
Configure SASE TLS Decryption

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

Transport Layer Security (TLS) decryption is an industry-standard protocol that is used to provide a secure communications channel between clients (end devices) and servers (destination sites) over the internet. TLS decryption uses two mechanisms to secure traffic:

- Handshake protocol—Authenticates the client and server devices at both ends of a secure communications channel, negotiates cryptographic modes and parameters, and establishes shared keying material used to negotiate the security parameters of a connection. The handshake protocol then sends messages to the TLS record protocol.
- Record protocol—Takes transmitted messages from the handshake protocol, fragments the data into manageable blocks, protects the records, and transmits the result. The data received is verified, decrypted, reassembled, and then delivered to higher-level clients.

Note: You must configure the following SASE rules, profiles, and settings in a specific order:

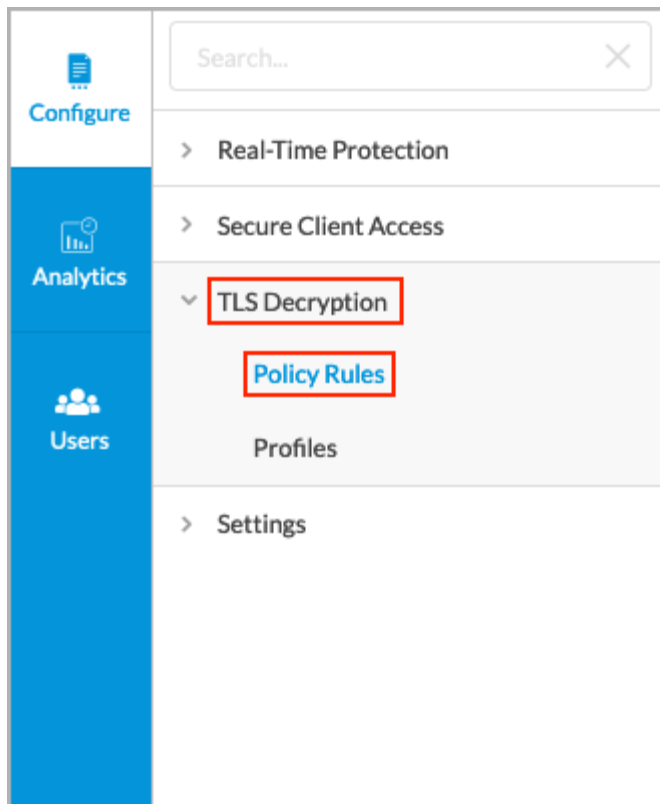
1. Configure users and groups, and then publish them to the gateway. For more information, see [Configure Users and Device Authentication](#).
2. Configure site-to-site tunnels. For more information, see [Configure SASE Site-to-Site Tunnels](#).
3. Configure secure client access profiles and rules. For more information, see [Configure SASE Secure Client Access Rules](#).

The remaining SASE rules, profiles, and settings do not need to be configured in a specific order.

Configure TLS Decryption Rules

To configure TLS decryption rules:

1. Go to Configure > TLS Decryption > Policy Rules.



The TLS Decryption Rules List screen displays all current rules.

Configure > SASE > TLS Decryption > Policy Rules

TLS Decryption Rules List Publish

Below are all the TLS Decryption Rules

RULE NAME		DECRYPTION PROFILE	BYPASS URL FILTERING PROFILE	USERS	SOURCE & DESTINATION	SERVICES	SCHEDULE	URL CATEGORIES AND REPUTATIONS	ENABLED
<input type="checkbox"/>	Rule123	Rish	allow_all	▼ tag:25 All Users	All Source and Destination	All Layer 4 Services	Not Available	All URL Categories And Reputations selected	Enabled

Showing 1-1 of 1 results 10 rows Go to page 1 < Previous 1 Next >

- To customize which columns display, click Select Columns and click the columns select or deselect the columns you want to display. Click Reset to return to the default columns settings.

Select Columns

☒ Decryption Profile

☒ Bypass URL Filtering Profi

☒ Users

☒ Source & Destination

Reset

3. Click + Add to add a TLS decryption rule. The Create TLS Decryption Rule screen displays. In the first step, Decryption Enforcement, enter information for the following fields.

Configure > SASE > TLS Decryption > Policy Rules

Create TLS Decryption Rule

1

2

3

4

DECRIPTION ENFORCEMENT

USER GROUPS

NETWORK

REVIEW & VALIDATE

What type of rule would you like to create?.

You can customize either configuration you'd like to enforce

Decrypt and Inspect the Traffic

Normally, encrypted traffic is not blocked. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network

Use the following decryption profile

+ Add New

Bypass decryption for the following URL profiles(optional)

Select a URL Profile

This rule scans for web and email traffic

Do Not Decrypt

This option does not decrypt and enforce security rules on traffic because the traffic remains encrypted. This option should be used on sites, applications or services you need for your organization.

Do not decrypt but do inspect the traffic

Encryption does not necessarily mean that content is safe. Gain visibility into the hidden traffic within your network and identify, classify, and inspect the packets for threats. Know what is being intentionally or accidentally sent outside of your organization.

Select Profile

Do not decrypt and do not inspect the traffic

Allow traffic from certain trusted sites to go uninspected. Keep in mind, this can be risky because webpages are not static.

