your IPsec configuration and disable it.

If you can only set a replay window size:

Set the replay window to `0` to effectively disable the check.

For devices that do not support disabling anti-replay:

Enable replay protection in the Cloudflare dashboard. This routes all tunnel traffic through a single server, maintaining proper sequence numbers at the cost of losing anycast benefits.

1. Go to the **Connectors** page.

   Go to Connectors ↗

2. In **IPsec/GRE tunnels**, select **Edit** on your IPsec tunnel.

3. Enable **Replay protection**.

4. Select **Update tunnel**.

For Cisco IOS/IOS-XE routers experiencing "invalid SPI" errors:

Enable ISAKMP invalid SPI recovery to help the router resynchronize Security Associations:

```
configure terminal
crypto isakmp invalid-spi-recovery
exit
```

For a detailed explanation of why this setting is necessary, refer to Anti-replay protection.

Tunnel degraded after rekey events

Symptoms

- Tunnel health drops to `Degraded` or `Down` periodically
- Issues coincide with IPsec rekey intervals (typically every few hours)
- Tunnel recovers automatically after 1-3 minutes
- Router logs show successful rekey completion

Cause

When your tunnel endpoint initiates an IPsec rekey, new Security Associations (SAs) must propagate across Cloudflare's network. Rekey propagation delays have been significantly reduced and are uncommon in most deployments. However, brief tunnel degradation during rekeys can still occur in some configurations.

Cloudflare never initiates rekey — only responds. All rekey attempts must come from your tunnel endpoint. If your device receives a TEMPORARY_FAILURE response during rekey, it must re-establish the IKE session to recover.

Solution

This behavior is expected and the tunnel will automatically recover. To minimize impact:

1. **Configure Dead Peer Detection (DPD) with restart**: Set your tunnel endpoint's DPD action to "restart" so it automatically re-establishes the IKE session if a rekey fails with TEMPORARY_FAILURE. Without DPD restart, the device can get stuck in a loop of failed rekeys.

2. **Increase rekey intervals**: Configure longer SA lifetimes on your tunnel endpoint to reduce rekey frequency. Common values are 8-24 hours for IKE SA and 1-8 hours for IPsec SA.

3. **Adjust health check sensitivity**: If brief degradation during rekeys triggers alerts, consider lowering the health check rate:

    1. Go to the **Connectors** page.

    Go to Connectors ↗

2. In **IPsec/GRE tunnels**, select **Edit** on the tunnel.
3. Change **Health check rate** to *Low*.

4. **Stagger rekey times**: If you have multiple tunnels, configure different SA lifetimes so they do not rekey simultaneously.

Bidirectional health check failures

Symptoms

- Health checks configured as bidirectional fail consistently
- Unidirectional health checks work correctly
- Traffic flows through the tunnel normally

Cause

Bidirectional health checks require both the probe and response to traverse the tunnel. Your router must:

1. Accept ICMP packets destined for the tunnel interface IP addresses
2. Route the ICMP response back through the tunnel to Cloudflare

If traffic selectors or firewall rules do not permit this traffic, bidirectional health checks fail.

Solution

For IPsec tunnels:

Configure traffic selectors to accept packets for the tunnel interface addresses. For example, if your tunnel interface address is `10.252.2.27/31`:

- Permit traffic to/from `10.252.2.26` (Cloudflare side)
- Permit traffic to/from `10.252.2.27` (your side)

For all tunnel types:

Ensure your firewall permits ICMP traffic on the tunnel interface. Many firewalls require explicit rules to allow management traffic (including ping) on tunnel interfaces.

For detailed information on how bidirectional health checks work, refer to Tunnel health checks.

IPsec tunnel establishment failures

Symptoms

- Tunnel status shows `Down` and never becomes healthy
- No traffic passes through the tunnel
- Router logs show IKE negotiation failures

Cause

IPsec tunnel establishment can fail due to several configuration mismatches:

Issue	Symptom
Crypto parameter mismatch	IKE negotiation fails with "no proposal chosen"
Incorrect PSK	Authentication failures in Phase 1
Wrong IKE ID format	Authentication failures despite correct PSK
Firewall blocking IKE	No IKE traffic reaches Cloudflare

Solution

1. **Verify crypto parameters match Cloudflare's supported configuration:**

   Phase 1 (IKE)

