Improving the End User Experience when Using Azure Active Directory and MFA

For supported software information, click here.

This solution article describes how to use multifactor authentication (MFA) in Azure Active Directory along Versa Secure SD-WAN local breakout (LBO) to improve the end user experience of an organization's employees while allowing network administrators to centrally manage network access and authentication requests.

Azure Active Directory and MFA Overview

Azure Active Directory (AD) is an Identity as a Service (IDaaS) solution that builds on the concepts of Active Directory Domain Services (AD DS), which was first introduced in Windows 2000 and is sometimes referred to as Active Directory version 1. Both Active Directory Domain Services and the newer Azure Active Directory, sometimes referred to as Active Directory version 2, allow organizations to manage on-premises infrastructure components and systems using a single identity for each user. Azure Active Directory, which is also referred to as a cloud-based identity and access management (IAM) service, helps an organization's employees access both internal and external resources, such as Microsoft 365, the Azure portal, and SaaS applications that have been integrated with the IAM platform.

To further secure user sign-in events in Azure Active Directory, you can enable multifactor authentication (MFA) for your organization. MFA helps safeguard access to data and applications, providing another layer of security by using a second form of authentication.

Organizations can enable MFA and then apply exceptions to when MFA rules apply. This approach blends the additional layer of security provided by MFA together with an improved end user experience. For example, if an end user is connected to the corporate network and the corporate network is trusted, you can disable MFA. Disabling MFA also improves the end user experience, because fewer steps are required to access resources from trusted sources.To apply exceptions, you use MFA trusted IPs, which bypass MFA prompts for end users who sign in from a predefined range of IP addresses. As an example, organizations can set trusted IP address ranges for all on-premises environments. The result is that when end users are accessing resources from one of these locations, there is no Azure Active Directory MFA prompt.

Secure SD-WAN and Internet Access Overview

Versa Secure SD-WAN allows organizations to access the internet locally from local branches rather than centrally, either at the data center or corporate headquarters. While this local access improves the end user experience, the list of trusted IP addresses for MFA bypass dramatically increases because each branch now presents users directly to the Azure Active Directory platform.

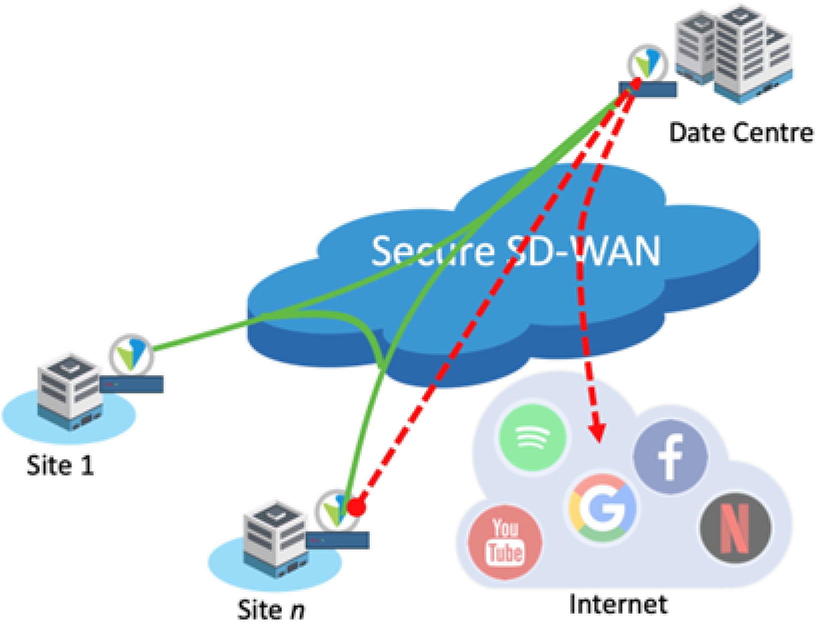
To address this issue, you can configure Secure SD-WAN so that authentication requests are processed, or broken out, centrally while all other SaaS traffic is broken out locally. This architecture provides all the advantages of local breakout (LBO) without any of the issues of Active Directory MFA. This architecture permits the following:

- Authentication traffic for Azure Active Directory is forwarded to the data center, corporate headquarters, or its equivalent, which minimizes the number of MFA trusted IP addresses that an organization must manage.
- End users have a consistent experience regardless of which branch office they are accessing SaaS applications from, provided that the branch office is integrated with Active Directory using MFA bypass. This consistent experience also applies to branches that use dynamically assigned WAN IP addresses
- All approved SaaS applications break out to the Internet from the local branch, which minimizes application latency and bandwidth utilization.