Cancel

Back

Skip to Review

Next

Field	Description
Decrypt and Inspect the Traffic (Group of Fields)	Select to decrypt and inspect all traffic.
<div>◦ Use the following decryption profile</div>	Select a decryption profile.
<div>◦ + Add New</div>	Click to add a decryption profile. To create a profile, see Create a TLS Decryption Profile .
<div>◦ Bypass decryption for the following URL-filtering</div>	To bypass the decryption action in a URL filtering profile, select a URL-filtering profile. This URL-filtering

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...)

Updated: Wed, 23 Oct 2024 08:38:13 GMT

Copyright © 2024, Versa Networks, Inc.

3

Field	Description
profile	profile must be one in which decrypt bypass is enabled. The user-defined URL profile must be created in the Tenant-Common template in the Director before it displays in the drop-down list. Contact Versa Support to configure this option.
Do Not Decrypt (Group of Fields)	Select how to bypass decryption of the traffic.
<ul style="list-style-type: none"> Do not decrypt but do inspect the traffic 	Do not decrypt the traffic but inspect the traffic to identify, classify, and inspect the traffic for threats. Select a profile.
<ul style="list-style-type: none"> Do not decrypt and do not inspect the traffic 	Click to allow traffic from certain trusted sites to no be inspected.

- Click Next to go to the second step, User Groups. The User Groups screen displays. By default, security enforcement is applied to all users and user groups.

Configure > SASE > Settings > TLS Decryption > Rule

Create TLS Decryption Rule

1

2

3

4

DECRYPTION ENFORCEMENT

USER GROUPS

NETWORK

REVIEW & VALIDATE

By default we have chosen all users and groups to apply your security enforcements

If you prefer, you can select the specific users or groups for the security posture.

Users & User Groups

✓ All users from ACME-Group-Profile servers

[Customize](#)

Cancel

Back

Skip to Review

Next

- To accept the default, click Next to continue the Geolocations match criteria.
- To change these settings, click Customize. The Users and User Groups screen displays.

← Back Users & User Groups

Enable TLS Decryption for the following matched users or user groups

ACME-Group-Profile

User Groups Users

Search for User Groups

User Groups (20) + Add New User Group

NAME	DISTINGUISHED NAME (DN)
<input type="checkbox"/> vd-group1	CN=vd-group1,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107852
<input type="checkbox"/> vd-group10	CN=vd-group10,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107861
<input type="checkbox"/> vd-group11	CN=vd-group11,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107862
<input type="checkbox"/> vd-group12	CN=vd-group12,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107863
<input type="checkbox"/> vd-group13	CN=vd-group13,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107864
<input type="checkbox"/> vd-group14	CN=vd-group14,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107865
<input type="checkbox"/> vd-group15	CN=vd-group15,OU=VD-Automation,DC=versa-qa-lab,DC=local S-1-5-21-604474016-2011482265-4024304318-107866

Cancel Back Skip to Review Next

7. Select the group profile to use.
8. Under the User Groups tab, select the user groups to include in the match list, or type the name of a user group in the search box and then select it from the search results.
9. To create a user group based on LDAP authentication, select an LDAP group profile, and then click + Add New User Group. In the Add User Group window, enter a user group name and a distinguished name (DN).

Add User Group ×

User Group*

Distinguished Name (DN)*

Cancel Add

10. Click the Users tab in the submenu. The following screen displays.

← Back Users & User Groups

Enable TLS Decryption for the following matched users or user groups

ACME-Group-Profile

User Groups Users

Search for Users

Users (21) + Add New User

	USER NAME	WORK EMAIL
<input type="checkbox"/>	vd-ldap-admin	vd-ldap-admin@versa-qa-lab.local
<input type="checkbox"/>	vd-user1	vd-user1@versa-qa-lab.local
<input type="checkbox"/>	vd-user10	vd-user10@versa-qa-lab.local
<input type="checkbox"/>	vd-user11	vd-user11@versa-qa-lab.local
<input type="checkbox"/>	vd-user12	vd-user12@versa-qa-lab.local
<input type="checkbox"/>	vd-user13	vd-user13@versa-qa-lab.local
<input type="checkbox"/>	vd-user14	vd-user14@versa-qa-lab.local
<input type="checkbox"/>	vd-user15	vd-user15@versa-qa-lab.local

Cancel
Back
Skip to Review
Next

11. Select the group profile to use.
12. Under the Users tab, select the users to include in the match list, or type the name of a user in the search box and then select it from the search results.
13. To create a user based on LDAP authentication, select an LDAP group profile, and then click + Add New User. In the Add User window, enter a username and the user's work email in the fields provided.

Add User ✕

User Name*

Work Email*

Cancel
Add

14. Click Add.
15. Click Next to go to the Network screen, or click Back to return to the Create TLS Decryption Rule screen, and then click Next. The following screen displays.

Configure > SASE > TLS Decryption > Policy Rules

Create TLS Decryption Rule

1

DECRYPTION ENFORCEMENT

2

USER GROUPS

3

NETWORK

4

REVIEW & VALIDATE

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Source & Destination Traffic

Source

Zone

✓ GW1-Tunnel

✓ GW2-Tunnel

✓ SD-WAN Zone

Load More

Destination

Zone

✓ Internet

Customize

Services

✓ All layer 4 services

Customize

URL Categories & Reputations

None Selected

Customize

Schedule

✓ None Selected

Customize

Cancel

Back

Skip to Review

Next

- By default, all source and destination traffic is included in the match list. To change the source and destination traffic to include in the match list, click **Customize** under **Source & Destination Traffic**. In the **Source & Destination Traffic** screen, enter information for the following fields.

