Configure Encryption on WAN Interfaces

For supported software information, click here.

By default, site-to-site traffic is sent over a secure tunnel on the WAN interface, which performs both encryption and authentication on all traffic that is sent on the WAN access link. Encrypting traffic incurs an overhead that may be undesirable or unnecessary. One example of when encryption may be unnecessary is if the end hosts themselves use SSL to encrypt and authentication traffic. In this case, you can choose to send the traffic as plain text.

To control the WAN access link encryption for an organization, you can modify the default encryption behavior in one of the following ways:

- Modify the encryption behavior for all traffic on a specific access circuit, or path, as described in this article.
- Modify the encryption behavior for specific applications, as described in the Configure SD-WAN Traffic Steering article. Application-specific encryption behavior applies to traffic regardless of the path encryption.

It is recommended that you configure encryption by creating a forwarding profile so that the encryption applies to specific application traffic rather than to all traffic transiting a WAN access link.

Understand How WAN Interface Encryption Works

Each WAN access circuit supports the following encryption modes:

- Always—Encrypt all traffic.
- Never—Do not encrypt traffic.
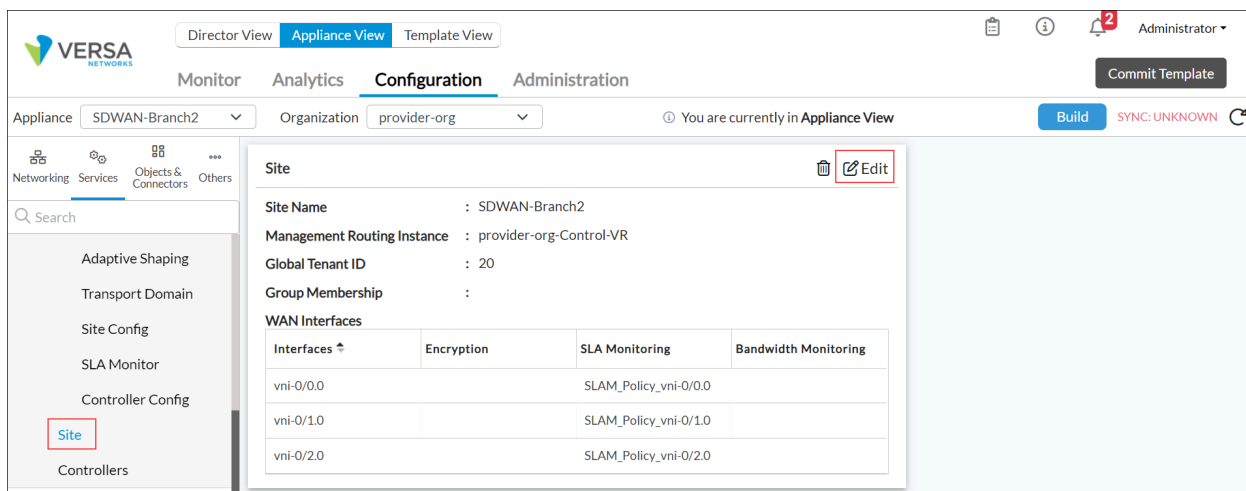- Optional—Encryption is optional.

The site-to-site path between two Versa Operating System^{TM} (VOS^{TM}) devices sends either encrypted or plain text traffic depending on how encryption is configured on the two devices at either end of the path, as described in the following table.

Local Access Circuit Encryption	Remote Access Circuit Encryption	Path Encryption
Optional	Optional	Always
Optional	Always	Always
Optional	Never	Never

Local Access Circuit Encryption	Remote Access Circuit Encryption	Path Encryption
Always	Optional	Always
Always	Always	Always
Always	Never	Always
Never	Optional	Never
Never	Always	Never
Never	Never	Never

Configure WAN Interface Encryption

1. In Director mode:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a device from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > System > Site in the left menu bar. The main pane displays a list of sites.

4. Click the ✏ Edit icon in the Site pane. The Edit Site popup window displays.

5. Click the name of the WAN interface. The Edit WAN Interfaces popup window displays.

6. In the Encryption field, select the encryption:

  ◦ Always—Encrypt all traffic.

  ◦ Never—Do not encrypt traffic.

  ◦ Optional—Encryption is optional. This is the default.

7. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure SD-WAN Traffic Steering](#)