Two architectures allow secure SD-WAN networks to access the network: central internet breakout (CBO) and local internet breakout (LBO). The following two figures illustrate these architectures

Figure 1 illustrates how devices in Secure SD-WAN networks can access the internet using CBO. The figure shows that traffic from users at Site n accesses the internet by going from the local branch site through a central site, here, a data center.

Figure 1: Central Internet Breakout



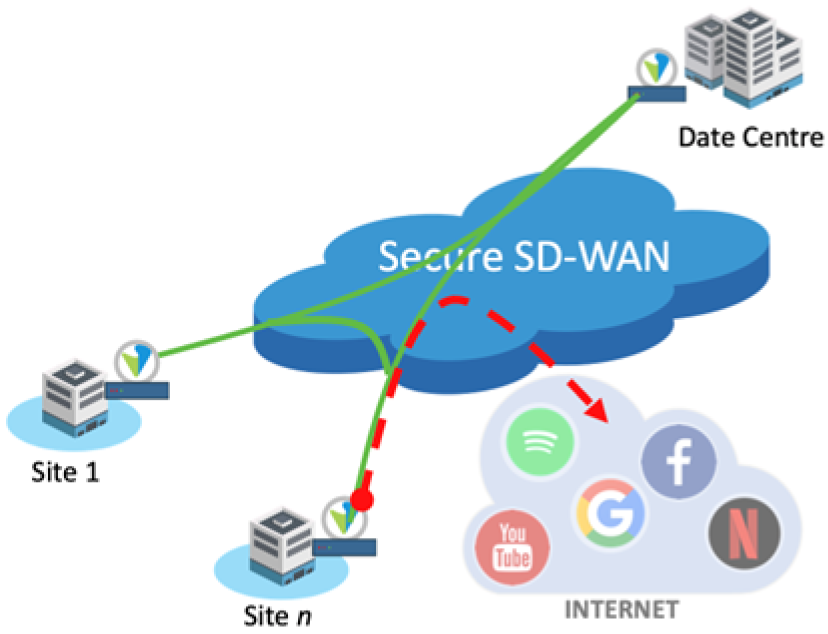
The CBO approach has several disadvantages:

- Increased latency between the end user and the application, affecting throughput and application responsiveness.

- Increased WAN bandwidth required at the data center to handle traffic tromboning between branches and the internet. This has cost implications.
- Network devices must be scaled at the data center to handle traffic tromboning between branches and the internet, which again has cost implications.

Figure 2 illustrates how devices in Secure SD-WAN networks can access the internet using LBO. With LBO, Secure SD-WAN breaks out traffic destined for the internet at the local branch rather than backhaul it to the data center so that it breaks out centrally. This architecture saves bandwidth at the data center and reduces application latency, which improves the end user experience.

Figure 2: Local Internet Breakout



You can build a network that mixes both central and local internet access. For example, an organization may choose to locally break out traffic at the branches for some trusted applications, perhaps by leveraging the NGFW features of the Secure SD-WAN CPE, while choosing to break out other internet-destined traffic centrally. For example, if an organization considers Microsoft 365 to be a trusted application, the organization can locally break out Microsoft 365 traffic at the branches, while breaking out internet-destined traffic for all other applications centrally.

For more information about central and local internet breakout, see Application-Based Breakout.

Combine Secure SD-WAN LBO and Azure Active Directory MFA

Using a CBO architecture, an organization can trust the source IP address of the data center on their Azure Active Directory IAM platform. Consequently, MFA could be bypassed for all users sourced from that trusted IP address. There would be a small number of static IP addresses and therefore easy to manage.

