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:

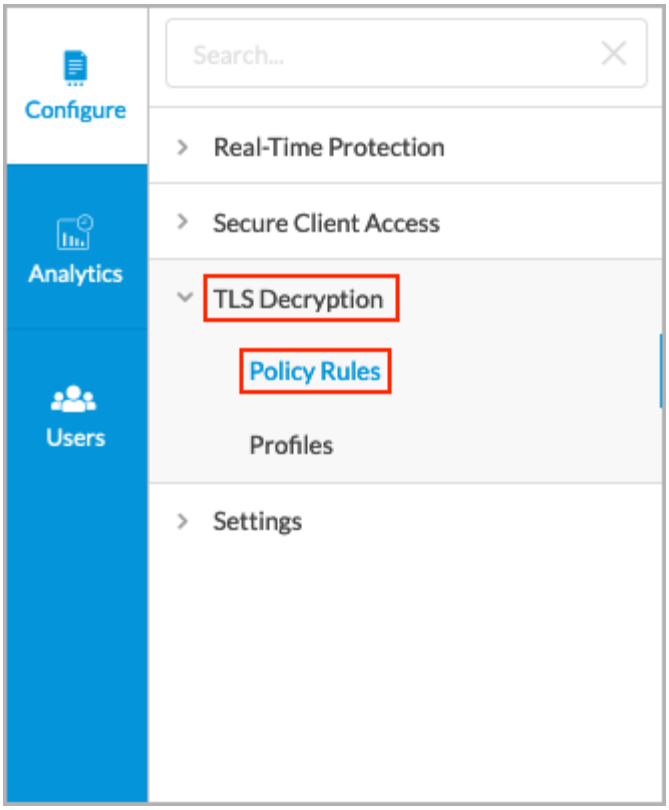
1. Configure users and groups, and then publish them to the gateway. For more information, see Configure Users and Device Authentication.
2. Configure site-to-site tunnels. For more information, see Configure SASE Site-to-Site Tunnels.
3. Configure secure client access profiles and rules. For more information,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

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

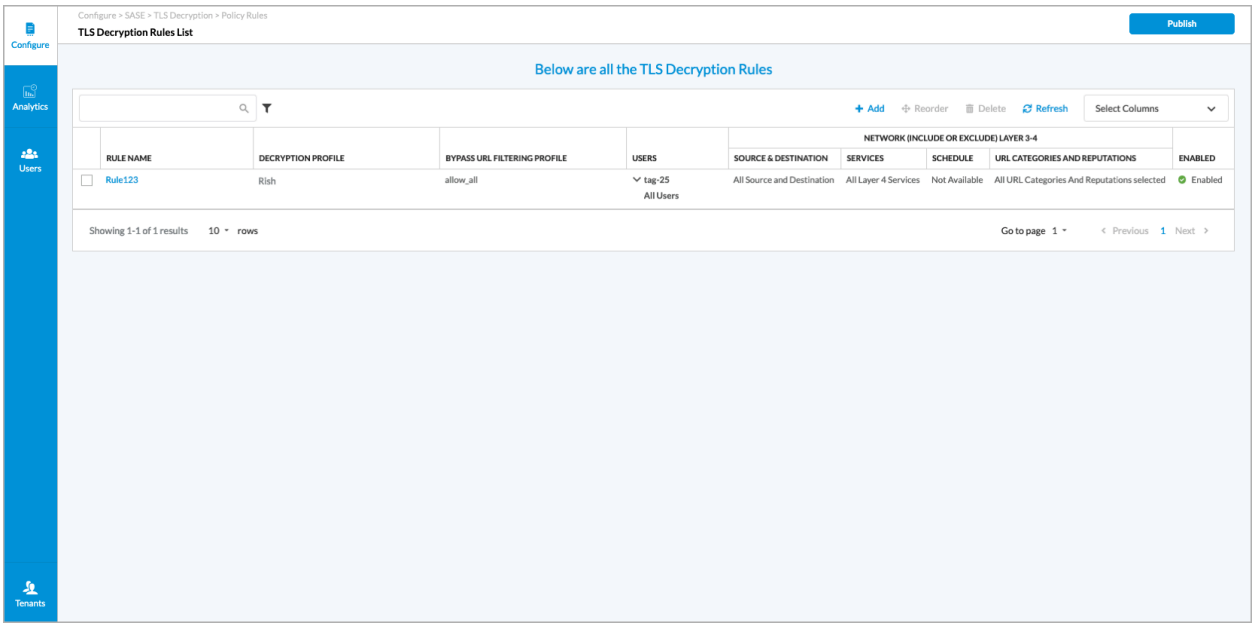
Configure TLS Decryption Rules

To configure TLS decryption rules:

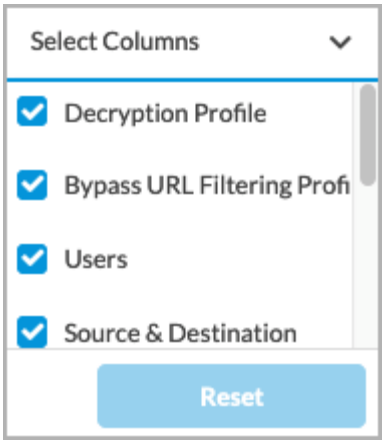
1. Go to Configure > TLS Decryption > Policy Rules.



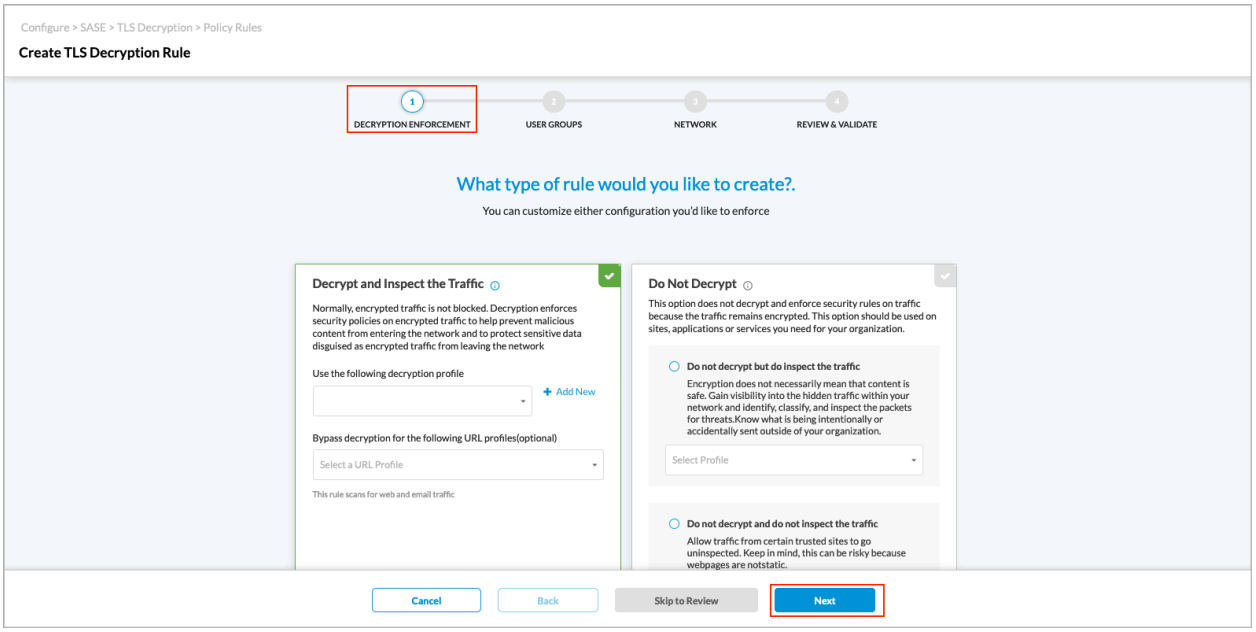
The TLS Decryption Rules List screen displays all current rules.



2. 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.



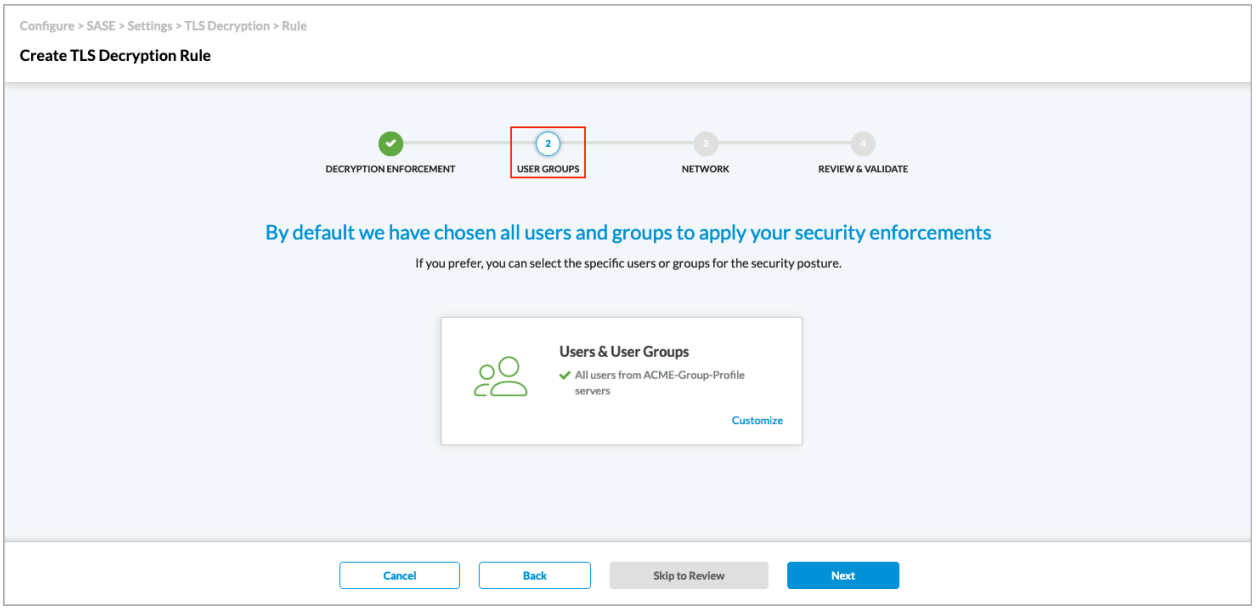
3. Click + Add to add a TLS decryption rule. The Create TLS Decryption Rule screen displays. In the first step, Decryption Enforcement, enter information for the following fields.



