
Secure Communication for SD-WAN Devices and SASE Clients

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

Versa Networks SD-WAN secure edge devices, also called Versa Operating System™ (VOS™) devices, and the Versa SASE clients installed on end-user devices have built-in processes that run automatically. These processes establish the secure connections required to validate the secure edge and client devices and to authenticate the users who are allowed to access the enterprise's on-premises and cloud-hosted resources through the devices.

This article describes how the SD-WAN secure edge devices and SASE clients establish these secure connections, and it describes how to troubleshoot issues with establishing and maintaining the connections.

Secure Communication for Versa SD-WAN Devices

Secure Communication for Onboarding SD-WAN Secure Edge Devices

To allow secure communication between a Versa Networks SD-WAN secure edge (branch) device and the SD-WAN Controller node, the secure edge device establishes an IKEv2-based IPsec secure control plane connection with the Controller node. When you onboard secure edge devices using zero-touch provisioning (ZTP), ZTP ensures that the connection between the branch devices and the SD-WAN Controller nodes is secure. After this secure control plane tunnel is successfully established, branch-to-branch encrypted SD-WAN connections are automatically initiated without using IKE. This section discusses how the secure control plane tunnels are established between the SD-WAN secure edge devices and the SD-WAN Controller node.

To onboard on-premises and cloud-based SD-WAN devices, the VOS provisioning process occurs in two steps:

- Establish a prestaging IPsec tunnel—This tunnel is used to retrieve the full VOS device configuration from the Versa Director node and to download the latest software version to the secure edge device if a software upgrade is required.
- Establish a post-staging IPsec tunnel with VXLAN outer encapsulation.

The Versa SD-WAN solution supports genuine multitenancy, in which one component negotiates multiple independent IPsec tunnels. For simplicity, this article discusses a basic example for a single tenant.

In first step of the IKE-based IPsec negotiation, the ZTP process is triggered, as illustrated in the screenshot below. The IKE-based IPsec negotiation occurs in two phases:

- Phase 1—IKEv2 establishes a channel for control communication and sets up a security association (SA) on both sides of the connection
- Phase 2—IKEv2 sets up an IPsec SA that to use for data channel encryption. The data channel is used to transfer the full VOS device configuration and, if necessary, the new VOS software version to the secure edge device.

In Phase 1 of IKE-based IPsec negotiation, the SA exchanges two pairs of messages. The first pair, shown in the following screenshot, is sent as plain text and is used for the VOS device agree which security policy to use for the IKE SA. This SA pair includes the keying data, which uses the Diffie-Hellman algorithm to calculate the encryption key. A security parameter index (SPI) is assigned to identify the communication channel. In the example shown here, the connection uses the UDP protocol and port 500. If Network Address Translation–Traversal (NAT-T) is detected in the path, the UDP connection uses port 4500.

The screenshot displays a Wireshark packet capture of an IKEv2 Phase 1 negotiation. The left pane shows a list of packets, and the right pane shows the details of packet 27, which is an IKE_SA_INIT message. The details pane shows the Security Association (33) and the Key Exchange (34) payloads.

Packet 27: ZTP_auth_success.pcapng

- Frame 27: 327 bytes on wire (2616 bits), 327 bytes captured (2616 bits) on interface -, id 0
- Ethernet II, Src: 0c:26:31:ad:f0:02 (0c:26:31:ad:f0:02), Dst: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02)
- Internet Protocol Version 4, Src: 192.168.122.50, Dst: 192.168.122.179
- User Datagram Protocol, Src Port: 500, Dst Port: 500
- Internet Security Association and Key Management Protocol
 - Initiator SPI: 020005aea47dce67
 - Responder SPI: 0200000e1e202e475
 - Next payload: Security Association (33)
 - Version: 2.0
 - Exchange type: IKE_SA_INIT (34)
 - Flags: 0x20 (Responder, No higher version, Response)
 - Message ID: 0x00000000
 - Length: 285
 - Payload: Security Association (33)
 - Payload: Key Exchange (34)
 - Payload: Nonce (40)
 - Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
 - Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
 - Payload: Notify (41) - HTTP_CERT_LOOKUP_SUPPORTED
 - Payload: Notify (41) - IKEV2_FRAGMENTATION_SUPPORTED
 - Payload: Vendor ID (43) : Unknown Vendor ID
 - Payload: Vendor ID (43) : Unknown Vendor ID

The second pair of IKEv2 SA messages, shown in the following screenshot, is used to exchange identity information, and to encrypt and authenticate the payload of authentication data packet.

