Configure SD-WAN Header Compression

For supported software information, click here.

In the Versa Operating System™ (VOS™) SD-WAN solution, the overlay and tunnel headers introduce additional overhead into packets, which can be an issue in networks in which bandwidth is expensive, such as satellite networks. To lower the packet overhead, you can use SD-WAN header compression, which provide a tunnel-free method for saving bandwidth. With SD-WAN header compression, portions of the inner headers of ESP, GRE, IPv4, IPv6, MPLS, TCP, UDP, and VXLAN packets that do not change during a flow's lifetime are omitted from the packets.

SD-WAN header compression is activated after the first few packets of a flow are exchanged between the ingress and peer SD-WAN nodes. The first packet contains all the header fields , including the flow ID selected by the ingress node. When a session is created, the fields that remain static during the flow's lifetime are stored. After the nodes on both ends learn about the flow, all subsequent packets contain only the metadata (dynamic fields), hint bits, and the flow ID. The flow ID encodes all information related to the inner packet, and it also encodes the encryption.

The VOS SD-WAN header contains three hint bits that indicate the following:

- Flow learning status
- Packet type, either compressed or uncompressed
- Fragmented inner Layer 3 packet
- Level of compression (low or high)
- Whether to skip the hash-based message authentication protocol (HMAC)

When the following conditions are met, SD-WAN header compression activates:

- Compression is enabled on both peers.
- The flow is unicast.
- The flow is either ESP, TCP, or UDP
- The IP headers have no extension headers. (Note that IPv6 fragmentation extension headers are exempt.)
- The flow is bidirectional.

There are two levels of compression:

- Low—Use when both CPU performance and bandwidth usage are minimal. This is the default compression level.
- High—Use when bandwidth usage is more important than CPU performance.

You can configure the compression level independently for each branch. For example, Branch-1 can have a low compression level, and Branch-2 can have a high compression level. In this case, Branch-2 uses more CPU, because it must decompress the packets with a high level of compression.

When traffic is directed towards an external encryption device, such as a high-assurance Internet Protocol encryptor (HAIPE), you can choose to skip the HMAC authentication to avoid double encryption. Skipping the HMAC authentication saves 16 bytes.

You enable or disable header compression at the system level. The system-level compression configuration information is sent to the peer branch as part of the branch information. Before a branch sends a compressed packet, it checks whether the peer is able to handle compressed packets. Note that when the state changes, the branch must be reset to synchronize the state with the peer branch.

To set the compression levels and whether to the skip HMAC authentication on a VOS device, you configure rules in a forwarding profile. If you do not configure a forwarding profile for a session, the default compression level is set to low and skipping the HMAC authentication is not done.

Note The header compression configuration is associated with a rule, not with a path, because if a path changes mid-flow, it is not possible to adjust the TCP maximum segment size (MSS). This scenario is an issue when the state changes from compressed to uncompressed, because the negotiated MSS cannot accommodate the uncompressed packet. For the same reason, you cannot disable compression in the middle of a session.

The peer's flow learned hint bit for the session is cleared and the flow-learning process starts from beginning as if it is the first packet of the flow in the following cases:

- Next hop changes.
- Security parameter index (SPI) is rekeyed.
- Peer's session ages out or is cleared. When the peer's session is aged out or cleared and it then receives a compressed packet, the peer's session responds with an ICMP error. When the sender receives the ICMP error, it resets the flow learned status, and then flow learning starts from beginning.