Using an LBO architecture, users can access SaaS applications, including Microsoft 365, directly from their local branch. Traffic is no longer sourced from the data center. Therefore, the list of trusted IP addresses increases, because each branch directly presents users to the Azure Active Directory platform. For example, 500 sites with two WAN links per site requires the configuration of 1,000 trusted source IP address on the Azure Active Directory platform. Moreover, for branches that do not used fixed IP addresses but are dynamically assigned WAN IP addresses, it is not possible for the Azure Active Directory administrators to populate the trusted IP address list, because the addresses change continuously. An example is mobile technologies, which typically use a dynamically assigned private IP address for end users. There is also an argument that a dynamically assigned address could be used by any user or organization, so MFA should not be disabled for dynamically assigned address ranges.

While using LBO improves the end-user experience in several ways, there are some Azure Active Directory MFA exceptions:

- Network administrators may need to manage large lists of trusted source IP addresses. As a result, end users may have an inconsistent user experience, because some sites bypass MFA whereas others do not.
- An organization cannot consider a dynamically assigned WAN IP address to be trusted, because it is not guaranteed that other users or organizations cannot also be assigned the same address. This situation also results in an inconsistent end user experience, because some sites bypass MFA whereas others do not, depending on their trusted status.

To address these exceptions, you can configure Versa Secure SD-WAN so that authentication requests to Azure Active Directory are broken out centrally and all other SaaS traffic is broken out locally. This architecture provides all the advantages of LBO without any of the Azure Active Directory MFA exceptions. This architecture improves the end user experience when using Azure AD and MFA and permits the following:

- Authentication traffic to Azure Active Directory is forwarded to the data center (or equivalent). This design minimizes the number of trusted IP addresses that must be managed.
- End users have a consistent experience, regardless of which branch office they are accessing SaaS applications from (assuming the branch is integrated with Azure AD using MFA bypass) and including branches that are using dynamically assigned WAN IP addresses.
- All approved SaaS applications break out to the internet through the local branch, which minimizes application latency and bandwidth utilization.

Configuration

This section offers guidelines for configuring the Azure Active Directory MFA and Versa Secure SD-WAN LBO, and it illustrates the configuration procedure using an example in which a branch in an organization directs authentication traffic to the corporate headquarters but breaks out all other SaaS traffic locally.

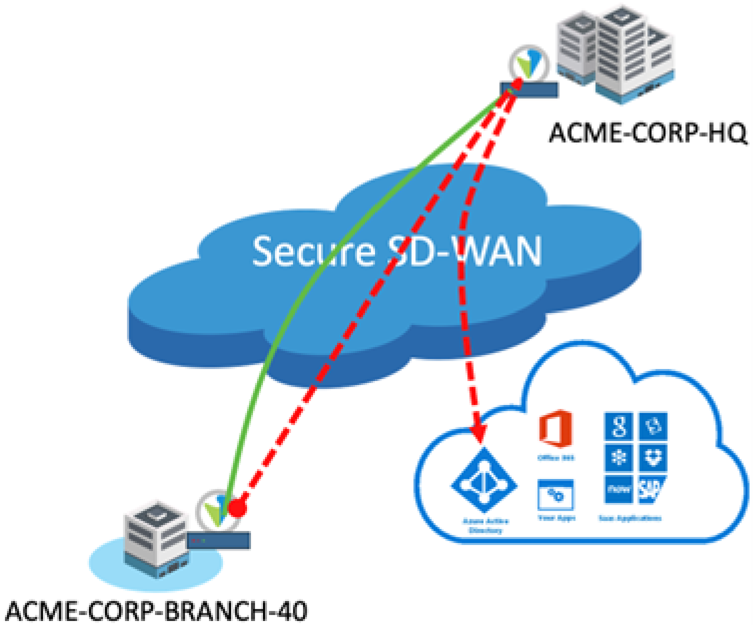
The following are best practice guidelines you may want to consider for the configuration:

- Depending on the security posture of the organization, the information in this article may also apply to Versa Secure Access (VSA) users. Specifically, network administrators may want to create allow lists (also known as whitelists) for the public IP addresses of their offices because they are generally treated as trusted locations. As such, the organization may not deem MFA essential for users connecting through such sites. However, to protect the corporate network, network administrators may want to retain MFA for remote or traveling users (such as VSA users) who are authenticated using Azure Active Director from unknown locations.