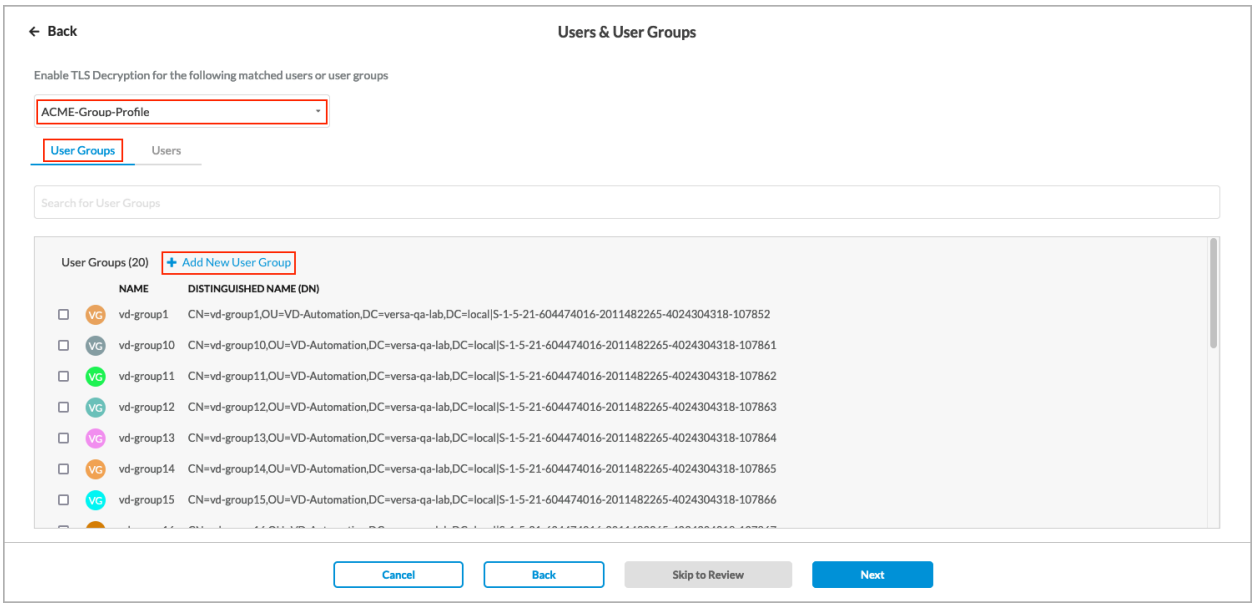
Field	Description
Decrypt and Inspect the Traffic (Group of Fields)	Select to decrypt and inspect all traffic.
◦ Use the following decryption profile	Select a decryption profile.
◦ + Add New	Click to add a decryption profile. To create a profile, see Create a TLS Decryption Profile.
◦ Bypass decryption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

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.
◦ 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.
◦ Do not decrypt and do not inspect the traffic	Click to allow traffic from certain trusted sites to no be inspected.

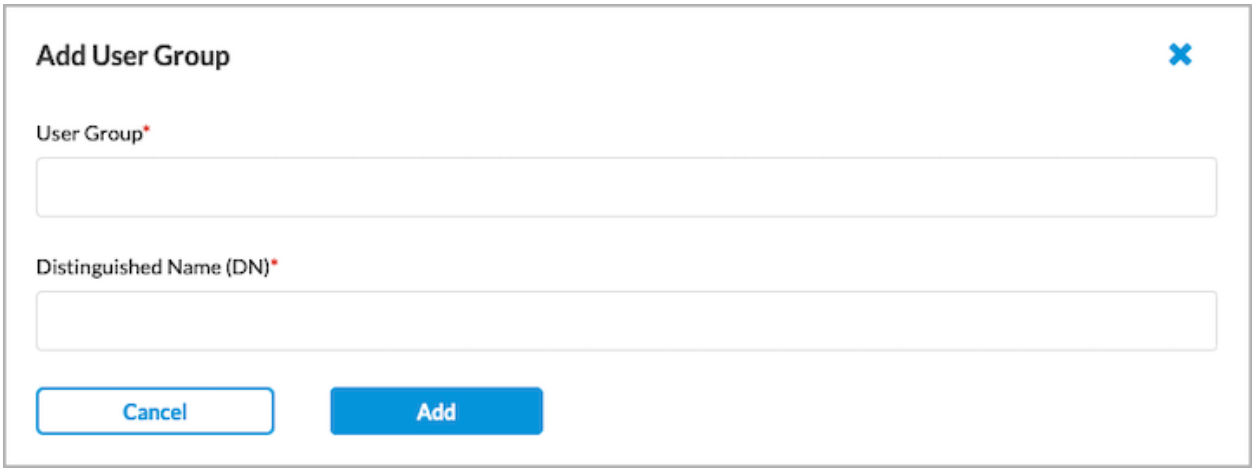
4. Click Next to go to the second step, User Groups. The User Groups screen displays. By default, security enforcement is applied to all users and user groups.



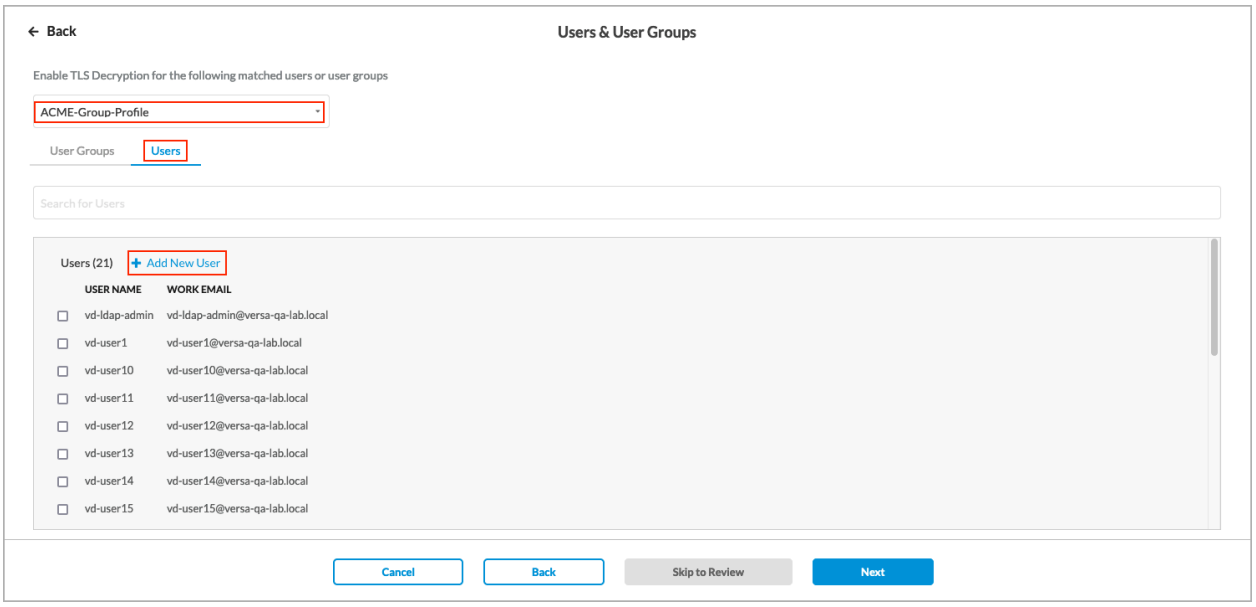
5. To accept the default, click Next to continue the Geolocations match criteria.
6. To change these settings, click Customize. The Users and User Groups screen displays.



