# IPSec Tunnels Flap between Secure Access and C8000Vs Hosted in Azure/AWS

## Contents

## Issue

IPsec network tunnels between C8000V / Cisco IOS-XE routers and the Cisco Secure Access network in the us-east-2 region are flapping.

All tunnel groups are affected, resulting in tunnels being down between the on-premise routers and the Cisco Secure Access network.

## Environment

- Technology: Solution Support (SSPT - contract required)
- Subtechnology: Secure Access - Network Tunnels (IPSEC, Site-to-Site, Private Resource)
- Product Family: SECACCS
- Routers: C8000V / Cisco IOS-XE routers (on-premise)
- Remote Endpoint: Cisco Secure Access network (us-east-2 region)
- Software Version: Not specified
- Error Messages, Logs, Debugs observed
- No end users affected during the outage

## Resolution

From CNHE Splunk Logs

port =  1409

sourceIpAddr =  x.x.x.x

port =  1408

sourceIpAddr = x.x.x.x

1. Remote endpoint change was detected (port was updated)
2. Cortex triggers child rekey on this update
3. No response from client on rekeys using new port so cortex exhausts retries and terminates the tunnel
4. Shortly after client re-initiation using new port where tunnel comes up

**From CSA Splunk logs.**

```
2026-02-02T16:36:02.188+00:00 triggering child rekey for ike update with local IP: x.x.x.x, ike_spi:new_datanode:

2026-02-02T16:36:04.207+00:00 retransmit 1 of request with message ID 0
```

```
2026-02-02T16:36:08.207+00:00 retransmit 2 of request with message ID 0

2026-02-02T16:36:16.207+00:00 retransmit 3 of request with message ID 0

2026-02-02T16:36:32.207+00:00 retransmit 4 of request with message ID 0

2026-02-02T16:37:04.207+00:00 retransmit 5 of request with message ID 0

2026-02-02T16:38:08.208+00:00 giving up after 5 retransmits

2026-02-02T16:38:08.208+00:00 terminating IKE, child SA rekey failed
```

**From the debug log 1769305781091_vJY_CENTRAL_R2.log**:

Invalid SPI Errors - Occurring very frequently:

```
*Jan 24 07:55:04.209: %CRYPTO-4-
RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=x.x.x.x prot=50, spi=, srcaddr=x.x

*Jan 24 07:56:06.829: %CRYPTO-4-
RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for destaddr=x.x.x.x, prot=50, spi=, srcaddr=x.
```

Tunnel Flapping - Multiple instances of tunnels going down/up:

```
*Jan 24 08:33:12.069: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Tunnel12, changed state to down

*Jan 24 08:33:14.459: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Tunnel11, changed state to down

*Jan 24 08:33:15.275: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Tunnel11, changed state to up
```

## Cause

This seems like a flaky client issue if their port is flapping.

Flapping seems to be stable for now after making a change in Azure.

## Related Content

- Cisco Technical Support & Downloads