- For deep packet inspection (DPI) application recognition, VOS Releases 21.1 and later support SaaS application detection using endpoints, while earlier VOS software released use an application cache. The application cache is used to cache the detected application based on its specific IP address and port. However, the application cache could not assist the first session to a given destination. Therefore, the first session would often break out to the internet centrally even though subsequent sessions were broken out locally. Because SaaS vendors are now using many IP addresses to serve applications, this limitation has become an increasing issue. Adding SaaS application detection using the endpoints in VOS Releases 21.1 and later allows applications to be identified from the first packet and addresses the limitation of the application cache. For more information about SaaS application detection using endpoints, see the VOS Release Notes for Release 21.1. For more information about the application cache, see the System Application Cache article in the Versa Networks Knowledge Base.

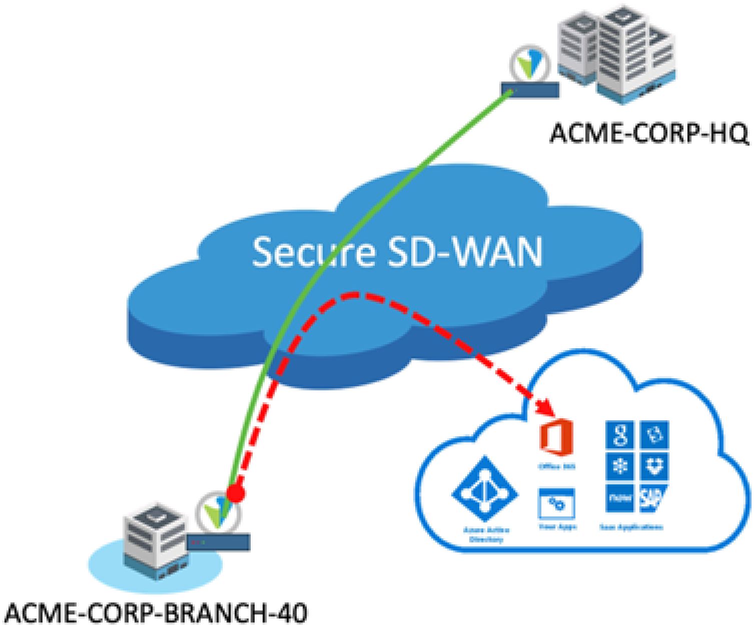
In the configuration example in this section, user authentication requests from ACME-CORP-BRANCH-40 to Azure Active Directory traverse ACME-CORP-HQ. This is achieved by originating a default route from ACME-CORP-HQ and injecting it into the Secure SD-WAN fabric. Because user authentication requests traverse ACME-CORP-HQ, the network administrators of ACME-CORP can configure Azure Active Directory trusted IP for the IP address of the ACME-CORP-HQ WAN interface. The network administrators have disabled MFA for users whose source IP address is the WAN interface of ACME-CORP-HQ. As traffic from ACME-CORP-BRANCH-40 passes through ACME-CORP-HQ, carrier-grade NAT (CGNAT) translates the private source IP address of the end users' requests to the public IP address of the WAN link. Figure 3 illustrates the user authentication portion of the example configuration.

Figure 3: CBO for Traffic Destined to Azure Active Directory



In addition, user traffic to SaaS applications, such as Microsoft 365, is broken out locally at ACME-CORP-BRANCH-40. This is achieved using a forwarding profile, which is configured on ACME-CORP-BRANCH-40. As a result of the forwarding profile, the default route through ACME-CORP-HQ is ignored, and applications such as Microsoft 365 are broken out locally at the branch. As traffic from ACME-CORP-BRANCH-40 passes to the internet, CGNAT translates the private IP address of the end users' requests to the public IP address of the WAN link of ACME-CORP-BRANCH-40. Figure 4 illustrate the LBO portion of the example configuration.

Figure 4: LBO for SaaS Applications



There are a couple of approaches to LBO and CBO, which are summarized in Table 1. Design 1 implements the approach described above, and this is the design that is shown in the configuration example. Design 2 is an alternate approach. Both designs use the same approach to achieve the desired outcome of breaking out Azure Active Directory traffic centrally. In both designs, it is Rule 1 that breaks out the traffic centrally. For clarity, this step is highlighted in green.