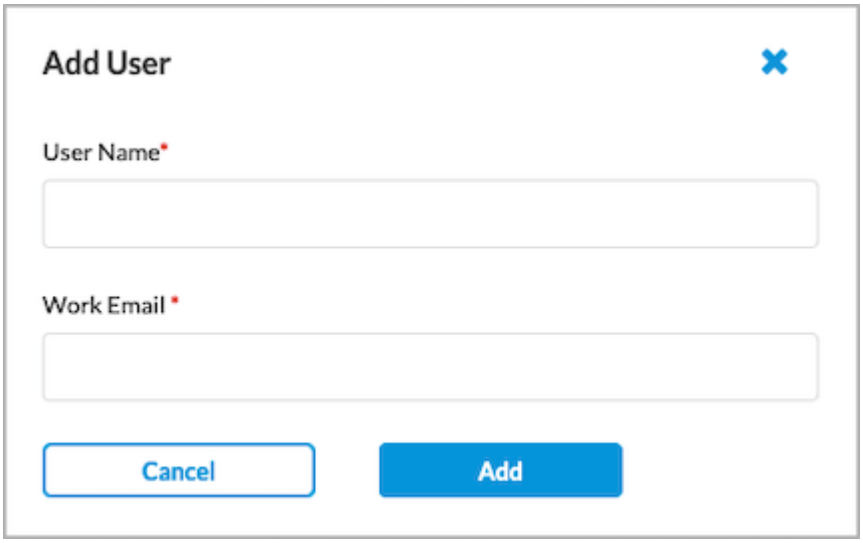
7. Select the group profile to use.
8. Under the User Groups tab, select the user groups to include in the match list, or type the name of a user group in the search box and then select it from the search results.
9. To create a user group based on LDAP authentication, select an LDAP group profile, and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



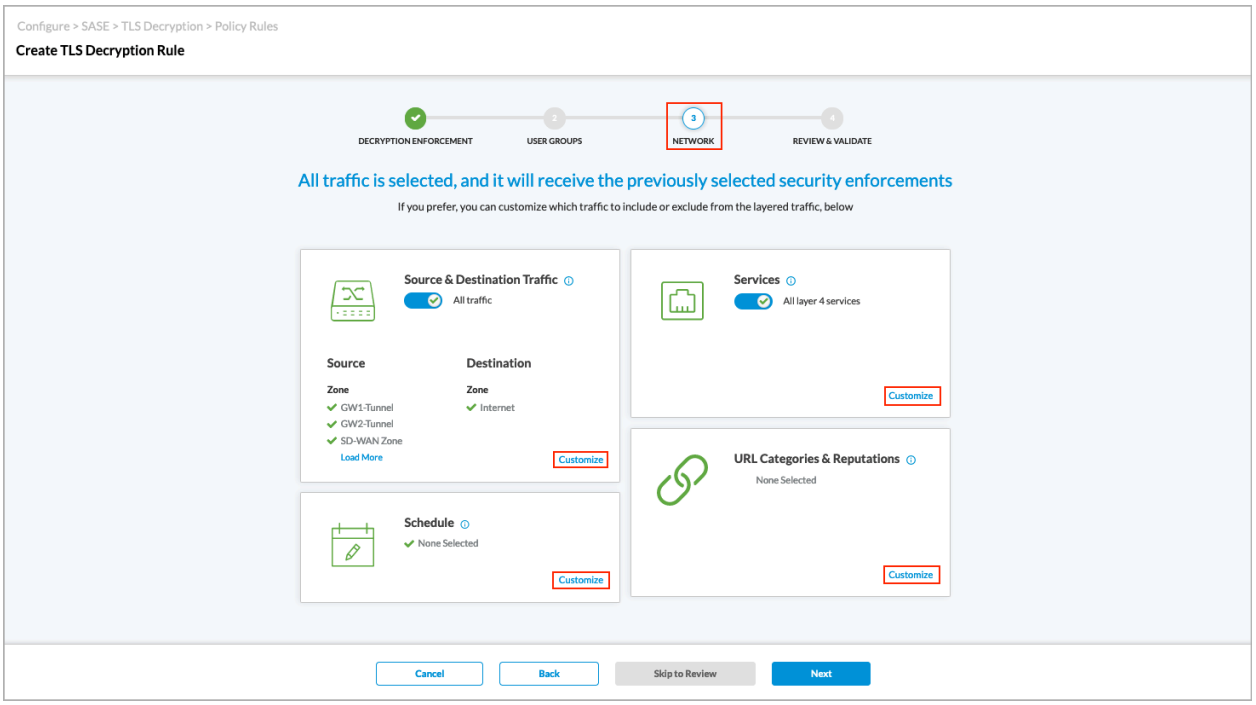
10. Click the Users tab in the submenu. The following screen displays.



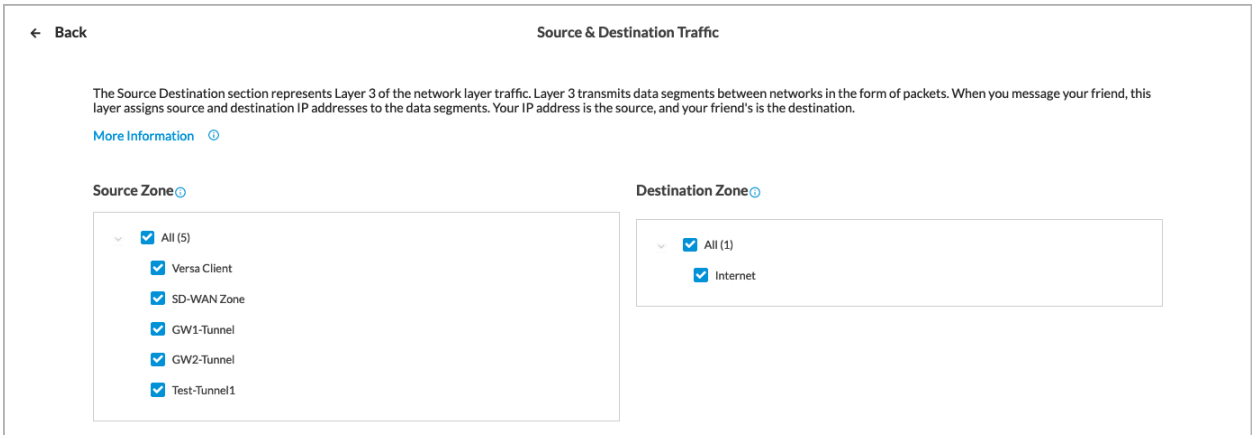
11. Select the group profile to use.
12. Under the Users tab, select the users to include in the match list, or type the name of a user in the search box and then select it from the search results.
13. To create a user based on LDAP authentication, select an LDAP group profile, and then click + Add New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

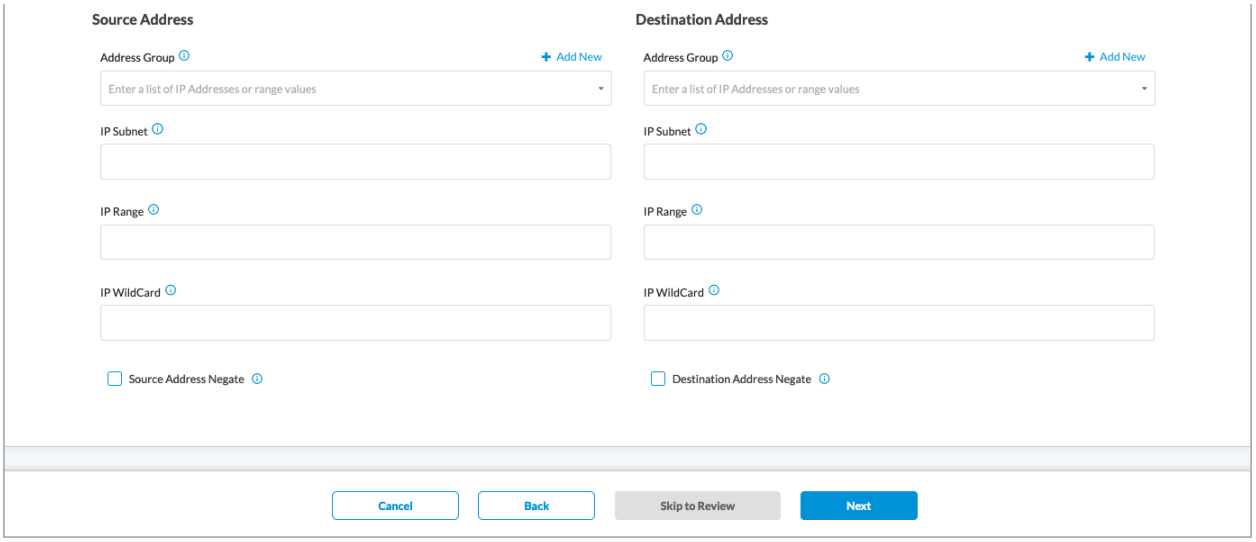


14. Click Add.
15. Click Next to go to the Network screen, or click Back to return to the Create TLS Decryption Rule screen, and then click Next. The following screen displays.

