Secure Access IPsec Tunnel Connectivity Issue with Versa Networks Router Due to ESN Negotiation

Contents

Issue

During deployment of Cisco Secure Access at a branch office using Versa-Network Router as the edge device, connectivity issues were encountered despite both IPsec tunnels appearing operational. T

The specific symptoms included:

- No connectivity from the branch to Cisco Secure Access
- Internet access via static routes not functioning
- Unidirectional encrypted traffic observed (outbound to Secure Access only)
- Router statistics showing outbound packets being sent but no inbound packets received
- Dead peer detection functioning bidirectionally between SD-WAN router and Secure Access
- Security Parameter Index (SPI) values for outbound traffic matching correctly
- Tunnel flapping (resetting) did not resolve the connectivity issue
- Packet captures and screenshots confirmed the lack of inbound traffic
- Changing tunnel ciphers from CBC to GCM did not resolve the issue

Investigation revealed that traffic was failing to decrypt on the Cisco side due to checksum errors, which were traced to the Versa router negotiating ESN (Extended Sequence Number) functionality.

Environment

- Cisco Secure Access deployment
- Versa-Networks Router as edge device

- IP-Identity tunnel configuration
- IPsec tunnel configuration with both CBC and GCM cipher attempts

Resolution

The resolution involved disabling Extended Sequence Number (ESN) negotiation on the Versa router to prevent checksum errors that were causing decryption failures on the Cisco Secure Access head-end.

Steps to Resolve

Step 1: Identify the Root Cause

The investigation determined that the Versa router was negotiating ESN (Extended Sequence Number), which was causing the Cisco Secure Access head-end to receive checksum errors and fail to decrypt ESN-built packets.

Step 2: Disable ESN on Versa Router

Contact Versa Networks support or the router administrator to disable ESN checks and negotiation on the Versa router configuration. This addresses the known Versa bug that causes ESN to be improperly negotiated.

Step 3: Verify Connectivity

After disabling ESN negotiation, confirm that bidirectional traffic flow is established and full connectivity from the branch to Secure Access and Internet is restored.

Step 4: Monitor Traffic Flow

Verify that both inbound and outbound packet statistics on the Router show proper traffic flow in both directions, confirming successful resolution of the unidirectional traffic issue.

Cause

The root cause was identified as a known Versa Networks bug (Versa support bug ID: 122437 - ESN must not be negotiated by VOS) where the Versa router incorrectly negotiates Extended Sequence Number (ESN) functionality during IPsec tunnel establishment. This ESN negotiation causes the Cisco Secure Access head-end to receive packets with checksum errors, preventing proper decryption and resulting in unidirectional traffic flow. The Versa router sends outbound packets successfully, but the return traffic cannot be properly processed due to the ESN-related decryption failures.

Related Content

- Cisco Technical Support & Downloads