← Back

Source & Destination Traffic

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Zone

✓ All (5)

✓ Versa Client

✓ SD-WAN Zone

✓ GW1-Tunnel

✓ GW2-Tunnel

✓ Test-Tunnel1

Destination Zone

✓ All (1)

✓ Internet

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...)

Updated: Wed, 23 Oct 2024 08:38:13 GMT

Copyright © 2024, Versa Networks, Inc.

7

Source Address

Address Group ⓘ + Add New

Enter a list of IP Addresses or range values

IP Subnet ⓘ

IP Range ⓘ

IP WildCard ⓘ

☐ Source Address Negate ⓘ

Destination Address

Address Group ⓘ + Add New

Enter a list of IP Addresses or range values

IP Subnet ⓘ

IP Range ⓘ

IP WildCard ⓘ

☐ Destination Address Negate ⓘ



Cancel

Back

Skip to Review

Next

Field	Description
Source Zone	<p>Select one or more source zones to include in the match list. By default, three source zones are available:</p> <ul style="list-style-type: none"> SD-WAN Zone—Select if traffic comes from an SD-WAN device. User-defined zones—Select for zones, such as zones for IPsec or GRE tunnels. Versa Client—Select if traffic comes from a Versa Secure Access (VSA) client application.
Source Address (Group of Fields)	
<ul style="list-style-type: none"> Address Group 	<p>Click in the box, and then select one or more address groups. These address groups are defined in the User Defined Objects section.</p> <p>Note: You do not need to select an address group if you want to provide one or more specific source IP addresses, in which case you use the IP Wildcard field to enter the IP addresses.</p> <p>To create an address group, click + Add New, and then enter the following information.</p>

Field	Description
	<div><div>Configure > SASE > Settings > TLS Decryption</div><div>Address Group</div><div><div>1 ENTER ADDRESSES</div><div><div>Type</div><div>Subnet</div><div>IP Addresses</div></div><div><div>Cancel</div><div>Next</div></div></div><div><div>2 NAME AND TAGS</div></div></div> <div><div>1. Click the Enter Addresses section, and then select the group Type. The type can be Subnet, IP range, IP wildcard, or IPv6 subnet.</div><div>2. Based on the type selected, enter one of the following and then press Return: —Subnet: One or more IP addresses and subnet masks, for example, 10.2.1.0/24 —IP range: One or more IP address ranges, for example, 10.2.1.1-10.2.2.2 —IP wildcard: One or more specific IP addresses, for example, 192.68.0.56/255.255.0.255 —IPv6 subnet: One or more valid IPv6 subnets</div><div>3. To add additional IP address types, click the  Plus icon. To remove an address type, click the  Minus icon.</div><div>4. Click the Name and Tags section, and then enter a name for the address group and tags.</div></div> <div><div>Configure > SASE > Settings > TLS Decryption</div><div>Address Group</div><div><div><div>3 ENTER ADDRESSES</div><div>2 NAME AND TAGS</div></div><div><div>Name *</div><div>Tags</div></div><div><div>Cancel</div><div>Save</div></div></div></div> <div>5. Click Save.</div>

Field	Description
◦ IP Wildcard	Enter a list of comma-separated IP addresses and masks to include in the match list, for example, 192.68.0.56/255.255.0.255.
◦ IP Subnet	Enter a list of comma-separated subnets to include in the match list, for example, 10.2.1.0/24.
◦ IP Range	Enter a list of comma-separated IP addresses or ranges to include in the match list, for example, 10.2.1.1-10.2.2.2.
Source Address Negate	Select to apply the rule to any source addresses except the ones in the Source Address field.
Destination Zone	Internet—Select this zone if traffic comes from the internet.
Destination Address	Complete the fields under Destination Address in the same way as you did for the Source Address.

17. To customize services or schedules, click the Back button to return to the Network screen.
18. To change the services to include in the match list, click Customize under Services. The following screen displays.

Services

The Services section represents Layer 4 of the layer traffic. Layer 4 segments data from Layer 5 (Session). It ensures data arrives correctly and at what rate. Layer 5 establishes, maintains, ends communication between devices, and decides which packets belong to which files. Layer 6 (Presentation) translates data to binary and encrypts/decrypts it

[More Information](#)

Services

Custom
VideoServers
test
Pre-Defined

+ Add New

Cancel Back Skip to Review Next

19. Select one or more of the predefined services. To add a custom service, click + Add New. The following screen displays.

Configure > SASE > TLS Decryption > Policy Rules

Service

1 ENTER PROTOCOL & PORT

Protocol *

TCP

Source Port

Destination Port

Source or Destination Port

Cancel Next

2 NAME AND TAGS

20. In the Protocol field, select a protocol. If you select TCP, UDP, or TCP and UDP, enter information for the following fields.

Field	Description
Source Port	<p>Enter the source port number.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Destination Port	<p>Enter the destination port number.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Source or Destination Port	<p>Enter the source or destination port number.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>

21. Click Next. The Name and Tags section displays.

Configure > SASE > TLS Decryption > Policy Rules

Service

1 ENTER PROTOCOL & PORT +

2 NAME AND TAGS -

Name *

Tags

Cancel Save

22. In the Name field, enter a name for the new service, and optionally, enter tags and a description for the service
23. Click Save to add the service to the protocol list. You can then select the service in the drop-down list.
24. To customize schedules, click the Back button to return to the Network screen.
25. To create a schedule for the policy to be in effect, click Customize under Schedule. The following screen displays.

← Back Schedule

Schedule Hours ⓘ

Select a schedule to set the time and frequency at which the policy is in effect.