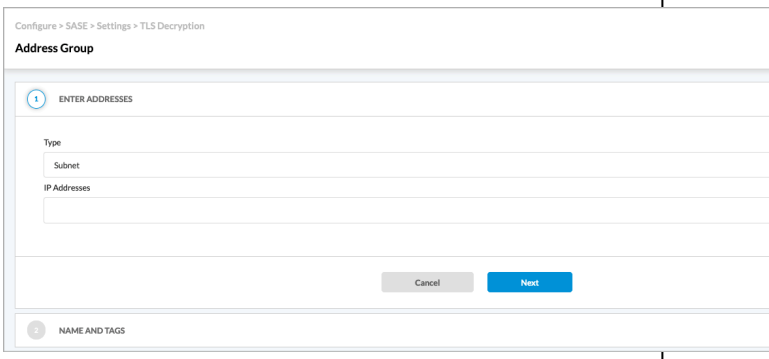
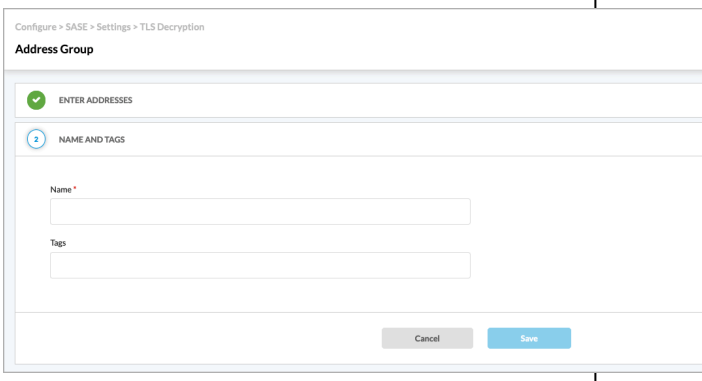


16. By default, all source and destination traffic is included in the match list. To change the source and destination traffic to include in the match list, click Customize under Source & Destination Traffic. In the Source & Destination Traffic screen, enter information for the following fields.



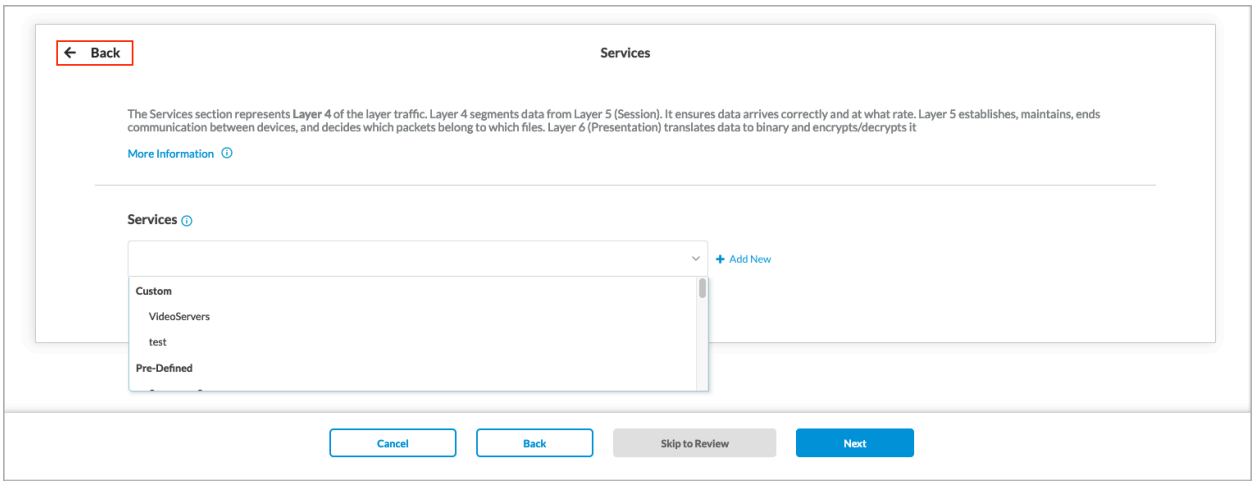


Field	Description
Source Zone	Select one or more source zones to include in the match list. By default, three source zones are available: ◦ SD-WAN Zone—Select if traffic comes from an SD-WAN device. ◦ User-defined zones—Select for zones, such as zones for IPsec or GRE tunnels. ◦ Versa Client—Select if traffic comes from a Versa Secure Access (VSA) client application.
Source Address (Group of Fields)	
◦ Address Group	Click in the box, and then select one or more address groups. These address groups are defined in the User Defined Objects section. 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. To create an address group, click + Add New, and then enter the following information.

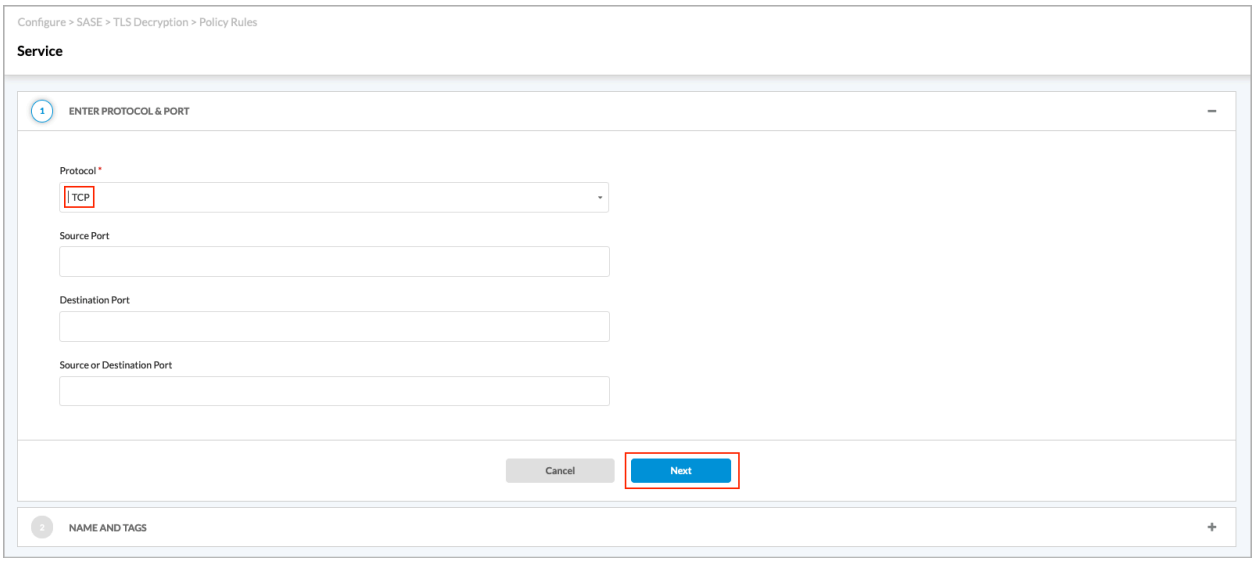
Field	Description
	 1. Click the Enter Addresses section, and then select the group Type. The type can be Subnet, IP range, IP wildcard, or IPv6 subnet. 2. Based on the type selected, enter one of the following and then press Return: —Subnet: One or more IP addresses and subnet masks, for example, 10.2.1.0/24 —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 3. To add additional IP address types, click the Plus icon. To remove an address type, click the Minus icon. 4. Click the Name and Tags section, and then enter a name for the address group and tags.  5. Click Save.

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.



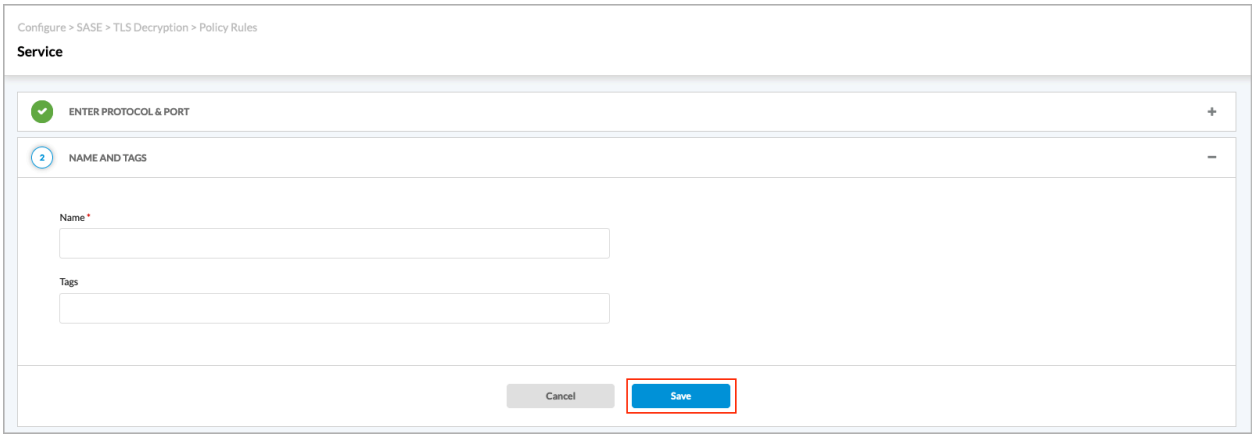
19. Select one or more of the predefined services. To add a custom service, click + Add New. The following screen displays.



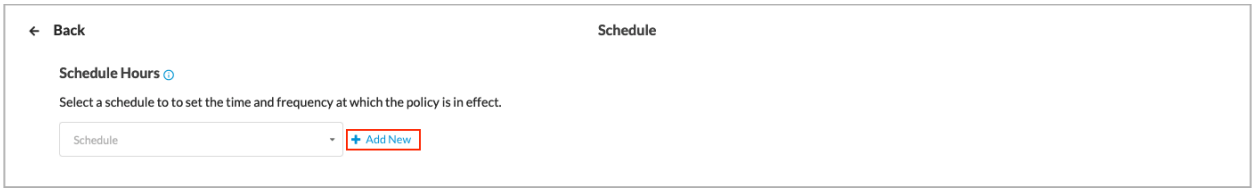
20. In the Protocol field, select a protocol. If you select TCP, UDP, or TCP and UDP, enter information for the following fields.