20	32.391948	0.0.0.0	255.255.255.255	DHCP	292 DHCP Discover - Transaction ID 0xf451b500
21	32.392499	192.168.122.1	255.255.255.255	DHCP	342 DHCP Offer - Transaction ID 0xf451b500
22	32.394448	0.0.0.0	255.255.255.255	DHCP	304 DHCP Request - Transaction ID 0xf551b500
23	32.395000	192.168.122.1	255.255.255.255	DHCP	342 DHCP ACK - Transaction ID 0xf551b500
24	32.859777	0c:26:31:2e:69:02	Broadcast	ARP	42 Who has 192.168.122.50? Tell 192.168.122.179
25	32.860236	0c:26:31:2e:69:02	0c:26:31:2e:69:02	ARP	42 192.168.122.50 is at 0c:26:31:2e:69:02
26	32.860502	192.168.122.179	192.168.122.50	ISAKMP	319 IKE_SA_INIT MID=00 Initiator Request
27	32.868325	192.168.122.50	192.168.122.179	ISAKMP	327 IKE_SA_INIT MID=00 Responder Response
28	32.870922	192.168.122.179	192.168.122.50	ISAKMP	586 IKE_AUTH MID=01 Initiator Request (fragment 1/2)
29	32.870957	192.168.122.179	192.168.122.50	ISAKMP	218 IKE_AUTH MID=01 Initiator Request (fragment 2/2)
30	32.873622	192.168.122.50	192.168.122.179	ISAKMP	406 IKE_AUTH MID=01 Responder Response
31	32.881845	192.168.122.179	192.168.122.50	ESP	118 ESP (SPI=0xb20067f2)
32	32.967406	192.168.122.50	192.168.122.179	ESP	118 ESP (SPI=0xb2002ad5)
33	33.170008	::	ff02::1:ff2e:6902	ICMPv6	
34	33.514226	192.168.122.50	192.168.122.179	ESP	
35	33.984807	ae:30:31:50:57:86	Spanning-tree-(for-bridges)_00	STP	
36	34.512134	192.168.122.50	192.168.122.179	ESP	
37	35.807376	192.168.122.50	192.168.122.179	ESP	
38	35.808811	192.168.122.179	192.168.122.50	ESP	
39	35.809829	192.168.122.50	192.168.122.179	ESP	
40	35.813617	192.168.122.50	192.168.122.179	ESP	
41	35.825315	192.168.122.179	192.168.122.50	ESP	
42	35.825374	192.168.122.179	192.168.122.50	ESP	
43	35.826432	192.168.122.50	192.168.122.179	ESP	
44	35.827538	192.168.122.50	192.168.122.179	ESP	

<p>> Frame 30: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface -, id 0</p> <p>> Ethernet II, Src: 0c:26:31:ad:f0:02 (0c:26:31:ad:f0:02), Dst: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02)</p> <p>> Internet Protocol Version 4, Src: 192.168.122.50, Dst: 192.168.122.179</p> <p>> User Datagram Protocol, Src Port: 500, Dst Port: 500</p> <p>> Internet Security Association and Key Management Protocol</p> <p>Initiator SPI: 020000aea47dce67</p> <p>Responder SPI: 020000e1e202e475</p> <p>Next payload: Encrypted and Authenticated (46)</p> <p>> Version: 2.0</p> <p>Exchange type: IKE_AUTH (35)</p> <p>Flags: 0x20 (Responder, No higher version, Response)</p> <p>... 0... = Initiator: Responder</p> <p>... 0... = Version: No higher version</p> <p>..1.... = Response: Response</p> <p>Message ID: 0xb0000001</p> <p>Length: 364</p> <p>> Payload: Encrypted and Authenticated (46)</p> <p>Next payload: Identification - Responder (36)</p> <p>0... = Critical Bit: Not Critical</p> <p>.000 0000 = Reserved: 0x00</p> <p>Payload length: 336</p> <p>Initialization Vector: 3af534f6</p> <p>Encrypted Data</p>	<p>Wireshark - Packet 28 - ZTP_auth_success.pcapng</p> <p>> Frame 28: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on interface -, id 0</p> <p>> Ethernet II, Src: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02), Dst: 0c:26:31:ad:f0:02 (0c:26:31:ad:f0:02)</p> <p>> Internet Protocol Version 4, Src: 192.168.122.179, Dst: 192.168.122.50</p> <p>> User Datagram Protocol, Src Port: 500, Dst Port: 500</p> <p>> Internet Security Association and Key Management Protocol</p> <p>Initiator SPI: 020000aea47dce67</p> <p>Responder SPI: 020000e1e202e475</p> <p>Next payload: Encrypted and Authenticated Fragment (53)</p> <p>> Version: 2.0</p> <p>Exchange type: IKE_AUTH (35)</p> <p>Flags: 0x08 (Initiator, No higher version, Request)</p> <p>... 1... = Initiator: Initiator</p> <p>... 0... = Version: No higher version</p> <p>..0.... = Response: Request</p> <p>Message ID: 0xb0000001</p> <p>Length: 544</p> <p>> Payload: Encrypted and Authenticated Fragment (53)</p> <p>Next payload: Identification - Initiator (35)</p> <p>0... = Critical Bit: Not Critical</p> <p>.000 0000 = Reserved: 0x00</p> <p>Payload length: 516</p> <p>Fragment Number: 1</p> <p>Total Fragments: 2</p>
--	--

0000	0c 26 31 ad f0 02 0c 26 31 2e 69 02 00 00 45 00	-&1...&1.i...E-
0010	02 3c ee 97 00 00 40 11 13 e3 c0 a8 7a b3 c0 a8	-<...@...2...-
0020	7a 32 01 f4 01 f4 02 28 e8 8c 02 00 05 ae a4 7d	22....{.....}

After the IKEv2 negotiation is completed, Phase 1 of the negotiation is done, and Phase 2 begins. In Phase 2, an IPsec channel forms using the defined initiator and responder SPIs, and then the devices agree on the configured IPsec SA. Phase 2 negotiation and data flow are encrypted using the ESP protocol.