Table 1: CBO and LBO Design Options

Design	Default Route Advertised By	SD-WAN Traffic-Steering Policy on ACME-CORP-BRANCH
1	Remote branch • In our example, this is ACME-CORP-HQ	• Rule 1—Match Azure Active Directory traffic and referenc follows the default route to the remote branch, based on t CBO. • Rule 2—Match on SaaS traffic (such as Microsoft 365), a • Rule 3 (default rule)—Match all other traffic, and referenc the default route to the remote branch for CBO.
2	Local branch	• Rule 1—Match Azure Active Directory traffic, and referen

Design	Default Route Advertised By	SD-WAN Traffic-Steering Policy on ACME-CORP-BRANCH
	- In our example, this is ACME-CORP-BRANCH-40	follow the default route through the local branch. Instead, branch for CBO. - Rule 2—Depending on the security posture of the organiz to the internet locally, *or*, like Rule 1, reference a forwardi traffic does *not* follow the default route through the local b branch for CBO.

Note that the screenshots in this configuration are based on VOS Release 21.2.3.

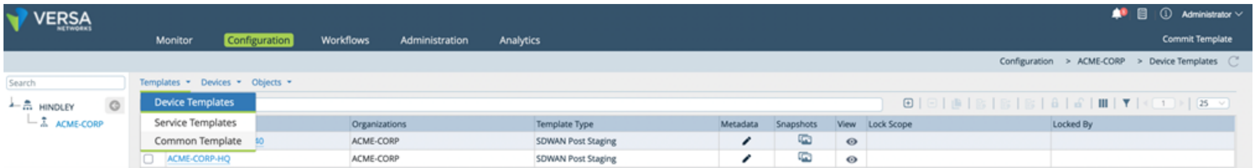
Configure Secure SD-WAN

The following procedure configures an SD-WAN traffic-steering rule based on the example described above and referenced as Design 1 in Table 1, above. This procedure, which is used to configure the ACME-CORP-BRANCH-40 site, breaks out Azure Active Directory traffic centrally based on four specific authentication URLs.

Note that in this procedure, we create a custom application in the common template. This method is recommended to avoid having to recreate the same application in each device template.

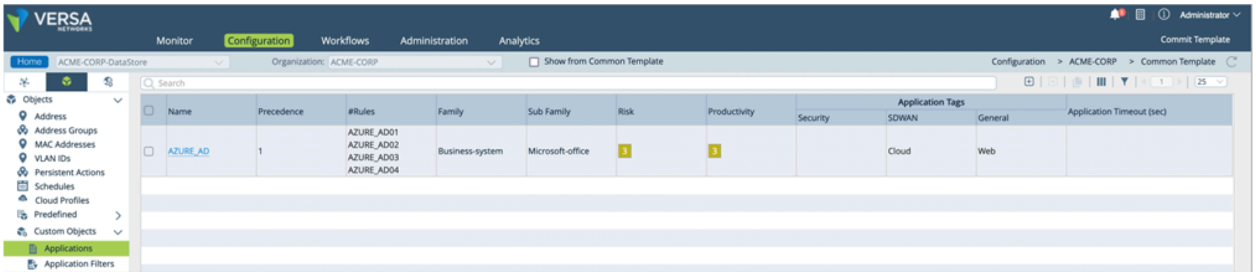
To configure the Secure SD-WAN:

1. Select Configuration > *organization-name* > Templates > Common Template. In this example, the organization name is ACME-CORP.