Field	Description
Source Port	Enter the source port number. *Range*: 0 through 65535 *Default*: None
Destination Port	Enter the destination port number. *Range*: 0 through 65535 *Default*: None
Source or Destination Port	Enter the source or destination port number. *Range*: 0 through 65535 *Default*: None

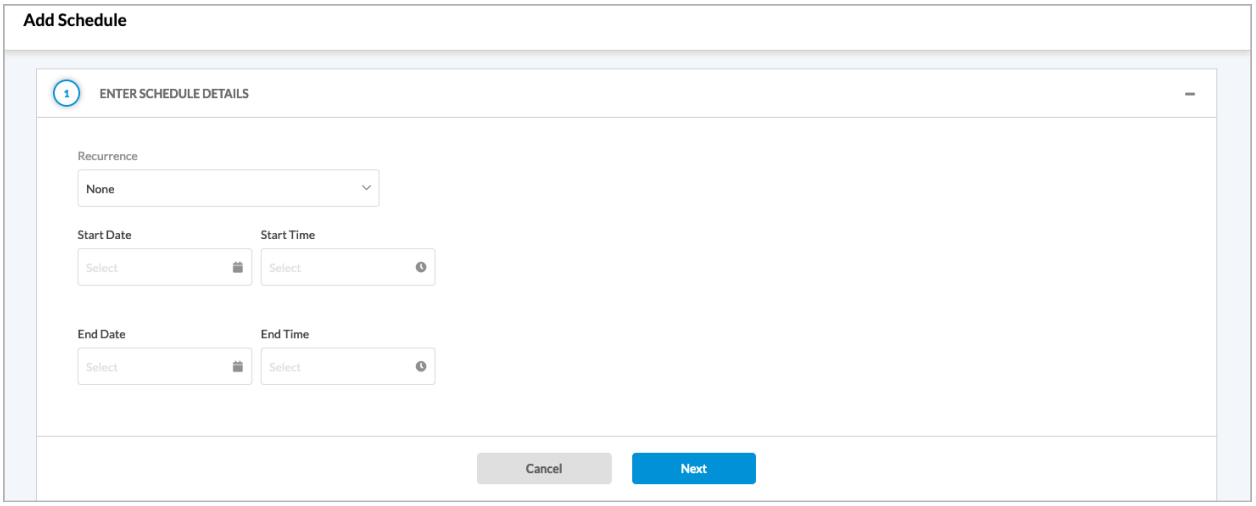
21. Click Next. The Name and Tags section displays.



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.

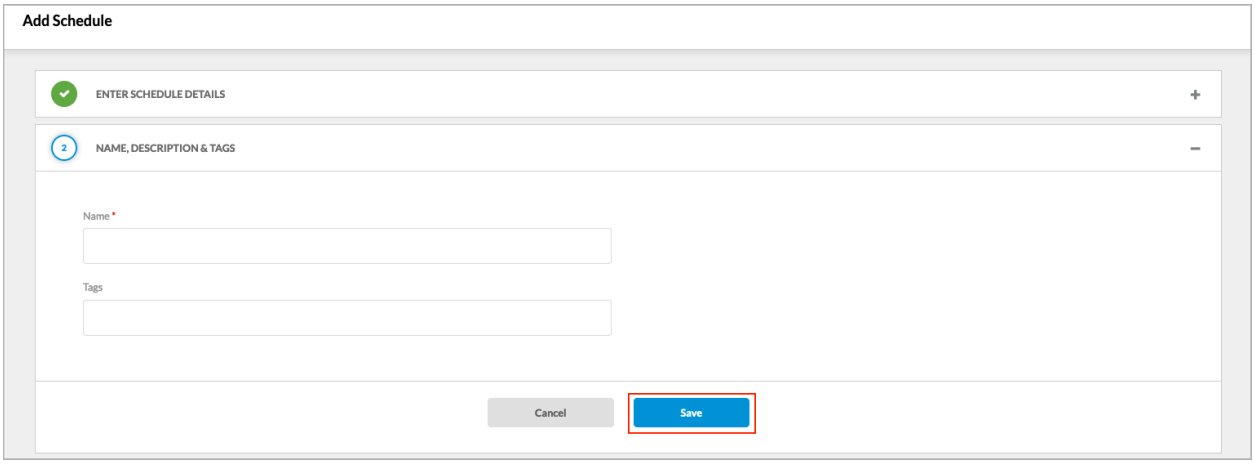


26. Click the drop-down list under Schedule Hours to select a schedule. If no schedules exist, create one by clicking + Add New. Under Enter Schedule Details, enter information for the following fields.

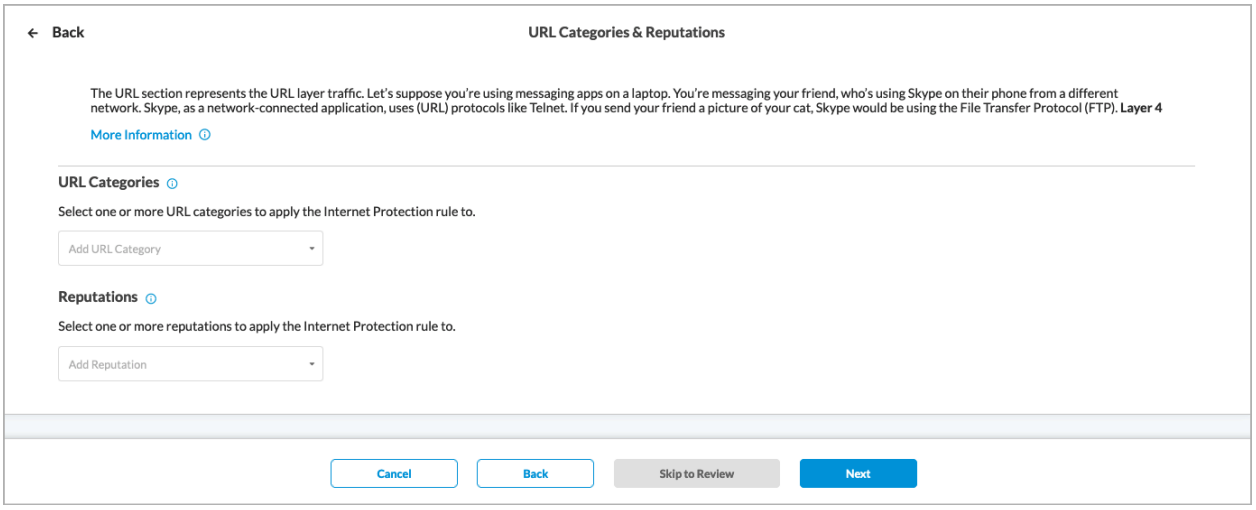


Field	Description
Recurrence	Select None, Daily, or Weekly.
Start Time	Enter the start time for the policy to be in effect.
End Time	Enter the end time for the policy to be in effect.
Days of the Week	If you select the recurrence to be weekly, select the days of the week for the policy to be in effect. 

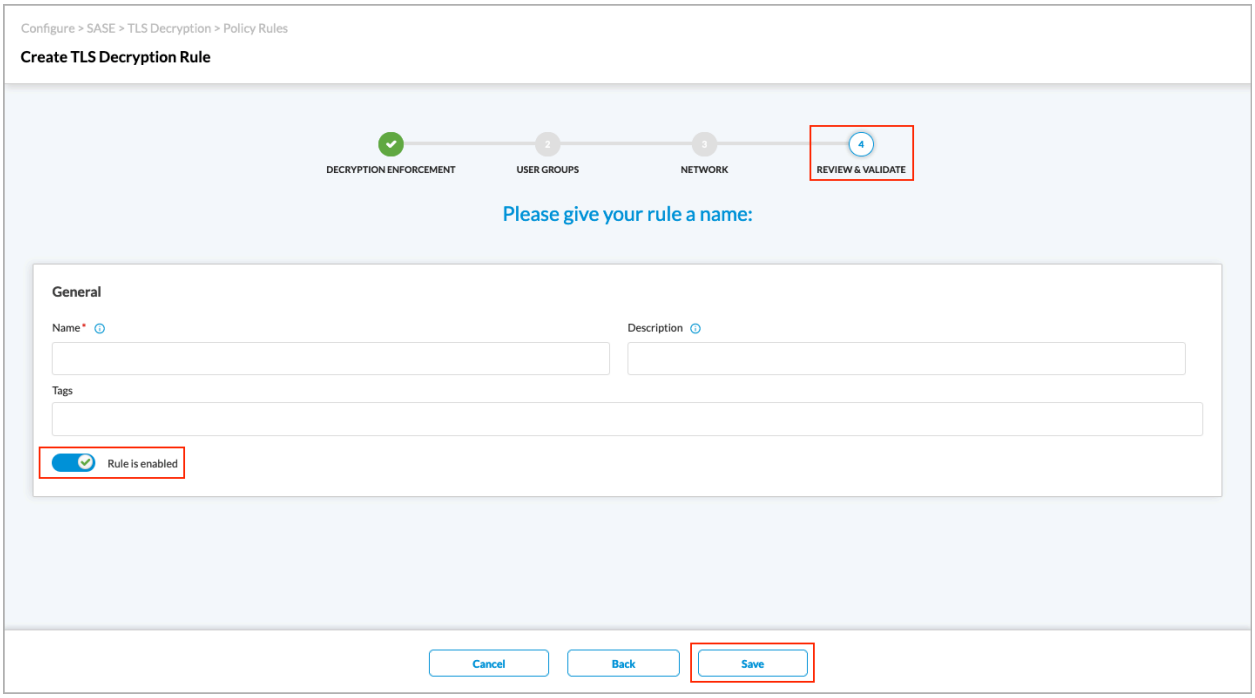
27. Click Next. The Name and Tags section displays.