Verify the Onboarding Process

You can verify and monitor the onboarding process from the Tasks menu in the Director GUI. In Director view, click the

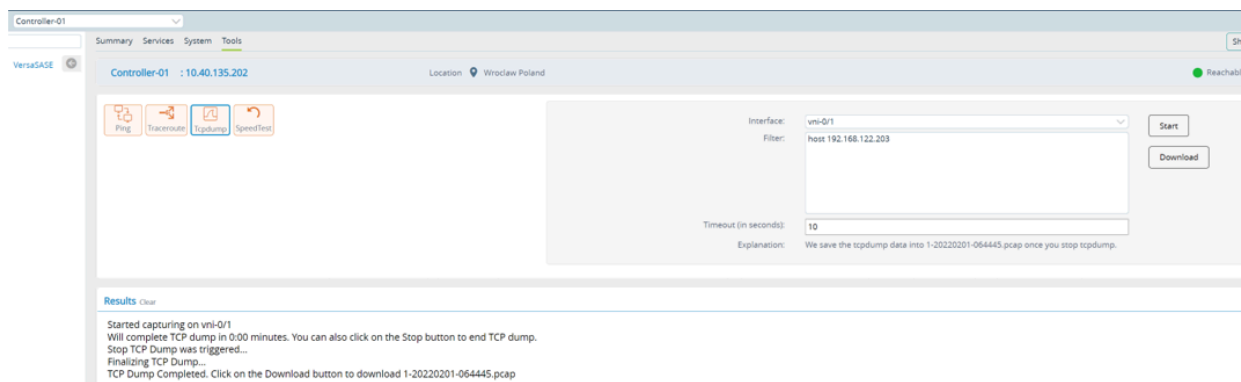


Tasks icon in the top menu bar. The Tasks popup window displays:

Tasks								
Failed 1 Pending 0 In Progress 0 Success 58 Total 59								
<input type="checkbox"/>	>	ID	User	Activity	Time		Description	Progress
					Start Time	End Time		
<input type="checkbox"/>	>	314	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	313	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	312	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	311	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	310	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	309	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	308	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	307	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	306	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	305	Administrator	Sync Config From v...	Thu, Mar 17 2022, 1...	Thu, Mar 17 2022, 1...	Sync Config From v...	✓
<input type="checkbox"/>	>	304	Administrator	Sync Config From v...	Thu, Mar 17 2022, 0...	Thu, Mar 17 2022, 0...	Sync Config From v...	✓
<input type="checkbox"/>	>	303	Administrator	Sync Config From v...	Wed, Mar 16 2022, ...	Wed, Mar 16 2022, ...	Sync Config From v...	✓

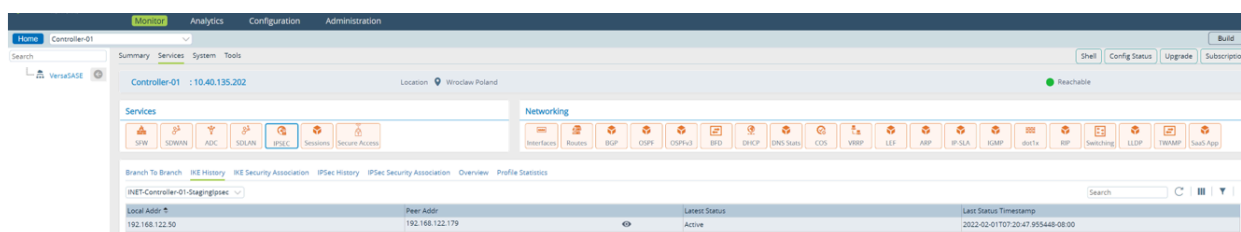
If the Tasks window does not display the onboarding process or does not show that the onboarding process has started, there is an issue with the initial IKEv2 SA or the IPsec SA. To troubleshoot this issue, you start the ZTP process and then run the tcpdump tool on the public interface of a staging Controller node, filtering the public host IP address of the remote branch device. To run tcpdump:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliance in the left menu bar.
 - c. Select the staging Controller device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the Tools tab, and click Tcpdump.
4. In the Interface field, select the interface.
5. In the Filter field, enter the IP address of the remote branch device.
6. Click Start. For more information, see [Access Monitoring Tools](#).
7. In the Results pane, verify that the the IKEv2 SA exchange has completed and that ESP packets have been sent. Check the Initiator and Responder SPI values to ensure that the ESP data plane traffic flows are in the same session.



To check the IKEv2 and IPsec SA validity and history:

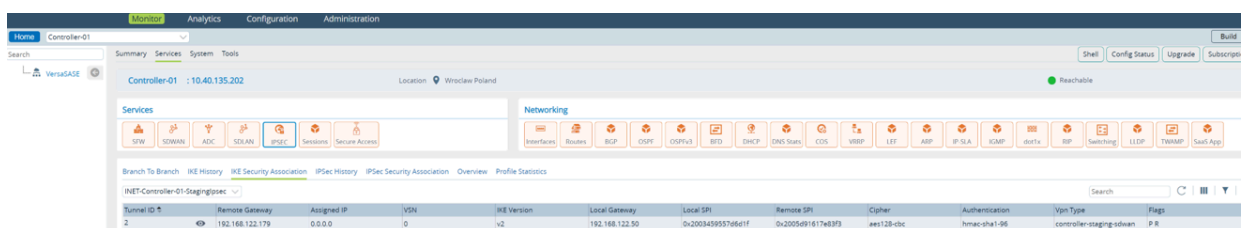
1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select the staging Controller device in the main pane. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the Services tab in the horizontal menu bar.
4. Select IPsec > IKE History, and then select an entity to view its IKE history. For more information, see [Monitor Device Services](#).



