

Configure SSL VPN Profiles

 For supported software information, click [here](#).

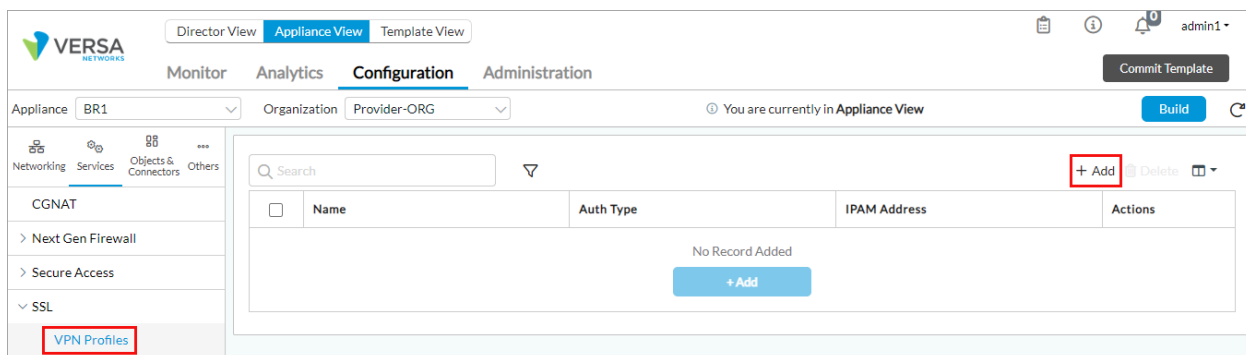
SSL VPN is an alternative to IPsec VPN for allowing remote users to connect to Versa gateways using the Versa SASE client. The Versa proprietary SSL VPN protocol is based on Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). SSL VPN generally uses port 443 to establish a secure connection with Versa gateways and ensures that you can deploy a Versa SASE client in any customer deployment.

You configure SSL VPN profiles to allow remote users to connect to an enterprise network on an SSL tunnel using a Versa SASE client. An SSL VPN profile defines the secure VPN tunnel that connects the remote user to the enterprise network.

The Versa SASE client supports IPsec VPNs and SSL VPNs to connect to a secure access gateway. For information about IPsec VPN profiles, see [Configure IPsec VPN Profiles](#).

To configure an SSL VPN profile:

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 name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > SSL > VPN Profiles in the left menu bar.



4. Click the + Add icon. The Add SSL VPN Profile popup window displays. Select the General tab, and then enter information for the following fields.

Add SSL VPN Profile

General

Address Pool

Protocol

Name *

Certificate

Certificate Name

---Please Select---

CA Chain

---Please Select---

Tunnel Routing Instance

---Please Select---

RAS ID

LEF Profile

---Please Select---

☐ LEF Profile Default

Interface List


---Please Select---

+

No Records to Display

OK

Cancel

Field	Description
Name	Enter a name for SSL VPN profile.
Certificate (Group of Fields)	
<ul style="list-style-type: none"> ◦ Certificate Name 	Select the EE certificate to use for the SSL VPN profile. For more information, see Generate CA and EE Certificates Using OpenSSL .
<ul style="list-style-type: none"> ◦ CA Chain 	Select the certificate authority (CA) chain to use.
Tunnel Routing Instance	Select the tunnel routing instance to use to reach the staging server.
RAS ID	Enter the name identifier of the remote access server (RAS) to associate with the VPN profile. For more information, see Configure a Remote Access Server .
LEF Profile	Select a log export functionality (LEF) profile to use to record logs for the SSL VPN profile.
LEF Profile Default	Click to use the default LEF profile to record logs.
Interface List	Click to select one or more interfaces for the IPsec remote access server (RAS) profile, and then click the  Add icon to add the interface. IPsec uses the RAS ID to select a VPN configuration with the same RAS ID to continue IKE negotiation. For more information, see Configure a Remote Access Server .

5. Select the Address Pool tab, and then enter information for the following field.

Add SSL VPN Profile

General

Address Pool

Protocol

IPAM Address *

---Please Select---

Accessible Subnets *


+ Add

	Subnet	Actions
No Record Added		

OK

Cancel

Field	Description
IPAM Address (Required)	Select the IP address of an IP address management (IPAM) service to assign IP addresses for SASE clients.

6. Click the + Add icon in the Accessible Subnets field to add an accessible subnet, or click the  Edit icon to modify an existing accessible subnet. The Add/Edit Accessible Subnets popup window displays.