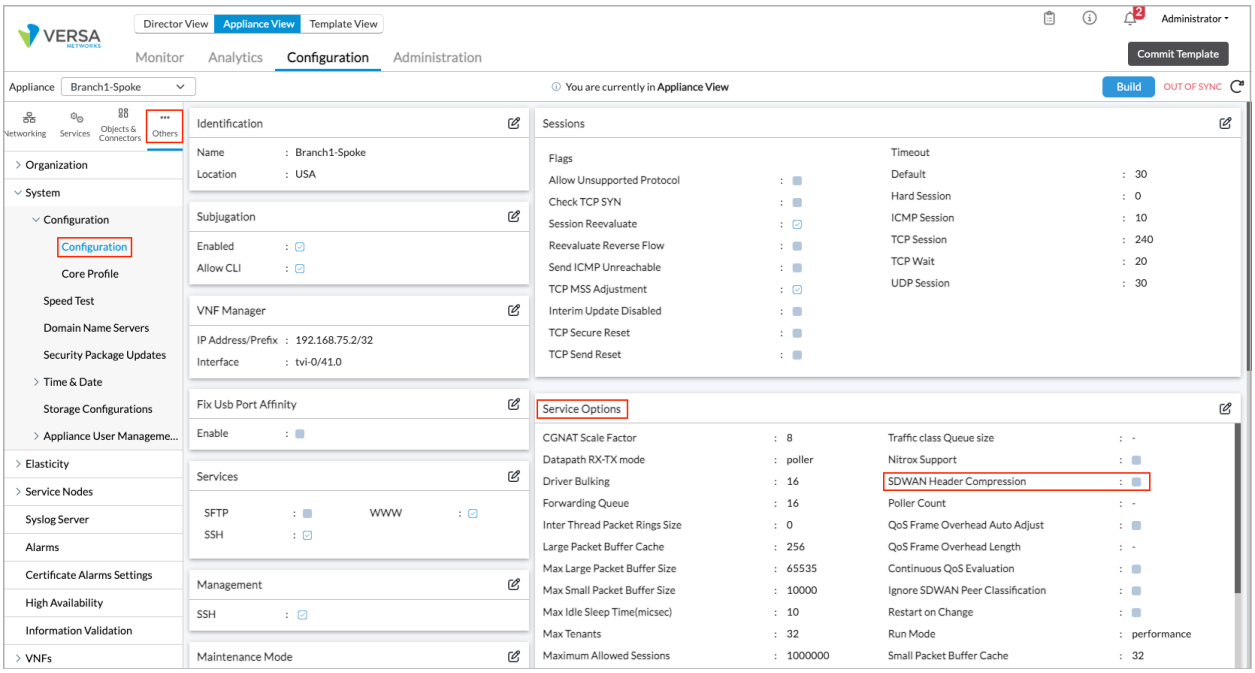
To prevent fragmentation on the tunnel interface, the VOS software adjusts the MSS in TCP SYN and SYN-ACK packets, because additional tunnel headers increase the overhead. If a flow can be compressed, the MSS is increased by 36 bytes for an IPv4 flow and by 57 bytes for an IPv6 flow.

Enable SD-WAN Header Compression

To enable SD-WAN header compression at the system level:

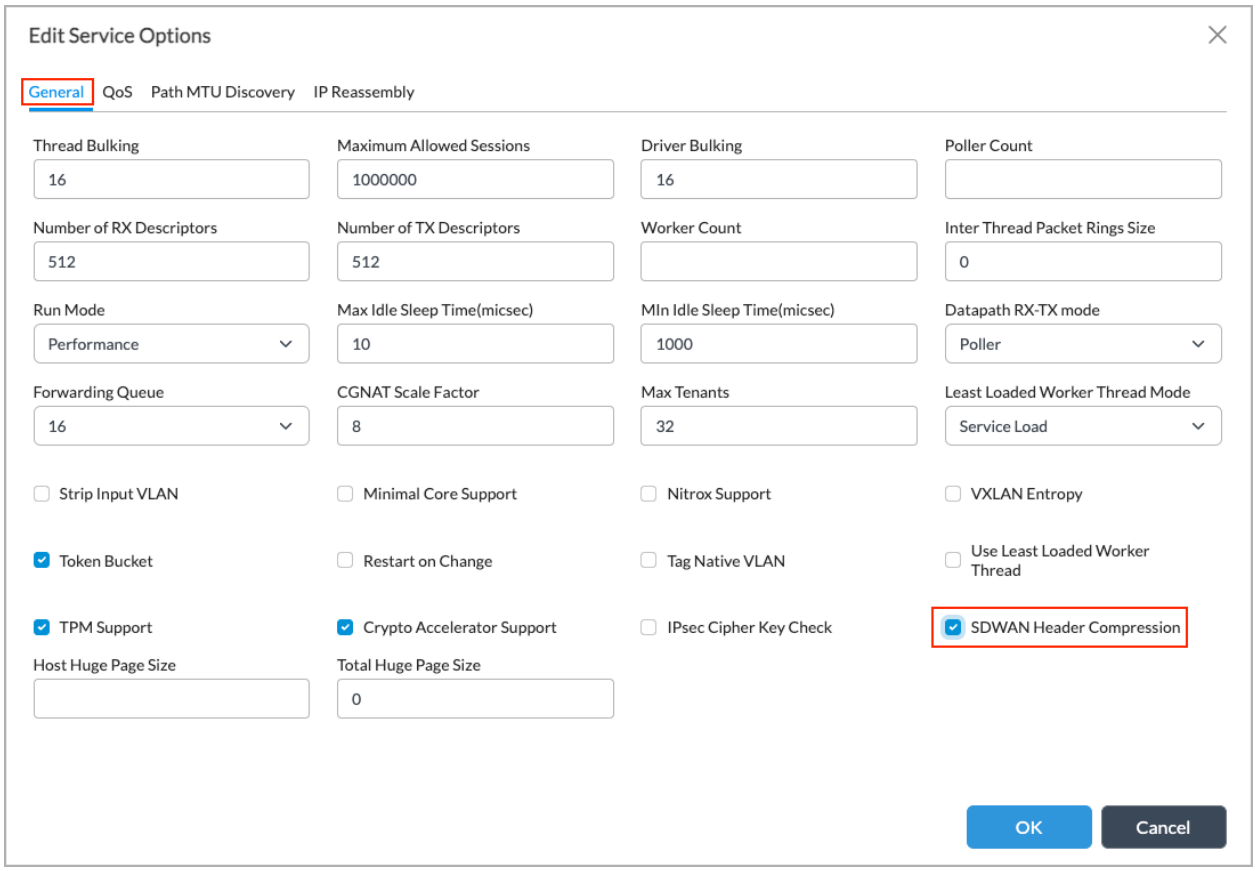
1. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