5. Click the Eye icon to view details about the negotiation.

To view the IKE SA:


1. Select the Monitor tab in the top menu bar.
2. Select the Services tab in the horizontal menu bar.
3. Select IPsec > IKE Security Association, and then select an entity to view its IKE SAs. For more information, see [Monitor Device Services](#).



https://docs.versa-networks.com/Reference/Architecture/Secure_Communication_for_SD-WAN_Devices_and_SASE_Clients

Updated: Thu, 24 Oct 2024 10:54:21 GMT

Copyright © 2024, Versa Networks, Inc.

- Click the  Eye icon to view details about the SAs.

You can view more details in the IPsec logs. To review the logs, log in to the Controller or branch shell, and check the `/var/log/versa/versa-ipsec.log` file.

Secure Communication for Provisioning VOS Devices

After the initial device configuration, the VOS devices in the secure SD-WAN network are provisioned. The VOS software creates an SD-WAN control virtual router (VR) for each available tenant. This VR is a transport-agnostic routing instance that uses point-to-multipoint (P2MP) interfaces to dynamically build the SD-WAN overlay network.

Each branch device has two tunnel virtual interfaces (TVI) interfaces:

- TVI for clear-text communication—The clear-text TVI tunnel exchanges the IPsec rekey negotiation parameters that maintain the encrypted tunnels. These exchanges are done in accordance with industry standards.
- TVI for encrypted communication—The post-staging dynamic IPsec encrypted tunnel is established in a control VR.

For both clear-text and encrypted TVI tunnels, VXLAN encapsulation is added, with the VOS-specific values in the Protocol field. VXLAN encapsulation also facilitates NAT-T functionality, by encapsulating the ESP packet inside the UDP 4790 packet. The following example shows a sample post-staging VXLAN encapsulation.

No.	Type	Source	Destination	Protocol	Length	Info
21. 170.201119		0c:26:31:ad:f0:02	0c:26:31:2e:69:02	ARP	42	192.168.122.50 is at 0c:26:31:ad:f0:02
21. 170.201313		192.168.122.203	192.168.122.50	VxLAN	166	
21. 171.999971		ae:30:31:50:57:06	Spanning-tree-(for-bridges_	STP	52	Conf. Root = 32768/0/52:54:00:44:b9:a7 Cost = 0 Port = 0x0003
21. 172.198613		192.168.122.203	192.168.122.50	VxLAN	166	
21. 172.210576		192.168.122.50	192.168.122.203	VxLAN	198	
21. 172.210906		192.168.122.203	192.168.122.50	VxLAN	198	
21. 172.512095		0c:26:31:ad:f0:02	LLDP Multicast	LLDP	225	PA/0a:31:ad:f0:00:00 IN/vni-0/1 120 SysN-Controller-01 SysD-versa-flexvni-20210910-060056-0045128_
21. 172.973152		192.168.122.50	192.168.122.203	VxLAN	134	
21. 173.472027		192.168.122.50	192.168.122.203	VxLAN	154	
21. 173.474894		192.168.122.50	192.168.122.203	VxLAN	342	
21. 173.477389		192.168.122.50	192.168.122.203	VxLAN	142	
21. 173.479730		192.168.122.50	192.168.122.203	VxLAN	162	
21. 173.519929		192.168.122.50	192.168.122.203	VxLAN	142	
21. 173.520956		192.168.122.50	192.168.122.203	VxLAN	1034	
21. 173.523402		192.168.122.50	192.168.122.203	VxLAN	142	
21. 173.563890		192.168.122.50	192.168.122.203	VxLAN	1134	
21. 173.808931		192.168.122.50	192.168.122.203	VxLAN	1514	
21. 173.983946		ae:30:31:50:57:06	Spanning-tree-(for-bridges_	STP	52	Conf. Root = 32768/0/52:54:00:44:b9:a7 Cost = 0 Port = 0x0003
21. 174.709058		192.168.122.203	192.168.122.50	VxLAN	198	
21. 174.709506		192.168.122.50	192.168.122.203	VxLAN	198	
21. 174.731580		192.168.122.50	192.168.122.203	VxLAN	162	

```

> Frame 2101: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on Interface -, id 0
> Ethernet II, Src: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02), Dst: 0c:26:31:ad:f0:02 (0c:26:31:ad:f0:02)
> Internet Protocol Version 4, Src: 192.168.122.203, Dst: 192.168.122.50
> User Datagram Protocol, Src Port: 4790, Dst Port: 4790
> Virtual eXtensible Local Area Network
  > Flags: 0xic
    Reserved: 36864
    Next Protocol: Unknown (251)
    VXLAN Network Identifier (VNI): 25889
    Reserved: 192
  > Data (116 bytes)

```

After the VXLAN encapsulation is decoded, the payload remains encrypted with ESP. The following example shows the post-staging ESP encryption inside VXLAN.