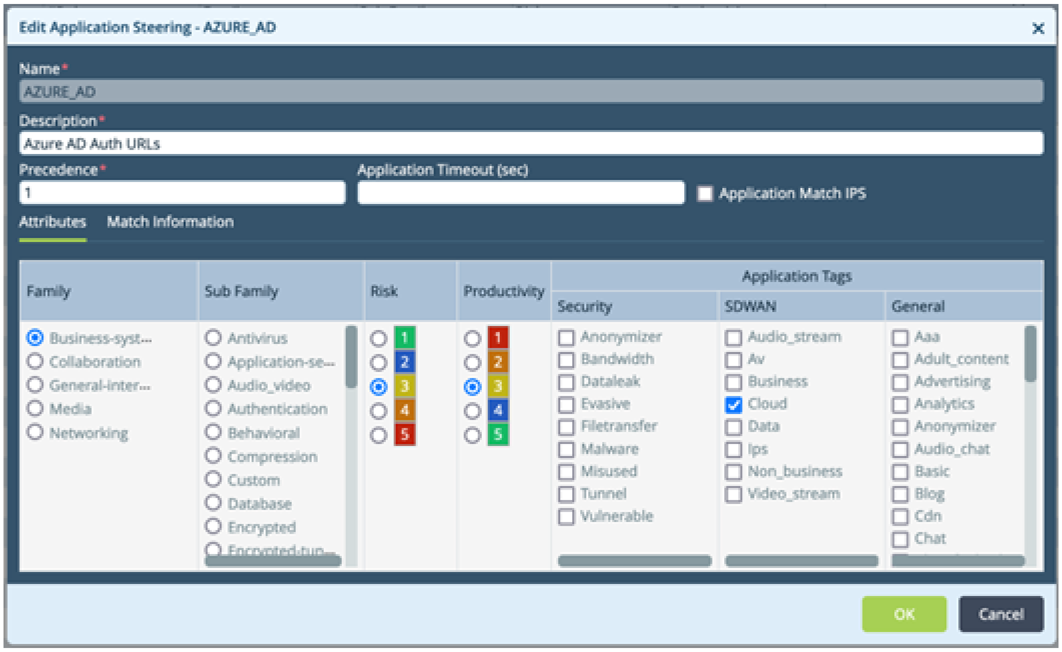
	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
...40	ACME-CORP	SDWAN Post Staging					
☐ ACME-CORP-HQ	ACME-CORP	SDWAN Post Staging					

2. Select Objects & Connectors > Objects > Custom Objects > Applications, and then click the ⊞ Add icon.



☐	Name	Precedence	#Rules	Family	Sub Family	Risk	Productivity	Application Tags			Application Timeout (sec)
								Security	SDWAN	General	
☐	AZURE_AD	1	AZURE_AD01 AZURE_AD02 AZURE_AD03 AZURE_AD04	Business-system	Microsoft-office	3	3		Cloud	Web	

3. Enter a name for the custom application. Here, we use the name AZURE_AD. Enter a text description for the application enter appropriate values in the Precedence field, and select the Attributes tab and click the appropriate attributes for your organization. For example:



Edit Application Steering - AZURE_AD

Name*
AZURE_AD

Description*
Azure AD Auth URLs

Precedence*
1

Application Timeout (sec)