Schedule + Add New

26. Click the drop-down list under Schedule Hours to select a schedule. If no schedules exist, create one by clicking + Add New. Under Enter Schedule Details, enter information for the following fields.

Add Schedule

1 ENTER SCHEDULE DETAILS -

Recurrence

None ▾

Start Date Start Time

Select Select ⓘ

End Date End Time

Select Select ⓘ

Cancel Next

Field	Description
Recurrence	Select None, Daily, or Weekly.
Start Time	Enter the start time for the policy to be in effect.
End Time	Enter the end time for the policy to be in effect.
Days of the Week	<p>If you select the recurrence to be weekly, select the days of the week for the policy to be in effect.</p> <div> <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday </div>

27. Click Next. The Name and Tags section displays.

Add Schedule

1 ENTER SCHEDULE DETAILS +

2 NAME, DESCRIPTION & TAGS -

Name *

Tags

Cancel Save

28. In the Name field, enter a name for the new schedule, and optionally, enter tags for the service.
29. Click Save.
30. Click the Back button to return to the Network screen.
31. To customize URL categories and reputations, click Customize under URL Categories & Reputations. The following screen displays.

←

Back

URL Categories & Reputations

The URL section represents the URL layer traffic. Let's suppose you're using messaging apps on a laptop. You're messaging your friend, who's using Skype on their phone from a different network. Skype, as a network-connected application, uses (URL) protocols like Telnet. If you send your friend a picture of your cat, Skype would be using the File Transfer Protocol (FTP). **Layer 4**

[More Information](#)

URL Categories

Select one or more URL categories to apply the Internet Protection rule to.

Add URL Category

Reputations

Select one or more reputations to apply the Internet Protection rule to.

Add Reputation

Cancel

Back

Skip to Review

Next

32. To specify the URL categories to which the rule applies, select one or more URL categories in the URL Categories field.
33. To specify the reputations to which the rule applies, select one or more reputations in the Reputations field.
34. Click Next. The Review and Validate screen displays.

Configure > SASE > TLS Decryption > Policy Rules

Create TLS Decryption Rule

1

DECIPHER ENFORCEMENT

2

USER GROUPS

3

NETWORK

4

REVIEW & VALIDATE

Please give your rule a name:

General

Name *

Description

Tags



Rule is enabled

Cancel

Back

Save

Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of the new rule.

Field	Description
Tags	Enter one or more tags for the new rule. A tag is an alphanumeric text descriptor with no spaces or special characters that is used for searching rules. You can specify multiple tags.
Rule is enabled	<p>Click the slider to enable the rule.</p>  <p>Click the slider again to disable the rule.</p> 

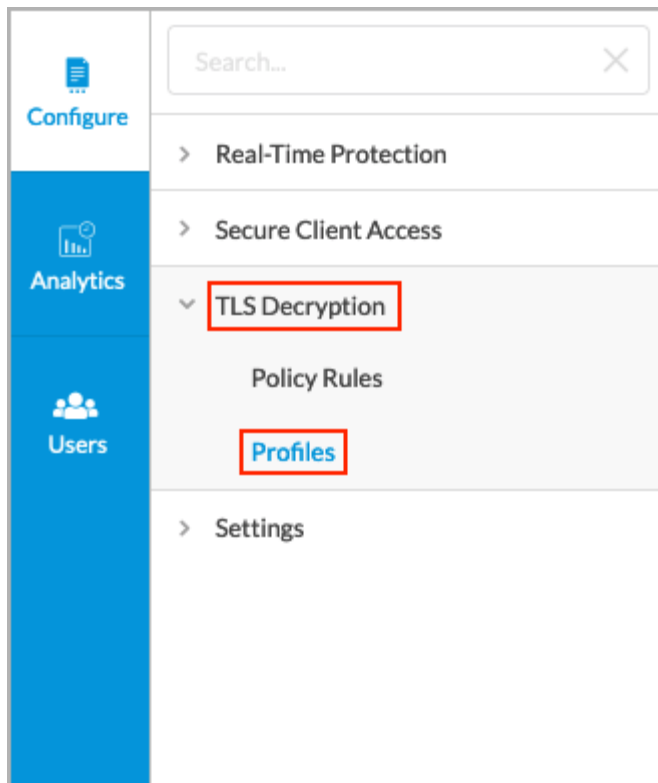
35. Click Save.

Create a TLS Decryption Profile

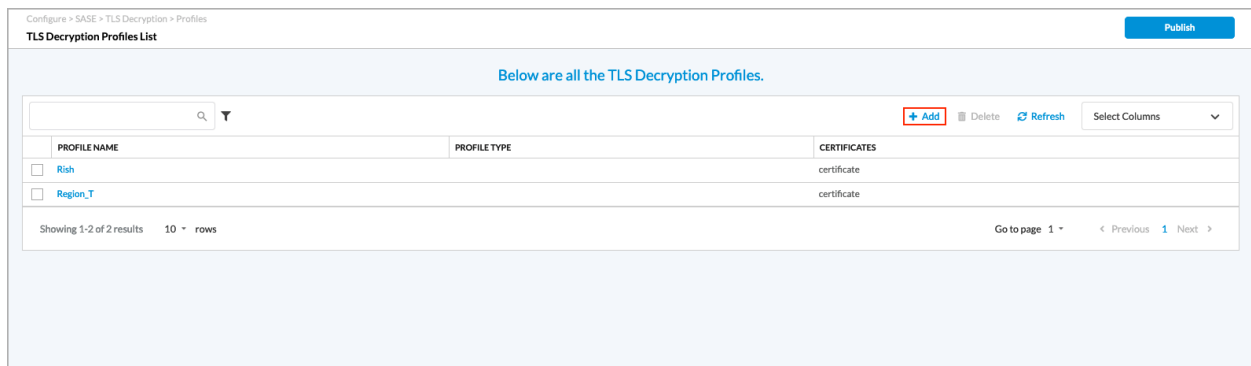
When you configure TLS decryption for a tenant, the VOS device behaves as an SSL proxy, and it generates a TLS/SSL certificate for each HTTPS URL that the tenant tries to access (for example, <https://example.com>). The certificate allows the VOS device to inspect the data flow and take any necessary actions. To optimize the SSL proxy behavior, the VOS device uses the same generated public–private key pair for certificates issued across domains. This key pair is generated for each configured decryption profile, and hence is unique for each tenant.