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.



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.



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	Click the slider to enable the rule.  Click the slider again to disable the rule. 

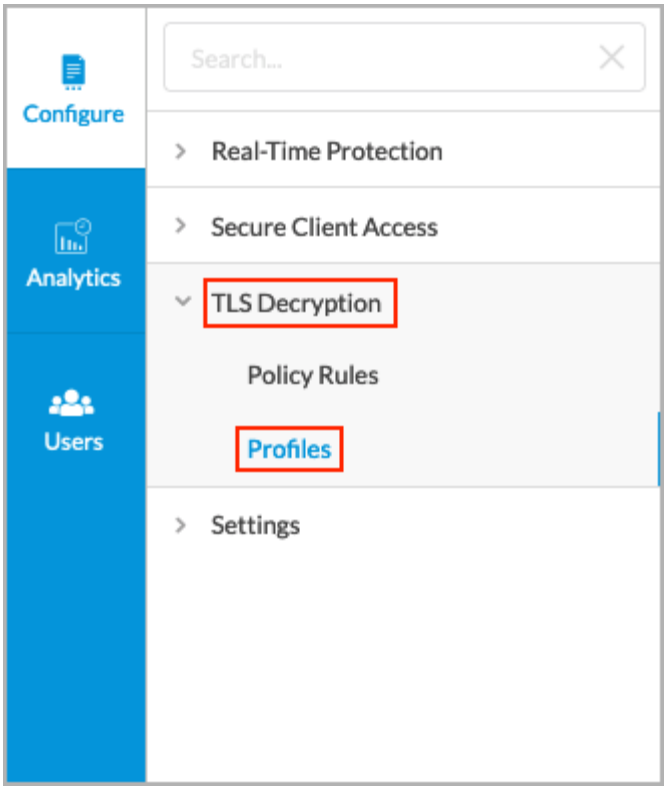
35. Click Save.

Create a TLS Decryption Profile

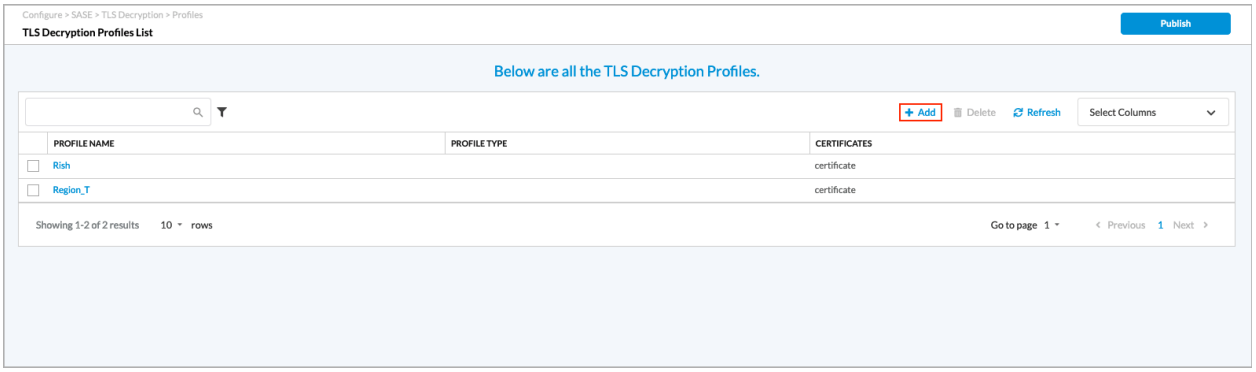
When you configure TLS decryption for a tenant, the VOS device behaves as an SSL proxy, and it generates a TLS/SSL certificate for each HTTPS URL that the tenant tries to access (for example, https://example.com). The certificate allows the VOS device to inspect the data flow and take any necessary actions. 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:

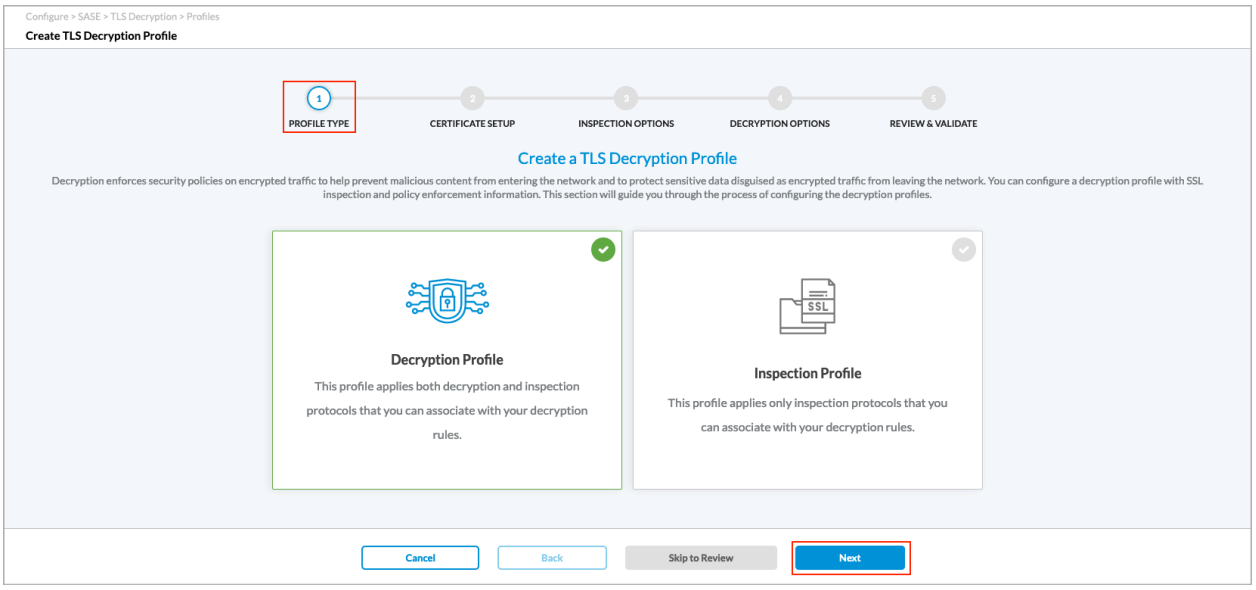
1. Go to Configure > TLS Decryption > Profiles.



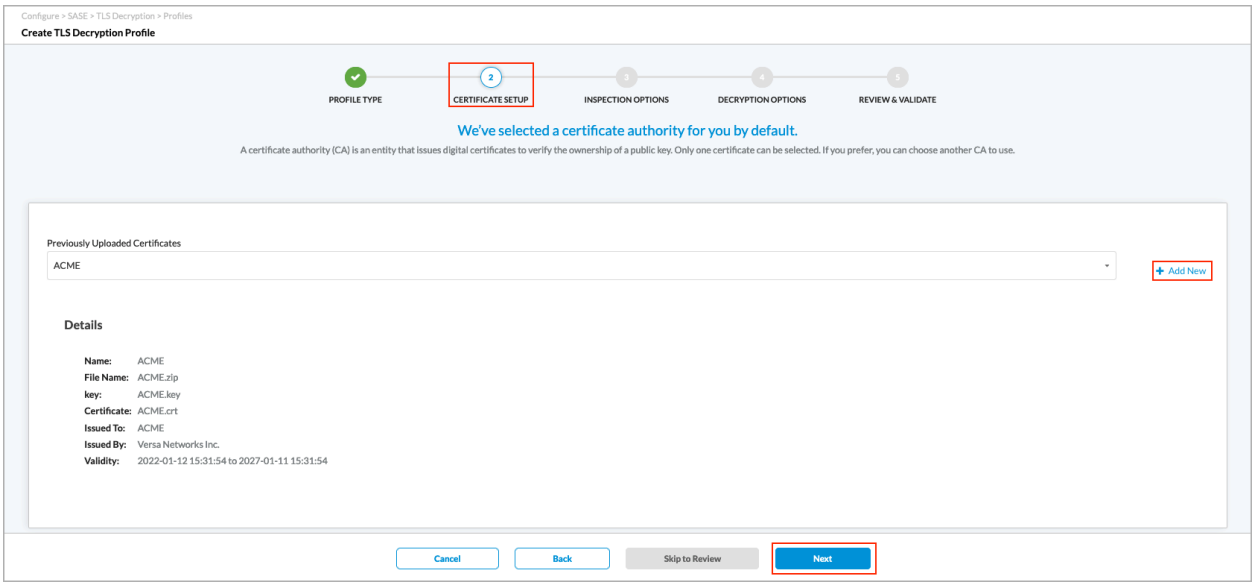
The TLS Decryption Profiles List screen displays all current profiles.