No.	Time	Source	Destination	Protocol	Length	Info
2099	170.200803	0c:26:31:2e:69:02	Broadcast	ARP	42	42 Who has 192.168.122.50? Tell 192.168.122.203
2100	170.201119	0c:26:31:ad:f0:02	0c:26:31:2e:69:02	ARP	42	192.168.122.50 is at 0c:26:31:ad:f0:02
2101	170.201313	192.168.122.203	192.168.122.50	ESP	166	ESP (SPI=0x020024bc)
2102	171.000971	ae:30:31:50:57:86	Spanning-tree (for-bridges)_00	STP	52	Conf. Root = 32768/0/52:54:00:44:09:a7 Cost = 0 Port = 0x0003
2103	172.198613	192.168.122.203	192.168.122.50	ESP	166	ESP (SPI=0x020024bc)
2104	172.210576	192.168.122.50	192.168.122.203	ESP	198	ESP (SPI=0x02000343)
2105	172.210906	192.168.122.203	192.168.122.50	ESP	198	ESP (SPI=0x020024bc)
2106	172.512915	0c:26:31:ad:f0:02	192.168.122.50	LLDP	228	0x00-01-01-00-00-00 In/vni-0/1 120 SysN-Controller-01 SysD-versa-flavmf-20210910-060056-0045128-21.2.2 versio...
2107	172.973152	192.168.122.50	192.168.122.203	ESP	134	ESP (SPI=0x02000343)
2108	173.472027	192.168.122.50	192.168.122.203	ESP	154	ESP (SPI=0x02000343)
2109	173.474894	192.168.122.50	192.168.122.203	ESP	342	ESP (SPI=0x02000343)
2110	173.477389	192.168.122.50	192.168.122.203	ESP	142	ESP (SPI=0x02000343)
2111	173.479730	192.168.122.50	192.168.122.203	ESP	162	ESP (SPI=0x02000343)
2112	173.519929	192.168.122.50	192.168.122.203	ESP	142	ESP (SPI=0x02000343)
2113	173.520956	192.168.122.50	192.168.122.203	ESP	1034	ESP (SPI=0x02000343)
2114	173.523482	192.168.122.50	192.168.122.203	ESP	142	ESP (SPI=0x02000343)
2115	173.563800	192.168.122.50	192.168.122.203	ESP	1134	ESP (SPI=0x02000343)
2116	173.800931	10.255.0.1	10.255.0.5	UDP	1514	65265 - 65265 len=1420
2117	173.983946	ae:30:31:50:57:86	Spanning-tree (for-bridges)_00	STP	52	Conf. Root = 32768/0/52:54:00:44:09:a7 Cost = 0 Port = 0x0003
2118	174.709058	192.168.122.203	192.168.122.50	ESP	198	ESP (SPI=0x020024bc)
2119	174.709506	192.168.122.50	192.168.122.203	ESP	198	ESP (SPI=0x02000343)
2120	174.711500	192.168.122.50	192.168.122.203	ESP	162	ESP (SPI=0x02000343)
2121	174.735154	192.168.122.50	192.168.122.203	ESP	154	ESP (SPI=0x02000343)

> Frame 2116: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface -, id 0
 > Ethernet II, Src: 0c:26:31:ad:f0:02 (0c:26:31:ad:f0:02), Dst: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02)
 > Internet Protocol Version 4, Src: 192.168.122.50, Dst: 192.168.122.203
 > User Datagram Protocol, Src Port: 4790, Dst Port: 4790
 > Versa Virtual Extended LAN, VNI: 0x112, Next Proto: 0x0b(vxlan-extension), Dst WQ ID: 0, Next Proto: 0x0d(gre)
 > Versa GRE Header
 > Versa MPLS Header
 > Internet Protocol Version 4, Src: 10.255.0.1, Dst: 10.255.0.5
 > User Datagram Protocol, Src Port: 65265, Dst Port: 65265
 > Data (1420 bytes)
 Data: 002008080eaca001121a00001200000010c0d1ea93031a00...
 [Length: 1420]

When a post-staging IPsec tunnel is established between a VOS device and an SD-WAN Controller, the VOS device establishes IPsec encrypted tunnels to other existing on-premises and cloud-hosted VOS devices without using IKE. To ensure that this process is fast and secure, VOS devices use IPsec negotiation without using IKE for branch-to-branch SD-WAN connections. The SD-WAN Controller sends an MP-BGP update to supply the VOS device with the required SA data, including Diffie-Hellman keys. The SD-WAN Controller also implements and centrally controls the rekey mechanism. Branch-to-branch dynamic IPsec negotiation without IKE avoids human errors related to SA configuration in a large full-mesh topology.

Secure Communication for Versa SASE Client

For Releases 20.2.3 and later.

The Versa SASE client installed on an end-user devices establishes an SD-WAN secure connection to authorize users. After the users are authorized, they can access on-premises and cloud-hosted resources.

Activating a new SASE client user is done in two steps:

1. The Versa SASE client registers on a Versa SASE portal. This registration is performed once, which is similar to the ZTP process for VOS devices and Versa cloud workloads, which is also performed only once.
2. The Versa SASE client establishes a secure connection to the Versa SASE gateway. The following example shows the details for SASE portal registration.