To create a TLS decryption profile:

1. Go to Configure > TLS Decryption > Profiles.



The TLS Decryption Profiles List screen displays all current profiles.



- Click + Add New to add a TLS decryption profile. The Create TLS Decryption Profile screen displays with the first step, Profile Type, selected by default. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network. You can configure a decryption profile with SSL inspection and policy enforcement information.

Configure > SASE > TLS Decryption > Profiles

Create TLS Decryption Profile

1 **PROFILE TYPE**
2 **CERTIFICATE SETUP**
3 **INSPECTION OPTIONS**
4 **DECRYPTION OPTIONS**
5 **REVIEW & VALIDATE**

Create a TLS Decryption Profile

Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network. You can configure a decryption profile with SSL inspection and policy enforcement information. This section will guide you through the process of configuring the decryption profiles.

Decryption Profile

This profile applies both decryption and inspection protocols that you can associate with your decryption rules.

Inspection Profile

This profile applies only inspection protocols that you can associate with your decryption rules.

Cancel
Back
Skip to Review
Next

3. Select a decryption profile or an inspection profile:
 - a. Decryption Profile—Applies both decryption and inspection protocols that you can associate with your decryption rules.
 - b. Inspection Profile—Applies only inspection protocols that you can associate with your decryption rules.
4. Click Next to go to Step 2, Certificate Setup.

Configure > SASE > TLS Decryption > Profiles

Create TLS Decryption Profile

1 **PROFILE TYPE**
2 **CERTIFICATE SETUP**
3 **INSPECTION OPTIONS**
4 **DECRYPTION OPTIONS**
5 **REVIEW & VALIDATE**

We've selected a certificate authority for you by default.

A certificate authority (CA) is an entity that issues digital certificates to verify the ownership of a public key. Only one certificate can be selected. If you prefer, you can choose another CA to use.

Previously Uploaded Certificates

ACME + Add New

Details

Name: ACME
 File Name: ACME.zip
 Key: ACME.key
 Certificate: ACME.crt
 Issued To: ACME
 Issued By: Versa Networks Inc.
 Validity: 2022-01-12 15:31:54 to 2027-01-11 15:31:54

Cancel
Back
Skip to Review
Next

5. Click Next to accept the default certificate authority (CA). To use a different CA, select one of the previously uploaded certificates, or click + Add New to configure a new CA. In the Certificates popup window, enter information for the following fields.

Certificates

✕

Certificate Type

☒ CA Certificate

☐ Default

The file to be uploaded needs to be in .zip format. They will consist of 2 files: a key and a certificate. The key file needs to have .key extension. There is no restriction on the extension of the certificate file.

Certificate Name *

Upload File

Cancel

Add

Field	Description
Certificate Type	Click CA Certificate.
Default slide	Click the slider to have the added CA certificate to be the default CA certificate. <div> <input checked="" type="checkbox"/> Default </div>
Certificate Name	Enter a name for the certificate.
Upload File	Click to upload a CA certificate file.
Add	Click to add the new certificate.

6. Click Next to go to Step 3, Inspection Options.

Configure > SASE > TLS Decryption > Profiles

Create TLS Decryption Profile

1

PROFILE TYPE

2

CERTIFICATE SETUP

3

INSPECTION OPTIONS

4

DECRYPTION OPTIONS

5

REVIEW & VALIDATE

Based on the most common secure enterprise settings, we've chosen the inspection options, below.

If you prefer, you can customize which inspection options you'd like to enable for your decryption.

TLS inspection is the process of intercepting and reviewing SSL or TLS encrypted internet communication between the client and the server. The inspection of SSL or TLS encrypted traffic has become critically important because the vast majority of Internet traffic is SSL or TLS encrypted, including malicious traffic.

[More Information](#)

Certificate Validation

This is the Internet protocol used by web browsers to determine the revocation status of SSL/TLS certificates supplied by HTTPS websites.

Verify with OCSP

Enable server certificate verification using the Online Certificate Status Protocol (OCSP).

Block Unknown Certificates

Block SSL sessions whose certificate status is unknown.

Response timeout(seconds) for an OCSP request

5

Server Certificate Actions

Choose what actions should occur for the following server certificate checks.

When the certificate expires, do the following:

Select

When the certificate is received from an untrusted issuer, do the following:

Select

Choose whether to restrict the certificate key usage extensions to either digital signature or key encipherment.

☐ Restrict Certificate Extension

SSL or TLS Protocol Checks

Choose what actions should occur for the following SSL or TLS protocol checks.