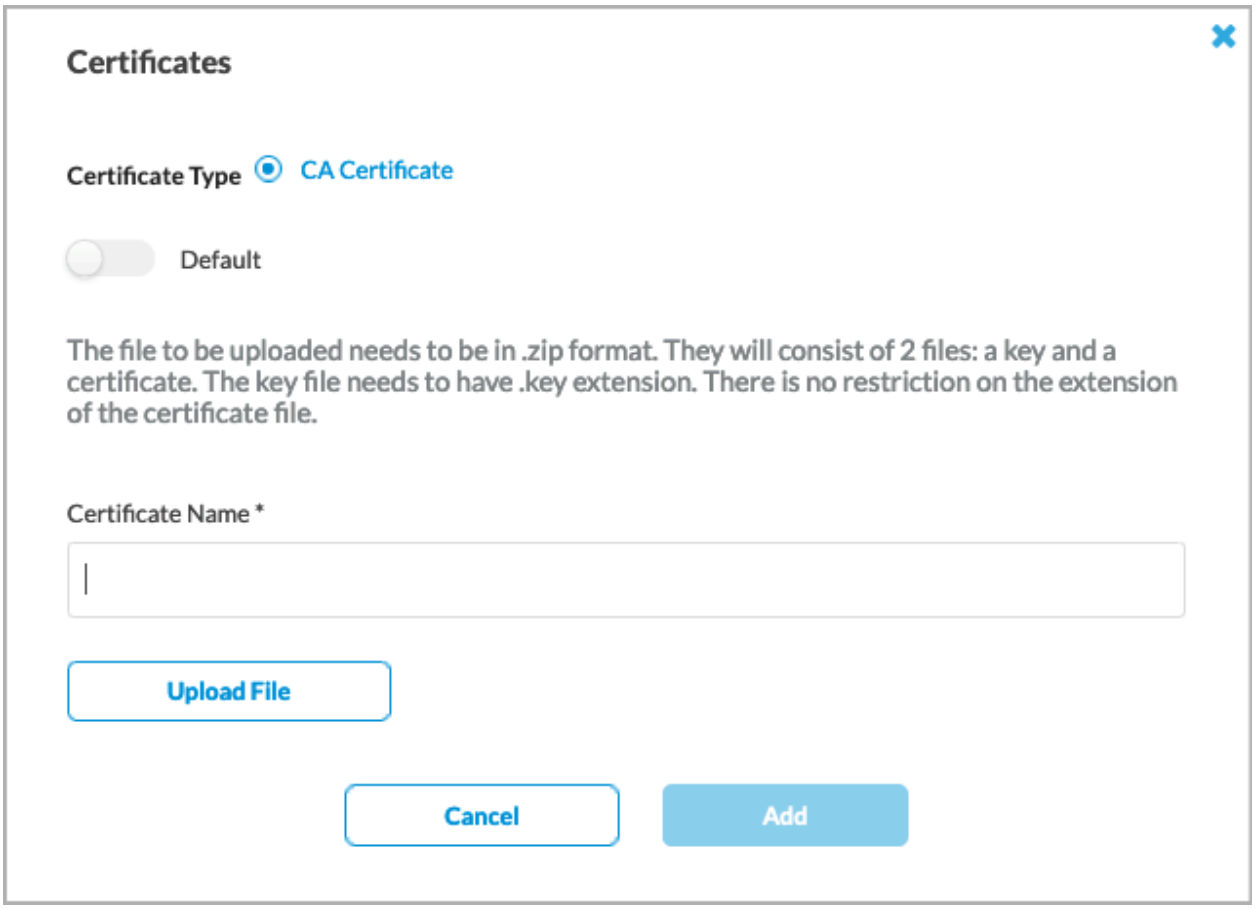
2. Click + Add New to add a TLS decryption profile. The Create TLS Decryption Profile screen displays with the first step, Profile Type, selected by default. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive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



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.

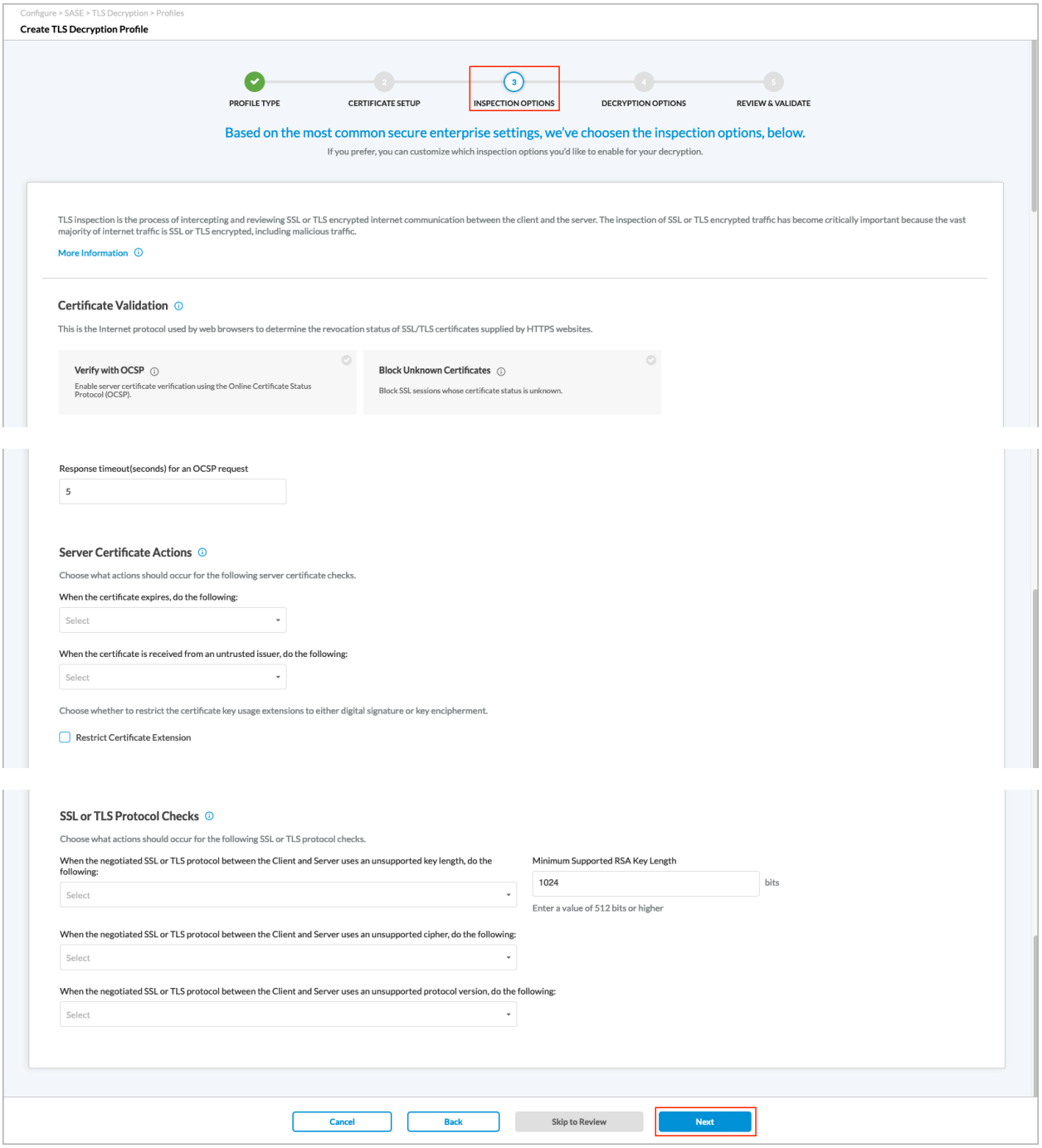


5. Click Next to accept the default certificate authority (CA). To use a different CA, select one of the previously uploaded certificates, or click + Add New to configure a new CA. In the Certificates popup window, enter information for the following fields.



Field	Description
Certificate Type	Click CA Certificate.
Default slide	Click the slider to have the added CA certificate to be the default CA certificate. 
Certificate Name	Enter a name for the certificate.
Upload File	Click to upload a CA certificate file.
Add	Click to add the new certificate.