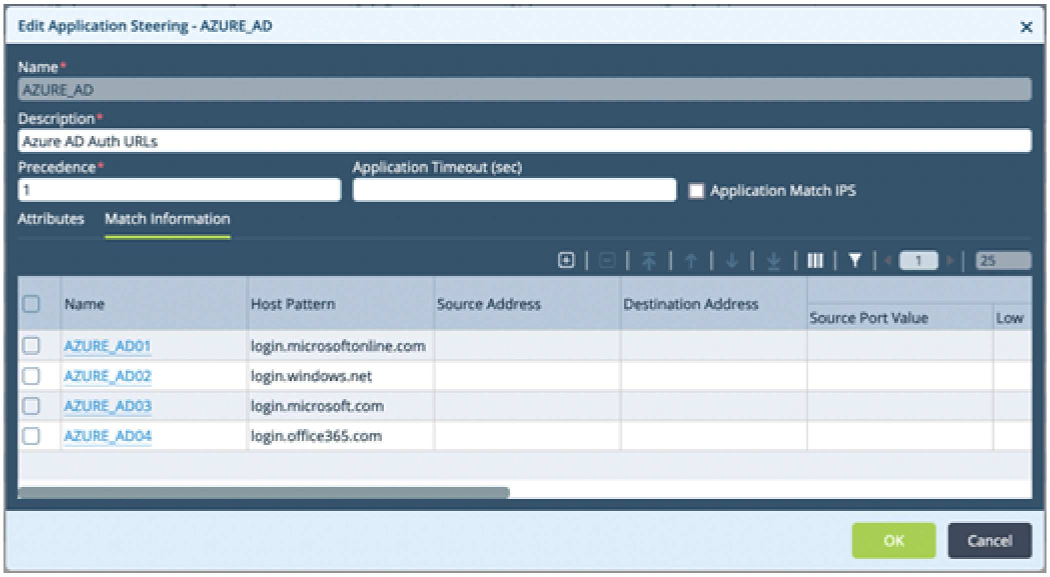
☐ Application Match IPS

Attributes | Match Information

Family	Sub Family	Risk	Productivity	Application Tags Security	 SDWAN	 General
● Business-syst...	○ Antivirus	○ 1	○ 1	☐ Anonymizer	☐ Audio_stream	☐ Aaa
○ Collaboration	○ Application-se...	○ 2	○ 2	☐ Bandwidth	☐ Av	☐ Adult_content
○ General-inter...	○ Audio_video	● 3	● 3	☐ Dataleak	☐ Business	☐ Advertising
○ Media	○ Authentication	○ 4	○ 4	☐ Evasive	☑ Cloud	☐ Analytics
○ Networking	○ Behavioral	○ 5	○ 5	☐ Filetransfer	☐ Data	☐ Anonymizer
	○ Compression			☐ Malware	☐ Ips	☐ Audio_chat
	○ Custom			☐ Misused	☐ Non_business	☐ Basic
	○ Database			☐ Tunnel	☐ Video_stream	☐ Blog
	○ Encrypted			☐ Vulnerable		☐ Cdn
	○ Encrypted-tun...					☐ Chat

OK | Cancel

4. Select the Match Information tab, and then click the ⊞ Add icon.



Edit Application Steering - AZURE_AD

Name*
AZURE_AD

Description*
Azure AD Auth URLs

Precedence*
1

Application Timeout (sec)

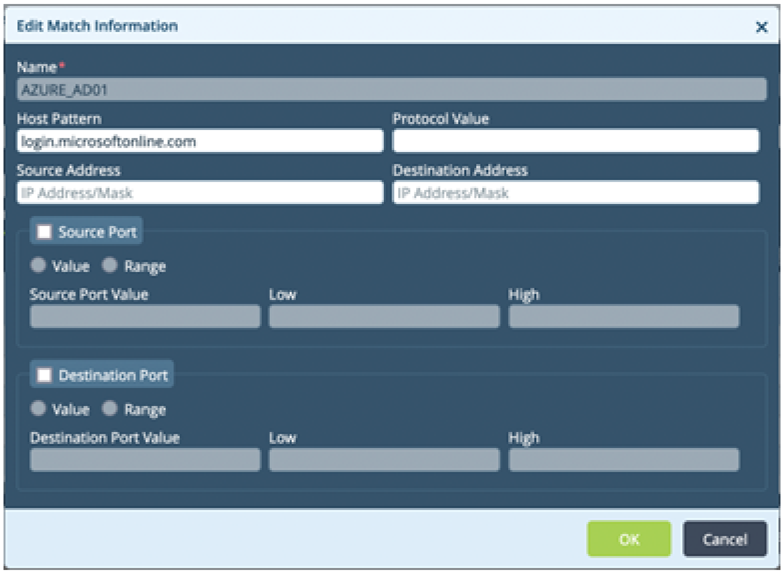
☐ Application Match IPS

Attributes | Match Information

☐	Name	Host Pattern	Source Address	Destination Address	Source Port Value	Low
☐	AZURE_AD01	login.microsoftonline.com				
☐	AZURE_AD02	login.windows.net				
☐	AZURE_AD03	login.microsoft.com				
☐	AZURE_AD04	login.office365.com				

OK | Cancel

5. In the Edit Match Information popup window, enter a name in the Name field (here, AZURE_AD01), add a string in the Host Pattern field (here, login.microsoftonline.com), and then click OK.