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported key length, do the following:

Select

Minimum Supported RSA Key Length

1024

bits

Enter a value of 512 bits or higher

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported cipher, do the following:

Select

When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported protocol version, do the following:

Select

Cancel

Back

Skip to Review

Next

Field	Description
Certificate Validation (Group of Fields)	
<ul style="list-style-type: none"> Verify with OCSP 	Select to use the Online Certificate Status Protocol (OCSP) to verify a server certificate.

Field	Description
◦ Block Unknown Certificates	Select to block SSL sessions whose certificate status is unknown.
◦ Response timeout (seconds) for an OCSP request	Enter how long, in seconds, before an OCSP request times out. <i>Default:</i> 5 seconds <i>Range:</i> 1 to 255 seconds
Server Certificate Actions (Group of Fields)	
◦ When the certificate expires, do the following:	Select an action to take when the certificate expires.
◦ When the certificate is received from an untrusted issuer, do the following	Select an action to take when a certificate is received from an untrusted issuer.
◦ Restrict Certificate Extension	Click to choose whether to restrict the certificate key usage extensions to either digital signature or key encipherment.
SSL or TLS Protocol Checks (Group of Fields)	
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported key length, do the following:	Select an action to take when SSL or TLS between the client and server uses an unsupported key length.
◦ Minimum Supported RSA Key Length	Enter the minimum supported RSA key length, in bits. <i>Default:</i> 1024 bit <i>Range:</i> 512 bits or longer
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported cipher, do the following:	Select an action to take when SSL or TLS between the client and server uses an unsupported cipher.
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported protocol version, do the following:	Select an action to take when SSL or TLS between the client and server uses an unsupported protocol version.

7. Click Next to go to Step 4, Decryption Options, and then enter information for the following fields.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...)

Updated: Wed, 23 Oct 2024 08:38:13 GMT

Copyright © 2024, Versa Networks, Inc.

Configure > SASE > TLS Decryption > Profiles

Create TLS Decryption Profile

1

2

3

4

5

PROFILE TYPE

CERTIFICATE SETUP

INSPECTION OPTIONS

DECRYPTION OPTIONS

REVIEW & VALIDATE

Based on the most common secure enterprise settings, we've chosen the protocol options, below.

If you prefer, you can customize which protocol options you'd like to enable for your decryption.

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security.

[More Information](#)

Transport Layer Security (TLS) Version Support

Select the minimum and maximum version of TLS that is supported. When you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.

TLS 1.0

TLS 1.1

TLS 1.2

TLS 1.3

Key Exchange Algorithms

☐ ECDHE—Elliptic-Curve Diffie–Hellman Key Exchange

☐ RSA—Rivest–Shamir–Adleman algorithm

ADVANCED

Algorithms

Select which encryption and authentication algorithms to use.

Encryption Algorithms

☐ AES-128-CBC

☐ AES-128-GCM

☐ AES-256-CBC

☐ AES-256-GCM

☐ CAMELLIA-256-CBC

☐ CHACHA20-POLY1305

☐ SEED-CBC

Authentication Algorithms

☐ SHA

☐ SHA256

☐ SHA384

TLS Cipher Suites

The following TLS cipher suites are automatically selected based on your algorithms above.

☐ TLS-AES-128-GCM-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA

☐ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA

☐ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA

☐ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA

☐ TLS-RSA-WITH-AES-128-CBC-SHA

☐ TLS-RSA-WITH-AES-256-CBC-SHA

☐ TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256

☐ TLS-RSA-WITH-SEED-CBC-SHA

☐ TLS-AES-256-GCM-SHA384

☐ TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384

☐ TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256

☐ TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384

☐ TLS-RSA-WITH-AES-128-CBC-SHA256

☐ TLS-RSA-WITH-AES-256-CBC-SHA256

☐ TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256

☐ TLS-CHACHA20-POLY1305-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256

☐ TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384

☐ TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256

☐ TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384

☐ TLS-RSA-WITH-AES-128-GCM-SHA256

☐ TLS-RSA-WITH-AES-256-GCM-SHA384

☐ TLS-RSA-WITH-CAMELLIA-256-CBC-SHA

Cancel

Back

Skip to Review

Next

https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_TLS_Decryp...

Updated: Wed, 23 Oct 2024 08:38:13 GMT

Copyright © 2024, Versa Networks, Inc.

21

Field	Description
Transport Layer Security (TLS) Version Support (Group of Fields)	
<ul style="list-style-type: none"> Minimum and maximum version of TLS that is supported 	Use the slider to select the minimum and maximum TLS version that is supported. If you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.
<ul style="list-style-type: none"> Key Exchange Algorithms 	Select one or more key exchange algorithms: <ul style="list-style-type: none"> ECDHE—Elliptic-Curve Diffie-Hellman Key Exchange RSA—Rivest-Shamir-Adleman algorithm.
Advanced	Click to configure algorithms and TLS cipher suites.
Algorithms	Select which encryption and authentication algorithms to use.
TLS Cipher Suites	Displays the TLS cipher suites selected depending on the algorithms.


8. Click Next to go to Step 5, Review & Validate, and then enter information for the following fields.

Configure > SASE > TLS Decryption > Profiles
Create TLS Decryption Profile

1 2 3 4 5
 PROFILE TYPE CERTIFICATE SETUP INSPECTION OPTIONS DECRYPTION OPTIONS REVIEW & VALIDATE

[Review and name your profile](#)

General

Name * 

Description

Tags

Certificate Setup [Edit](#)

Certificate Authority ACME

Issued For ACME

Issued By Versa Networks Inc.