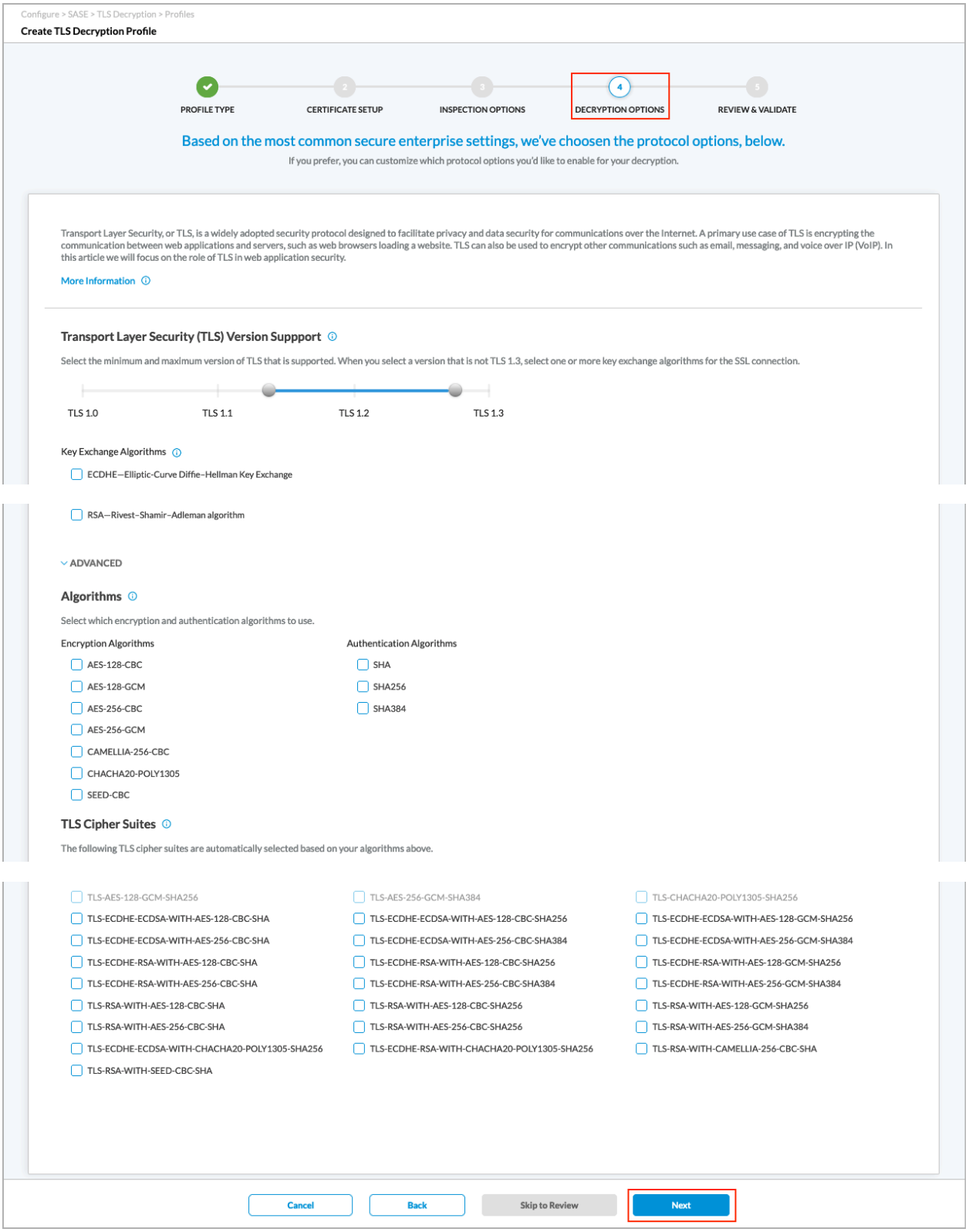
6. Click Next to go to Step 3, Inspection Options.



Field	Description
Certificate Validation (Group of Fields)	
◦ Verify with OCSP	Select to use the Online Certificate Status Protocol (OCSP) to verify a server certificate.

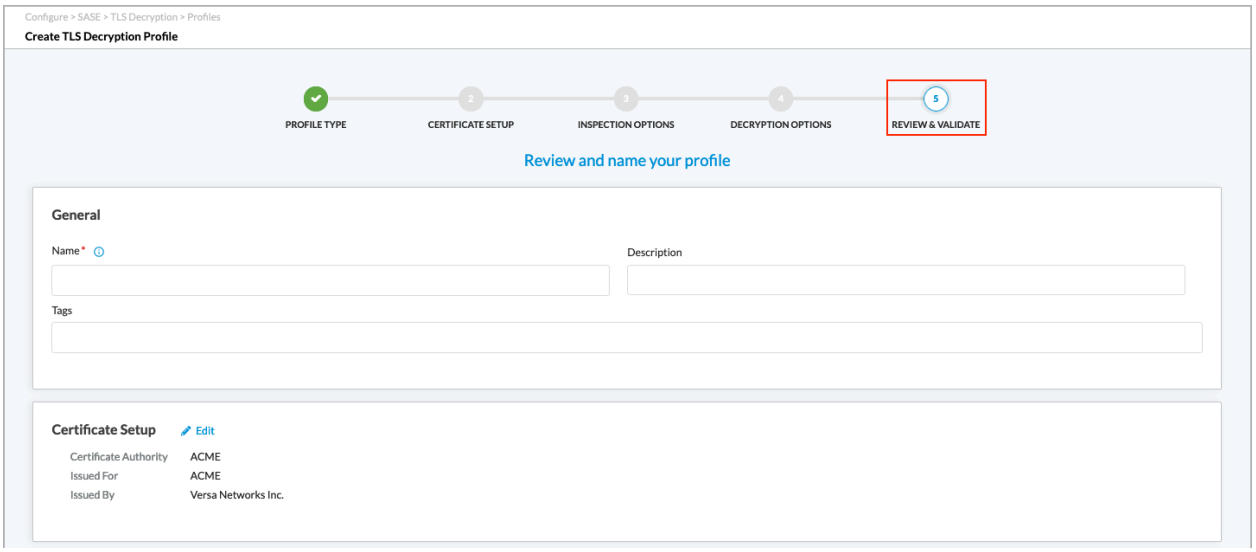
Field	Description
◦ Block Unknown Certificates	Select to block SSL sessions whose certificate status is unknown.
◦ Response timeout (seconds) for an OCSP request	Enter how long, in seconds, before an OCSP request times out. *Default*: 5 seconds *Range*: 1 to 255 seconds
Server Certificate Actions (Group 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	Section 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. *Default*: 1024 bit *Range*: 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.

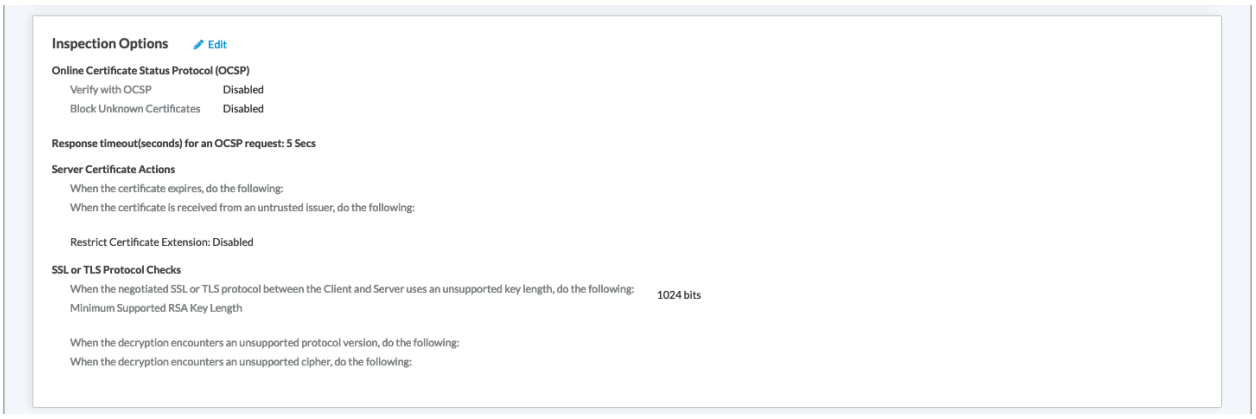
7. Click Next to go to Step 4, Decryption Options, and then enter information for the following fields.

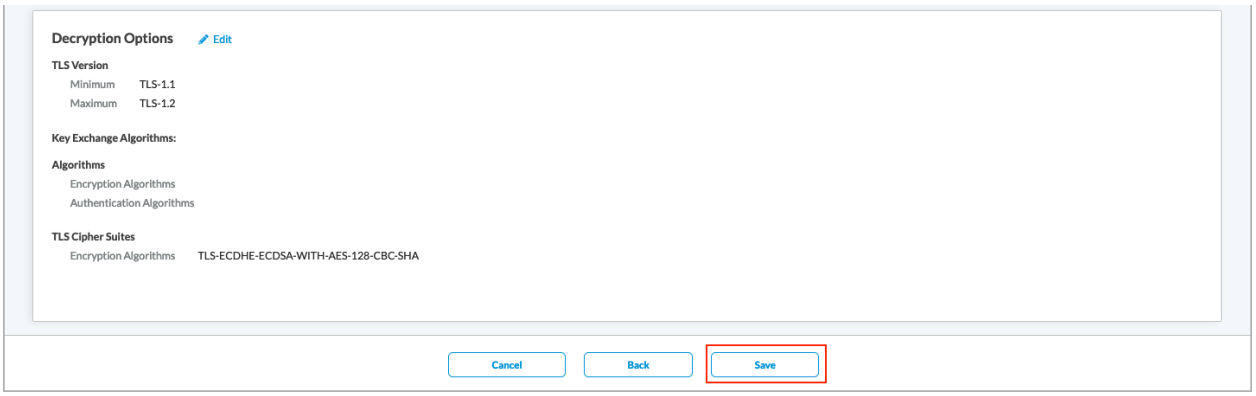


Field	Description
Transport Layer Security (TLS) Version Support (Group of Fields	
◦ Minimum and maximum version of TLS that is supported	Use the slider to select the minimum and maximum TLS version that is supported. If you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.
◦ Key Exchange Algorithms	Select one or more key exchange algorithms: ◦ 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.







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.

9. Review the Certificate Setup, Inspection Options, and Encryption Option sections.
10. To change any of the information, click the Edit icon in the section and then make the required changes.
11. 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
.*.onepagecrm.com	onepagecrm: 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
fesl.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	itune-base,itunes-appstore,apple-appstore,itunes-m: pinned-cert
itunes.apple.com	itune-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