Parameter	Supported values
IKE version	IKEv2 only
Encryption	AES-GCM-16, AES-CBC-256
Authentication	SHA-256, SHA-384, SHA-512
DH Group	DH group 14, 15, 16, 19, 20

Phase 2 (IPsec)

Parameter	Supported values
Encryption	AES-GCM-16, AES-CBC-256
Authentication	SHA-256, SHA-512
PFS Group	DH group 14, 15, 16, 19, 20

2. **Verify the Pre-Shared Key (PSK):**

   - Regenerate the PSK in the Cloudflare dashboard
   - Copy the new PSK exactly (no extra spaces or characters)
   - Update your router with the new PSK

3. **Check the IKE ID format:** Cloudflare uses FQDN format for the IKE ID. Ensure your router is configured to accept an FQDN peer identity. The FQDN is displayed in the tunnel details in the Cloudflare dashboard.

4. **Verify firewall rules:** Ensure your edge firewall permits:

   - UDP port `500` (IKE)
   - UDP port `4500` (IKE NAT-T)
   - IP protocol `50` (ESP)

For the complete list of supported parameters, refer to Supported configuration parameters.

Policy-based VPN health check failures

Symptoms

- Health checks fail consistently on policy-based IPsec tunnels
- Traffic matching the tunnel's traffic selectors (encryption domain) flows normally
- Route-based tunnels on the same device work correctly

Cause

Policy-based IPsec tunnels use traffic selectors to define which prefixes are permitted in the tunnel. Reply-style health checks are self-addressed to Cloudflare IP addresses. These addresses fall outside the tunnel's traffic selectors (which only permit customer network destinations), so the tunnel endpoint drops the health check packets.

Additionally, some firewalls (such as Check Point) may flag Reply-style health check packets as spoofed due to their self-addressed nature, even on route-based tunnels.

Solution

1. Change the health check type from *Reply* to *Request*.
2. Configure a loopback address on your tunnel endpoint as the health check target. The target must be:
    - Routable from the tunnel endpoint
    - Covered by the tunnel's traffic selectors (encryption domain)
3. For bidirectional health checks, ensure the health check source (the tunnel Interface Address configured in the Cloudflare dashboard) is also covered by a traffic selector.

Vendor-specific guidance

Common vendor-specific issues

Vendor	Common issue	Solution
Palo Alto Networks	Health checks fail with default settings	Change health check type to *Request*; disable anti-replay
Cisco Meraki	Cannot disable anti-replay	Enable replay protection in Cloudflare dashboard
AWS VPN Gateway	Cannot disable anti-replay	Enable replay protection in Cloudflare dashboard
VeloCloud	Cannot disable anti-replay	Enable replay protection in Cloudflare dashboard
Check Point	Out-of-state packet drops	Change health check type to *Request*

Gather information for support

If you have worked through this guide and still experience tunnel health issues, gather the following information before contacting Cloudflare support:

Required information

1. **Account ID** and **Tunnel name(s)** affected
2. **Timestamps** (in UTC) when the issue occurred
3. **Tunnel configuration details:**

- Tunnel type (GRE or IPsec)
- Health check type (Request or Reply)
- Health check direction (Bidirectional or Unidirectional)
- Health check rate (Low, Medium, or High)

4. **Router information:**

   - Vendor and model
   - Firmware/software version
   - IPsec configuration (sanitized to remove PSK)

5. **Symptoms observed:**

   - Dashboard tunnel health status
   - Whether user traffic is affected
   - Error messages from router logs

Helpful diagnostic data

- **Packet captures** from your router showing tunnel traffic
- **Router logs** covering the time period of the issue
- **Traceroute** results from your network to Cloudflare endpoints
- **Screenshots** of the tunnel health dashboard
- **Distributed traceroutes** using tools like ping.pe ↗ to test reachability from multiple global locations

Router diagnostic commands

Collect output from these commands (syntax varies by vendor):

- IPsec SA status: `show crypto ipsec sa`
- IKE SA status: `show crypto isakmp sa`
- Tunnel interface status: `show interface tunnel <number>`
- Routing table: `show ip route`

Resources

- Tunnel health checks: Technical details on health check behavior
- Anti-replay protection: Why anti-replay must be disabled
- Configure tunnel endpoints: Tunnel setup instructions
- Check tunnel health in the dashboard: Dashboard navigation guide
- Network Analytics: Traffic analysis tools