Inspection Options
[Edit](#)

Online Certificate Status Protocol (OCSP)
Verify with OCSP Disabled
Block Unknown Certificates Disabled

Response timeout(seconds) for an OCSP request: 5 Secs

Server Certificate Actions
When the certificate expires, do the following:
When the certificate is received from an untrusted issuer, do the following:

Restrict Certificate Extension: Disabled

SSL or TLS Protocol Checks
When the negotiated SSL or TLS protocol between the Client and Server uses an unsupported key length, do the following: 1024 bits
Minimum Supported RSA Key Length

When the decryption encounters an unsupported protocol version, do the following:
When the decryption encounters an unsupported cipher, do the following:

Decryption Options
[Edit](#)

TLS Version
Minimum TLS-1.1
Maximum TLS-1.2

Key Exchange Algorithms:

Algorithms
Encryption Algorithms
Authentication Algorithms


TLS Cipher Suites
Encryption Algorithms TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA

Cancel

Back

Save

Field	Description
General (Group of Fields)	
◦ Name	Enter a name for the TLS decryption profile.
◦ Description	Enter a text description for the profile.
◦ Tags	Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters that is used for searching profiles. You can specify multiple tags.

- Review the Certificate Setup, Inspection Options, and Encryption Option sections.
- To change any of the information, click the  Edit icon in the section and then make the required changes.
- Click Save to save the new TLS decryption profile.

Certificate Pinning and SSL Decryption Exclusions

Certificate pinning is a security mechanism to prevent man-in-the-middle (MITM) attacks. It enhances the security of SSL/TLS connections to establish a secure and encrypted communication channel between a client, such as a desktop or a mobile application, and a server.

Certificate pinning associates the digital certificate or public key of a server with the client application. It does not rely solely on the default trust provided by CAs. When a client connects to a server, it checks the server certificate against a copy of the stored certificate or public key. If there is no match, the connection terminates, which ensures that only trusted certificates are accepted. This adds an additional security layer for mobile and web applications.

Versa Networks offers a predefined list of applications that are excluded from SSL inspection to prevent issues caused by certificate pinning. For more information, see [SSL Decryption Exclusion List](#), below.

SSL Decryption Exclusion List

The table below includes the hostnames of applications that bypass SSL inspections due to certificate pinning.

Hostname	Description
*.whatsapp.net	whatsapp: pinned-cert
kdc.uas.aol.com	aim: client-cert-auth
bos.oscar.aol.com	aim: client-cert-auth
*.agni.lindenlab.com	second-life: client-cert-auth
*.onpagecrm.com	onpagecrm: pinned-cert
update.microsoft.com	ms-update: client-cert-auth
*.update.microsoft.com	ms-update: client-cert-auth
activation.sls.microsoft.com	ms-product-activation: client-cert-auth
yuuguu.com	yuuguu: client-cert-auth
*.softether.com	packetix-vpn: client-cert-auth
*.tpncs.simplifymedia.net	simplify: pinned-cert
tpnxmpp.simplifymedia.net	simplify: pinned-cert
*.table14.fr	winamax: client-cert-auth
*.gotomeeting.com	gotomeeting: client-cert-auth
*.live.citrixonline.com	gotomeeting: client-cert-auth

*.mozilla.org	For mozilla update, no appid: client-cert-auth
lr.live.net	live-mesh, live-mesh-remote-desktop, live-mesh-sync: client-cert-auth
anywhere2.telus.com	For call anywhere, no appid: client-cert-auth
accounts.mesh.com	live-mesh, live-mesh-remote-desktop, live-mesh-sync: client-cert-auth
storage.mesh.com	live-mesh, live-mesh-remote-desktop, live-mesh-sync: client-cert-auth
*.sharpcast.com	sugarsync: client-cert-auth
auth2.triongames.com	rift: client-cert-auth
*.zumodrive.com	zumodrive: pinned-cert
*.urlcloud.paloaltonetworks.com	paloalto-wildfire-cloud: client-cert-auth
*.wildfire.paloaltonetworks.com	paloalto-wildfire-cloud: client-cert-auth
*.telex.cc	telex: client-cert-auth
*.icloud.com	icloud: pinned-cert
*.onlive.com	onlive: pinned-cert
*.wetransfer.com	wetransfer: client-cert-auth
www.rooms.hp.com	hp-virtual-rooms: client-cert-auth

novafusion.ea.com	ea-fifa: client-cert-auth
fesi.ea.com	ea-fifa: client-cert-auth
courier.push.apple.com	apple-push-notifications: pinned-cert
courier.sandbox.push.apple.com	apple-push-notifications: pinned-cert
.* courier.sandbox.push.apple.com	apple-push-notifications: pinned-cert
.* pgiconnect.com	web-browsing: client-cert-auth
sap.mymeetingroom.com	web-browsing: client-cert-auth
.* logmein.com	logmein: pinned-cert
.*.* logmein.com	logmein: pinned-cert
.* itwin.com	itwin: client-cert-auth
notify.mql5.com	metatrader: client-cert-auth
updates.metaquotes.net	metatrader: client-cert-auth
.* vudu.com	vudu: pinned-cert
login.kaseya.net	kaseya: client-cert-auth
.* one.ubuntu.com	ubuntu-one: client-cert-auth