Add Accessible Subnets

Subnet *

OK

Cancel

- a. In the Subnet field, enter the value of the subnet accessible by the SASE client. The subnet value must be in the format *mask* or *mask/length* format; for example, 192.168.2.0/24.
 - b. Click OK.
 - c. To delete an existing accessible subnet, select the subnet and then click the Delete icon.
7. Select the Protocol tab, and then enter information for the following fields.

Add SSL VPN Profile

General

Address Pool

Protocol

TLS

Min Version

---Please Select---

Max Version

---Please Select---

Port

DTLS

Min Version

---Please Select---

Max Version

---Please Select---

Port

Cipher Suites

---Please Select---

No Records to Display

OK

Cancel

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_SSL_...

Updated: Wed, 23 Oct 2024 08:23:53 GMT

Copyright © 2024, Versa Networks, Inc.

5

Field	Description
TLS (Group of Fields)	
◦ Minimum Version	Select the minimum supported version of TLS: ◦ TLS 1.2.
◦ Maximum Version	Select the maximum supported version of TLS: ◦ TLS 1.2
◦ Port	Enter the port number on which the TLS server listens for incoming connections.
DTLS (Group of Fields)	
◦ Minimum Version	Select the minimum supported version of DTLS: ◦ DTLS 1.2
◦ Maximum Version	Select the maximum supported version of DTLS: ◦ DTLS 1.2
◦ Port	Enter the port number on which the DTLS server listens for the incoming connections.
Cipher Suites	<p>Select a cipher suite, and then click Add. You can select multiple cipher suites.</p> <ul style="list-style-type: none"> ◦ TLS-AES-128-GCM-SHA256 ◦ TLS-AES-256-GCM-SHA384 ◦ TLS-CHACHA20-POLY130S-SHA256 ◦ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA ◦ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA ◦ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256 ◦ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384 ◦ TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256 ◦ TLS-ECDHE -ECDSA-WITH-AES- 256-GCM-

	<p>SHA384</p> <ul style="list-style-type: none"> ◦ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA ◦ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA ◦ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256 ◦ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384 ◦ TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256 ◦ TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384 ◦ TLS-DHE-RSA-WITH-AES-128-CBC-SHA (Unsupported) ◦ TLS-DHE-RSA-WITH-AES-256-CBC-SHA (Unsupported) ◦ TLS-DHE-RSA-WITH-AES-128-CBC-SHA256 (Unsupported) ◦ TLS-DHE-RSA-WITH-AES-256-CBC-SHA256 (Unsupported) ◦ TLS-DHE-RSA-WITH-AES-256-GCM-SHA384 (Unsupported) ◦ TLS-RSA-WITH-AES-128-CBC-SHA ◦ TLS-RSA-WITH-AES-256-CBC-SHA ◦ TLS-RSA-WITH-AES-128-CBC-SHA256 ◦ TLS-RSA-WITH-AES-256-CBC-SHA256 ◦ TLS-RSA-WITH-AES-128-GCM-SHA256 ◦ TLS-RSA-WITH-AES-256-GCM-SHA384 ◦ TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA (Unsupported) ◦ TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA (Unsupported) ◦ TLS-ECDH-ECDSA-WITH-AES-128-CBC-SHA256 (Unsupported) ◦ TLS-ECDH-ECDSA-WITH-AES-256-CBC-SHA384 (Unsupported) ◦ TLS-ECDH-ECDSA-WITH-AES-128-GCM-SHA256 (Unsupported) ◦ TLS-ECDH-ECDSA-WITH-AES-256-GCM-SHA384 (Unsupported) ◦ TLS-ECDH-RSA-WITH-AES-128-CBC-SHA (Unsupported) ◦ TLS-ECDH-RSA-WITH-AES-256-CBC-SHA (Unsupported) ◦ TLS-ECDH-RSA-WITH-AES-128-CBC-SHA256 (Unsupported)
--	---

	<ul style="list-style-type: none"> ◦ TLS-ECDH-RSA-WITH-AES-256-CBC-SHA384 (Unsupported) ◦ TLS-ECDH-RSA-WITH-AES-128-GCM-SHA256 (Unsupported) ◦ TLS-ECDH-RSA-WITH-AES-256-GCM-SHA384 (Unsupported) ◦ TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256 ◦ TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256 ◦ TLS-RSA-WITH-CAMELLIA-256-CBC-SHA ◦ TLS-RSA-WITH-SEED-CBC-SHA
--	--

7. Click OK.

Supported Software Information

Releases 22.1.4 and later support all content described in this article.

Additional Information

[Configure IPsec VPN Profiles](#)

[Generate CA and EE Certificates Using OpenSSL](#)