

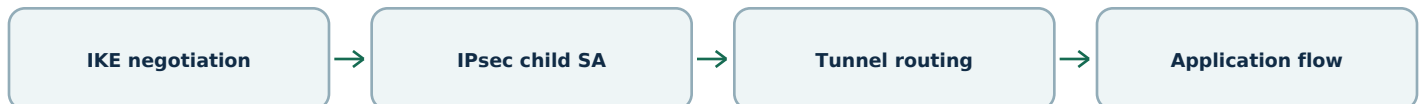
SECURITY | REV 2.0 | REVIEWED 2026-10-10

IPsec VPN: up, but traffic fails

01 / Quick reference and concepts

Separate IKE negotiation, IPsec selectors and real encrypted application traffic.

Route-based site-to-site VPN troubleshooting, PAN-OS inspection and cross-vendor workflow. IKEv1/IKEv2 and peer implementations differ.



A healthy IKE SA proves negotiation at one layer. Verify the child SA, selectors and traffic through the intended tunnel.

Layer	Inspect	Typical lead
Peer transport	Reachability / UDP 500 and 4500	NAT traversal / filtering
IKE	Identity, proposal, authentication	Mismatch or failed authentication
IPsec child SA	Transforms and traffic selectors	Proxy IDs / subnet mismatch
Routing	Destination through tunnel	Wrong VR or missing route
Policy / NAT	Intended flow permitted	Unexpected translation / deny
Traffic	Counters in both directions	Return routing / MTU / peer issue

What to understand first

- IKE establishes authenticated keying state. IPsec SAs protect selected traffic; an established IKE SA alone does not prove a useful child SA exists.
- IKEv1 proxy IDs and IKEv2 traffic selectors describe protected traffic, with negotiation differences between versions and peers. Compare local and remote definitions from both viewpoints.
- NAT traversal commonly carries IPsec over UDP 4500. Without NAT traversal, ESP uses IP protocol 50, not TCP/UDP port 50. Confirm the negotiated mode before checking filters.
- Tunnel-interface state, route selection, security policy and reverse path are independent. Overlapping networks or extra encapsulation can create failures despite healthy negotiation.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

IPsec VPN: up, but traffic fails

02 / Commands and worked example

Replace documentation addresses, example interfaces and every <PLACEHOLDER>. Check command help for your model/release and routing context. Examples are documentation-reviewed, not executed on customer equipment.

PAN-OS

Read-only operational

```
show vpn ike-sa
show vpn ipsec-sa
show vpn flow
```

Inspect: Compare gateway/tunnel identity, SA state and counter changes during one controlled attempt.

PAN-OS session inspection

Read-only operational

```
show session all filter source 198.51.100.10 destination 192.0.2.10
show session id <SESSION_ID>
```

Inspect: Check actual zones, rule, tunnel egress and translations. Use the correct vsys and routing engine context.

Illustrative one-direction VPN traffic

Illustrative teaching example, not captured device output.

```
IKE SA: established
IPsec SA: installed
During client attempt:
  Local encrypted packets: increasing
  Local decrypted packets: unchanged
```

- This narrows the investigation toward the remote path or missing return traffic; it does not prove the peer is at fault.
- Correlate peer counters, selectors, remote policy and application replies with the same timestamp and tuple.

SECURITY | REV 2.0 | REVIEWED 2026-10-10

IPsec VPN: up, but traffic fails

03 / Troubleshooting and acceptance

1. Identify the exact client/server subnets, application tuple and peer/tunnel names.
2. Check peer transport and IKE state without restarting negotiations.
3. Compare child-SA selectors and proposals at both ends.
4. Verify tunnel route, policy/NAT and return route for that flow.
5. Compare timed encrypted/decrypted counters; if transfers stall, investigate MTU and permitted ICMP feedback.

Common mistakes

- Treating a green tunnel indicator as end-to-end success.
- Bouncing every tunnel before collecting failure evidence.
- Opening ESP by port number or assuming all traffic uses NAT traversal.

Acceptance checks

- Required subnets and applications pass in both directions.
- Counters and session evidence identify the intended tunnel.
- Rekey, recovery and MTU behavior satisfy the approved acceptance plan.

Primary references

[PAN-OS networking CLI](#)[PAN-OS configuration tests](#)[PAN-OS session interpretation](#)[RFC 7296: IKEv2 and traffic selectors](#)[RFC 3948: UDP encapsulation of IPsec ESP](#)

Original Wolex diagrams, scenarios and troubleshooting sequences. Vendor names identify platform scope; no affiliation is implied.

[Read the full web guide and supporting references](#)

[Deployment and migration help](#) | [Network security review from Wolex](#)