*.cloudmosa.com	puffin: pinned-cert
*.las.citrixonline.com	gotomeeting: client-cert-auth
*.sjc.citrixonline.com	gotomeeting: client-cert-auth
*.ord.citrixonline.com	gotomeeting: client-cert-auth
*.iad.citrixonline.com	gotomeeting: client-cert-auth
authentication.citrixonline.com	gotomeeting: client-cert-auth
*.osdimg.com	gotomeeting: client-cert-auth
*.ams.citrixonline.com	gotomeeting: client-cert-auth
g2m.egw.citrixonline.com	gotomeeting: client-cert-auth
g2ac.egw.citrixonline.com	gotoassist: client-cert-auth
*.servers.citrixonline.com	gotomeeting: client-cert-auth
*.fra.citrixonline.com	gotoassist: client-cert-auth
*.atl.citrixonline.com	gotoassist: client-cert-auth
*.las2b.citrixonline.com	gotowebinar: client-cert-auth
*.launch.gotowebinar.com	gotowebinar: client-cert-auth
*.citrixonlinecdn.com	gotoassist: client-cert-auth

*.itunes.apple.com	itunes-base, itunes-appstore, apple-appstore, itunes-m: pinned-cert
itunes.apple.com	itunes-base, itunes-appstore, apple-appstore, itunes-m: pinned-cert
*.airddroid.com	airdroid: client-cert-auth
portal.aws.amazon.com	amazon-aws-console: client-cert-auth
connectivity.amazonworkspaces.com	amazon-workspace: pinned-cert
nds.norton.com	norton-zone: client-cert-auth
www.nortonzone.com	norton-zone: client-cert-auth
zpi.nortonzone.com	norton-zone: client-cert-auth
login.norton.com	norton-zone: client-cert-auth
*.bitdefender.com	bitdefender: client-cert-auth
*.bitdefender.net	bitdefender: client-cert-auth
*.pathviewcloud.com	pathview: client-cert-auth
secure.logmeinrescue.com	logmeinrescue: pinned-cert
*.rooms.hp.com	hp-virtual-rooms: client-cert-auth
secure.hp-ww.com	hp-virtual-rooms: client-cert-auth

*.line.naver.jp	naver-line: client-cert-auth
*.line-apps.com	naver-line: client-cert-auth
*.gc.apple.com	apple-game-center:client-cert-auth
*.wdcdn.net	wiredrive: client-cert-auth
*.wiredrive.com	wiredrive: client-cert-auth
meetfinch.com	finch: client-cert-auth
*.usefinch.com	finch: client-cert-auth
*.vagrantcloud.com	vagrant: client-cert-auth
appguru.com	appguru: client-cert-auth
*.silentcircle.com	silent-circle: client-cert-auth
*.silentcircle.net	silent-circle: client-cert-auth
www.tumblr.com	tumblr-posting: client-cert-auth
ecure.echosign.com	adobe-echosign: client-cert-auth
*.securewebportal.net	e-folder: client-cert-auth
*.mzstatic.com	apple-appstore: pinned-cert
*.dropcam.com	dropcam: client-cert-auth

www.origin.com	battlefield2: client-cert-auth
.* postlm.com	browsec: client-cert-auth
.* postls.com	browsec: client-cert-auth
two.postls.com	browsec: client-cert-auth
.* ntrsupport.com	ntr-support: client-cert-auth
crypto.cat	cryptocat: client-cert-auth
.* periscope.tv	periscope: client-cert-auth
owner-api.teslamotors.com	tesla-car-app: client-cert-auth
.* dochub.com	dochub-base,dochub-uploading: client-cert-auth
.* meerkatapp.co	meerkat: client-cert-auth
.* informaticaondemand.com	informatica-cloud: client-cert-auth
.* informaticacloud.com	informatica-cloud: client-cert-auth
.* logentries.com	surveymonkey: pinned-cert
webrootcloudav.com	webroot-secureanywhere: client-cert-auth
cloud.webroot.com	webroot-secureanywhere: client-cert-auth
.* ess.apple.com	apple-messages,itunes-base: pinned-cert

gsa.apple.com	apple-messages,itunes-base: pinned-cert
gsas.apple.com	apple-messages,itunes-base: pinned-cert
sso.8x8.com	8x8: pinned-cert
vm.8x8.com	8x8: pinned-cert
discordapp.com	discord: pinned-cert
.* whispersystems.org	signal: pinned-cert
.* snapchat.com	snapchat:pinned-cert
.* wbx2.com	cisco-spark: pinned-cert
.* ciscospark.com	cisco-spark:pinned-cert
.* mobile.yandex.net	yandex-maps:pinned-cert
.* agent.datadog.com	datadog: client-cert-auth
events-sjc.egnyte.com	egnyte: client-cert-auth
avl-egnyte-auth-service.egnyte.com	egnyte: client-cert-auth
.* kakao.com	kakaotalk: pinned-cert
.* wire.com	wire: pinned-cert
.* xhoot.com	wire: pinned-cert

*.tresorit.com	tresorit: pinned-cert
*.vortex-win.data.microsoft.com	windows-defender-atp-endpoint: pinned-cert
SevilleCloudGateway-PRD.trafficmanager.net	windows-defender-atp-endpoint: pinned-cert
mobile.surveymonkey.com	surveymonkey: pinned-cert
*.acompli.net	outlook-web-online: pinned-cert
*.coinbase.com	coinbase: client-cert-auth
*.ol.epicgames.com	fortnite: pinned-cert
*.cellcrypt.com	cellcrypt: pinned-cert
api.assembla.com	assembla: pinned-cert

Supported Software Information

Releases 11.1.1 and later support all content described in this article.

Additional Information

[Configure SASE Secure Client Access Rules](#)

[Configure SASE Site-to-Site Tunnels](#)

[Configure Users and Device Authentication](#)