3. Select Others > System > Configuration > Configuration. The system dashboard displays.



4. In the Service Options pane, click the Edit icon. The Edit Service Option popup window displays.

Updated: Wed, 23 Oct 2024 08:10:04 GMT

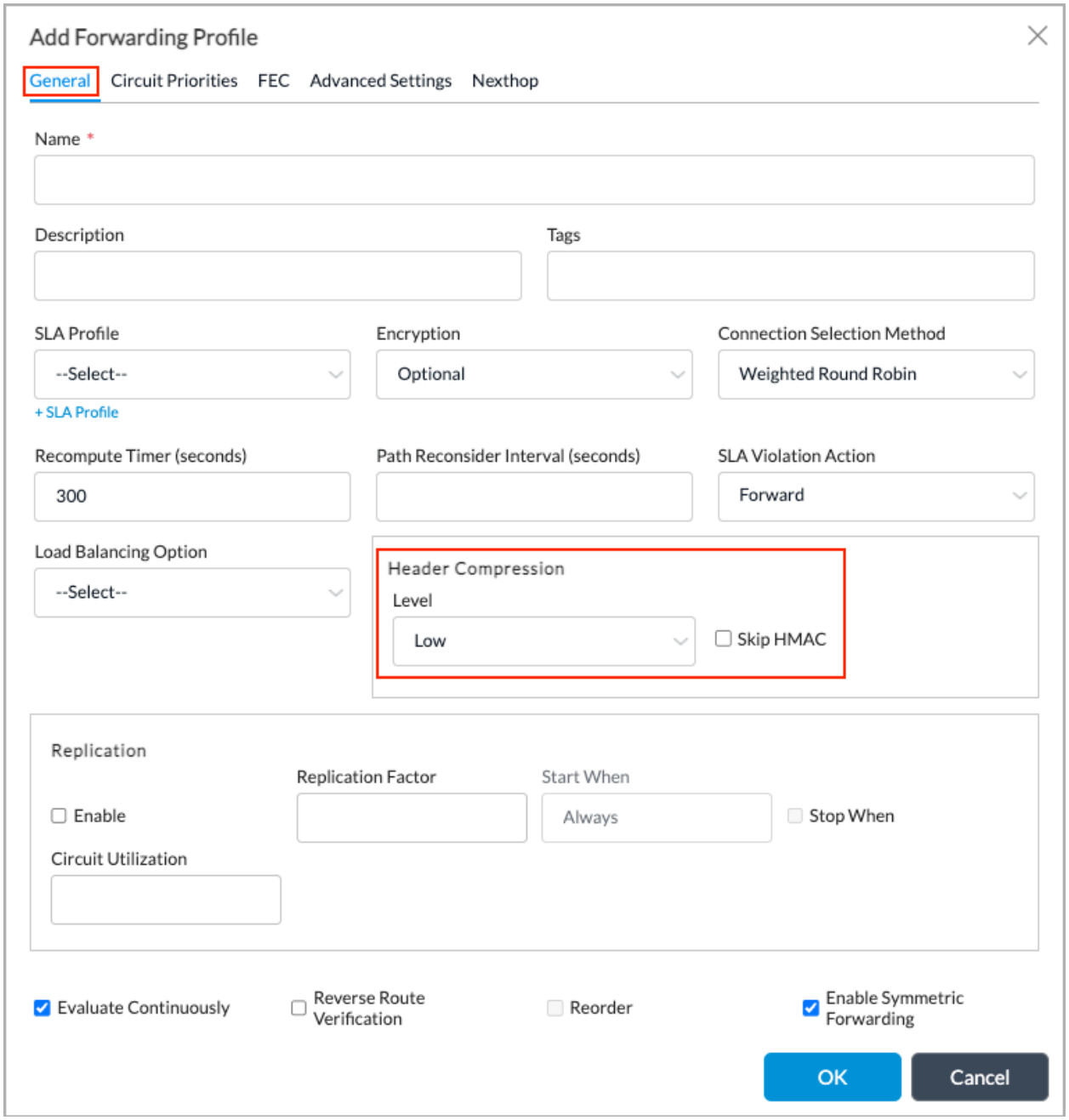


5. Select the General tab, and then click SD-WAN Header Compression to enable SD-WAN header compression at the system level.
6. Click OK.

Configure Header Compression on a VOS Device

To configure header compression in a forwarding profile and associate it with a rule:

1. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Forwarding Profiles in the left menu bar.
4. Click the Add icon or the Add button. The Add Forwarding Profile popup window displays.



5. Select the General tab.
6. In the Header Compression box, enter information for the following fields.

Field	Description
Level	Select the compression level: ◦ Low—Select when both the CPU performance

Field	Description
	and bandwidth usage are minimal. ◦ High—Select when bandwidth usage is more important than CPU performance.
Skip HMAC	Click to skip HMAC authentication.

7. Click OK.
8. Associate the forwarding profile with an SD-WAN traffic steering policy. For more information, see Configure Layer 2 or Layer 3 SD-WAN Traffic Steering Policy.

For more information about configuring forwarding profiles, see Configure SD-WAN Traffic Steering.

Software Support Information

Releases 22.1.1 and later support all content described in this article.

Additional Information

Configure SD-WAN Traffic Steering