No.	Time	Source	Destination	Protocol	Length	Info
21	13.381499	192.168.122.164	192.168.122.203	TCP	66	49754 → 443 [SYN] Seq=0 Win=64288 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	13.382285	192.168.122.203	192.168.122.164	TCP	66	443 → 49754 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1448 WS=256 SACK_PERM=1
23	13.382678	192.168.122.164	192.168.122.203	TCP	54	49754 → 443 [ACK] Seq=1 Ack=1 Win=263424 Len=0
24	13.383443	192.168.122.164	192.168.122.203	TLSv1.2	235	Client Hello
25	13.388549	192.168.122.203	192.168.122.164	TLSv1.2	1435	Server Hello, Certificate, Server Key Exchange, Server Hello Done
26	13.392368	192.168.122.164	192.168.122.203	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	13.393079	192.168.122.203	192.168.122.164	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
28	13.395158	192.168.122.164	192.168.122.203	TLSv1.2	448	Application Data
29	13.396346	192.168.122.203	192.168.122.164	TLSv1.2	793	Application Data
30	13.406573	192.168.122.164	192.168.122.203	TCP	54	49754 → 443 [ACK] Seq=669 Ack=2172 Win=263424 Len=0
31	14.015955	52.00.7a:82:e1:93	Spanning-tree (for-bridges)_00	STP	52	Conf. Root = 32768/0/1a:47:94:15:f6:fd Cost = 0 Port = 0x8004
32	16.000044	52.00.7a:82:e1:93	Spanning-tree (for-bridges)_00	STP	52	Conf. Root = 32768/0/1a:47:94:15:f6:fd Cost = 0 Port = 0x8004
33	18.010819	52.00.7a:82:e1:93	Spanning-tree (for-bridges)_00	STP	52	Conf. Root = 32768/0/1a:47:94:15:f6:fd Cost = 0 Port = 0x8004
34	18.016004	1a:47:94:15:f6:fd	0c:26:31:96:f3:00	ARP	42	Who has 192.168.122.164? Tell 192.168.122.1
35	18.016424	0c:26:31:96:f3:00	1a:47:94:15:f6:fd	ARP	42	192.168.122.164 is at 0c:26:31:96:f3:00
36	19.863612	192.168.122.164	192.168.122.203	TLSv1.2	380	Application Data
37	19.864871	192.168.122.203	192.168.122.164	TCP	1502	443 → 49754 [ACK] Seq=2172 Ack=995 Win=64512 Len=1448 [TCP segment of a reassembled PDU]
38	19.864920	192.168.122.203	192.168.122.164	TLSv1.2	683	Application Data
39	19.864952	192.168.122.203	192.168.122.164	TCP	1502	443 → 49754 [ACK] Seq=4249 Ack=995 Win=64512 Len=1448 [TCP segment of a reassembled PDU]
40	19.864970	192.168.122.203	192.168.122.164	TLSv1.2	683	Application Data
41	19.864987	192.168.122.203	192.168.122.164	TLSv1.2	1159	Application Data
42	19.865326	192.168.122.164	192.168.122.203	TCP	54	49754 → 443 [ACK] Seq=995 Ack=7431 Win=263424 Len=0
43	19.869996	52.00.7a:82:e1:93	Spanning-tree (for-bridges)_00	STP	52	Conf. Root = 32768/0/1a:47:94:15:f6:fd Cost = 0 Port = 0x8004

```

> Ethernet II, Src: 0c:26:31:96:f3:00 (0c:26:31:96:f3:00), Dst: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02)
> Internet Protocol Version 4, Src: 192.168.122.164, Dst: 192.168.122.203
> Transmission Control Protocol, Src Port: 49754, Dst Port: 443, Seq: 1, Ack: 1, Len: 181
< Transport Layer Security
  < TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 176
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 172
      Version: TLS 1.2 (0x0303)
      Random: 628cd77aac6d50b14da3beebd7ca7fcbaf310d97fd97098e...
      Session ID Length: 0
      Cipher Suites Length: 42
      Cipher Suites (21 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 89
      Extension: server_name (len=30)
      Extension: supported_groups (len=8)
      Extension: ec_point_formats (len=2)
      Extension: signature_algorithms (len=20)
      Extension: session_ticket (len=0)
      Extension: extended_master_secret (len=0)
      Extension: renegotiation_info (len=1)

```

When a user connects to an organization for the first time using the Versa SASE client, the user must register on the SASE portal. After the registration is successful, the Versa SASE client receives a gateway policy configuration that allows the secure connection to access the organization's resources.

The registration process begins with a three-way handshake TCP connection to the Versa SASE portal, followed by TLS negotiation, which uses industry-standard protocols to establish an encrypted TLS connection. The end host validates the portal server certificate and sends the enterprise name and username to the server over an encrypted TLS connection.

Next, the SASE portal authenticates the user. The SASE portal first verifies the identity of the client and server, and then it pushes the enterprise gateway policy configuration to the Versa SASE client so that the client can securely connect to the enterprise network. This configuration includes the available SASE gateways and a legitimate gateway root CA certificate. This exchange is encrypted, as shown in the following example.

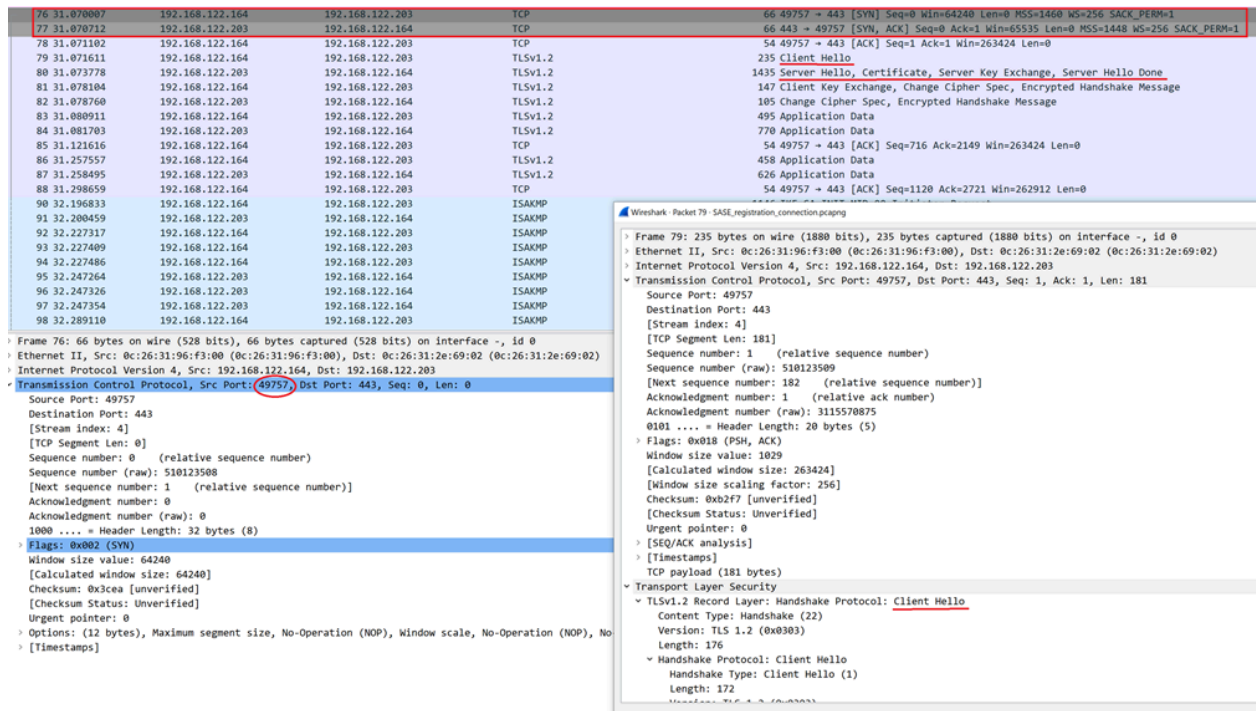
```

> Frame 28: 448 bytes on wire (3584 bits), 448 bytes captured (3584 bits) on interface -, id 0
> Ethernet II, Src: 0c:26:31:96:f3:00 (0c:26:31:96:f3:00), Dst: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02)
> Internet Protocol Version 4, Src: 192.168.122.164, Dst: 192.168.122.203
> Transmission Control Protocol, Src Port: 49754, Dst Port: 443, Seq: 275, Ack: 1433, Len: 394
< Transport Layer Security
  < TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 389
    Encrypted Application Data: 000000000000000016c429ef9256a64928b6f95fda5488fa2...

```

After the Versa SASE client successfully registers on the corporate SASE portal, the user can securely connect to the provisioned SASE gateways. These gateways can be SASE gateways hosted on-premises, multicloud gateways, or a combination of both. For the secure connection to a SASE gateway, during the registration process, the Versa SASE

client validates the installed CA certification to ensure that the gateway is legitimate. The following screenshot shows that the Versa SASE client establishes a new secure TLS session with the SASE gateway.



The screenshot above shows that even though the same VOS device provides both the SASE portal and gateway functions, the Versa SASE client establishes a new TCP session to the gateway. Then, a TLS session is established to encrypt further communication. The SASE gateway then sends its certificate, which is the certificate that was signed by the root CA certificate and that the Versa SASE client installed during the portal registration process. This signed certificate allows the SASE client to ensure the authenticity of the organization's gateway.

After the identify of the SASE gateway is confirmed, the client send its own authentication information. If the client authentication is successful, the Versa SASE gateway sends a one-time password (OTP) to the Versa SASE client. The following screenshot shows this process.

88 31.298659	192.168.122.164	192.168.122.203	TCP	54 49757 → 443 [ACK] Seq=1120 Ack=2721 Win=262912 Len=0
90 32.196833	192.168.122.164	192.168.122.203	ISAKMP	1146 IKE_SA_INIT MID=00 Initiator Request
91 32.200459	192.168.122.203	192.168.122.164	ISAKMP	412 IKE_SA_INIT MID=00 Responder Response
92 32.227317	192.168.122.164	192.168.122.203	ISAKMP	614 IKE_AUTH MID=01 Initiator Request (fragment 1/3)
93 32.227400	192.168.122.164	192.168.122.203	ISAKMP	614 IKE_AUTH MID=01 Initiator Request (fragment 2/3)
94 32.227486	192.168.122.164	192.168.122.203	ISAKMP	126 IKE_AUTH MID=01 Initiator Request (fragment 3/3)
95 32.247264	192.168.122.203	192.168.122.164	ISAKMP	582 IKE_AUTH MID=01 Responder Response (fragment 1/3)
96 32.247326	192.168.122.203	192.168.122.164	ISAKMP	582 IKE_AUTH MID=01 Responder Response (fragment 2/3)
97 32.247354	192.168.122.203	192.168.122.164	ISAKMP	486 IKE_AUTH MID=01 Responder Response (fragment 3/3)
98 32.289110	192.168.122.164	192.168.122.203	ISAKMP	130 IKE_AUTH MID=02 Initiator Request
99 32.291176	192.168.122.203	192.168.122.164	ISAKMP	178 IKE_AUTH MID=02 Responder Response
100 32.298530	192.168.122.164	192.168.122.203	ISAKMP	178 IKE_AUTH MID=03 Initiator Request
101 32.299773	192.168.122.203	192.168.122.164	ISAKMP	186 IKE_AUTH MID=03 Responder Response
102 32.302424	192.168.122.164	192.168.122.203	ISAKMP	114 IKE_AUTH MID=04 Initiator Request
103 32.303486	192.168.122.203	192.168.122.164	ISAKMP	138 IKE_AUTH MID=04 Responder Response
104 32.306514	192.168.122.164	192.168.122.203	ISAKMP	130 IKE_AUTH MID=05 Initiator Request
105 32.310858	192.168.122.203	192.168.122.164	ISAKMP	322 IKE_AUTH MID=05 Responder Response
114 32.374993	192.168.122.164	192.168.122.203	ESP	134 ESP (SPI=0x020036c4)
116 32.377643	192.168.122.164	192.168.122.203	ESP	150 ESP (SPI=0x020036c4)
121 32.384619	192.168.122.164	192.168.122.203	ESP	150 ESP (SPI=0x020036c4)

> Frame 90: 1146 bytes on wire (9168 bits), 1146 bytes captured (9168 bits) on interface -, id 0
 > Ethernet II, Src: 0c:26:31:96:f3:00 (0c:26:31:96:f3:00), Dst: 0c:26:31:2e:69:02 (0c:26:31:2e:69:02)
 > Internet Protocol Version 4, Src: 192.168.122.164, Dst: 192.168.122.203
 > User Datagram Protocol, Src Port: 500, Dst Port: 500
 > Internet Security Association and Key Management Protocol
 Initiator SPI: ac7d91b5bf56d64e
 Responder SPI: 0000000000000000
 Next payload: Security Association (33)
 > Version: 2.0
 > Exchange type: IKE_SA_INIT (34)
 > Flags: 0x08 (Initiator, No higher version, Request)
 > Message ID: 0x00000000
 > Length: 1104
 > Payload: Security Association (33)
 > Payload: Key Exchange (34)
 > Payload: Nonce (48)
 > Payload: Notify (41) - IKEV2_FRAGMENTATION_SUPPORTED
 > Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
 > Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP
 > Payload: Vendor ID (43) : MS NTS ISAKMP_OAKLEY
 > Payload: Vendor ID (43) : MS-Negotiation Discovery Capable
 > Payload: Vendor ID (43) : Microsoft Vid-Initial-Contact
 > Payload: Vendor ID (43) : Unknown Vendor ID


The next step is IKE negotiation, which uses the SASE gateway certificate to authenticate the gateway. The SASE client is authenticated using the OTP key that was generated and sent to the client. The key is sent in an encrypted format using the public key of the SASE gateway. The gateway decrypts this key using its own private key and compares it to the local copy of the OTP key from the SASE portal. After the gateway authenticates the Versa SASE client, the IKE negotiation is complete, and the IPsec Phase 2 negotiation creates a secure tunnel with the SASE gateway.

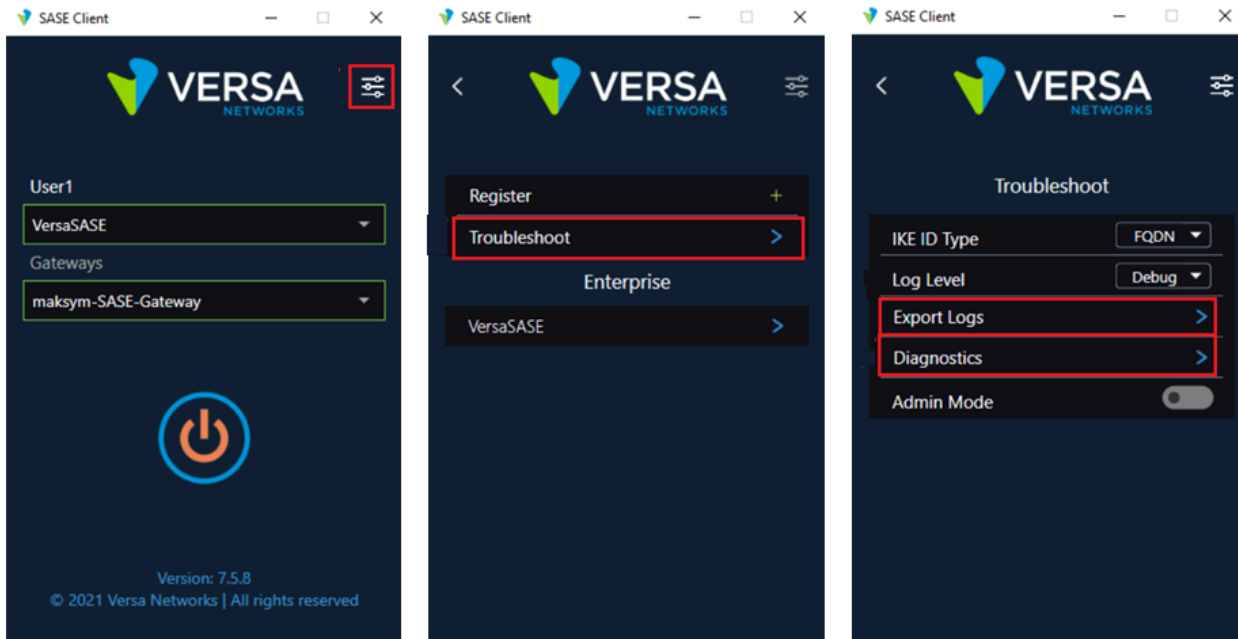
Troubleshoot the SASE Client

For Releases 20.2.3 and later.

Versa SASE client provides tools for troubleshooting issues during the registration or connection process.

To perform diagnostics and to troubleshoot the SASE client:

1. In the SASE client home screen, click the  Settings icon.
2. Click Troubleshoot, and then click Diagnostics to run diagnostics tests. These tests ensure that all necessary services are running on the host OS, and they generate a log file, in .zip format, that includes the test results.
3. Click Export Logs to download the diagnostics log file. You can use the information in the log files to validate end host issues like such as the blocking of firewall or antivirus connections and the supported IPsec encryption methods. For more information, see [Perform Diagnostics and Export Logs](#).



Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 20.2.3 and later add support for SASE clients.

Additional Information

[Access Monitoring Tools](#)

[Configure EVPN VXLAN](#)

[Monitor Device Services](#)

[Use the Versa SASE Client Application](#)