Edit Match Information

Name* AZURE_AD01

Host Pattern: login.microsoftonline.com

Protocol Value:

Source Address: IP Address/Mask

Destination Address: IP Address/Mask

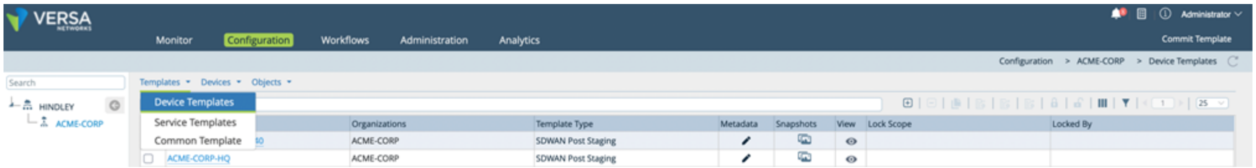
□ Source Port
○ Value ○ Range
Source Port Value | Low | High

□ Destination Port
○ Value ○ Range
Destination Port Value | Low | High

6. Repeat Steps 4 and 5 for the following URLs:
    - login.microsoftonline.com (as shown above)
    - login.windows.net
    - login.microsoft.com
    - login.office365.com
7. Click OK, and then click Home.

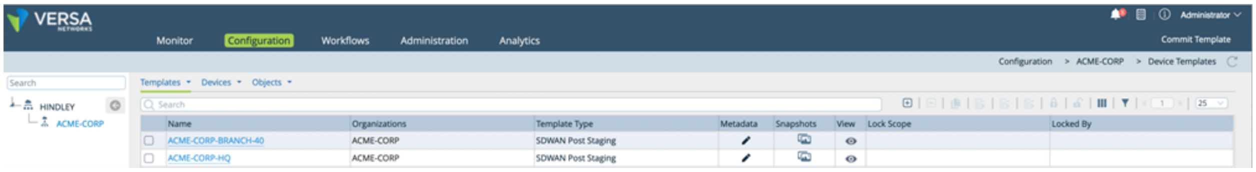
Note: DNS must be enabled on ACME-CORP-BRANCH-40 to resolve the URLs configured in Steps 4, 5, and 6. If DNS is already configured, you can skip Steps 8 through 11.

8. Select Templates > Device Templates.



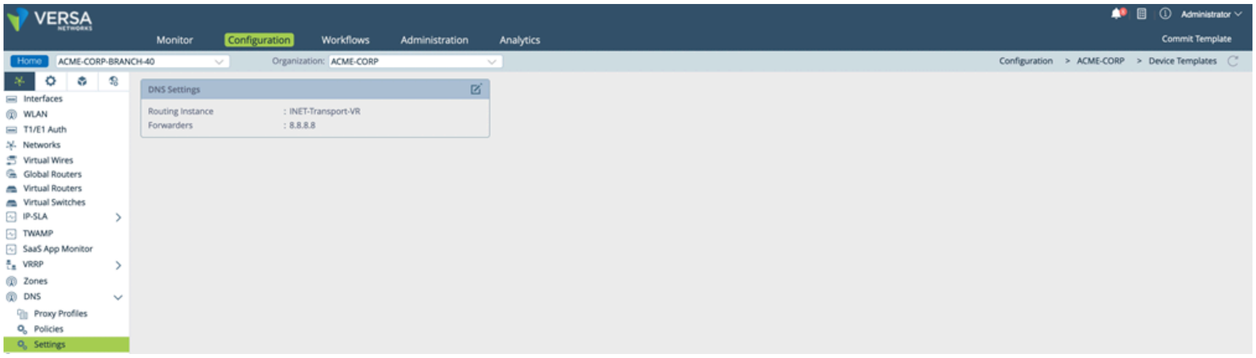
	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
40	ACME-CORP	SDWAN Post Staging	✎		👁		
□ ACME-CORP-HQ	ACME-CORP	SDWAN Post Staging	✎		👁		

9. Select the device template you want to configure. In this example, we configure ACME-CORP-BRANCH-40.



	Name	Organizations	Template Type	Metadata	Snapshots	View	Lock Scope	Locked By
□	ACME-CORP-BRANCH-40	ACME-CORP	SDWAN Post Staging	✎		👁		
□	ACME-CORP-HQ	ACME-CORP	SDWAN Post Staging	✎		👁		

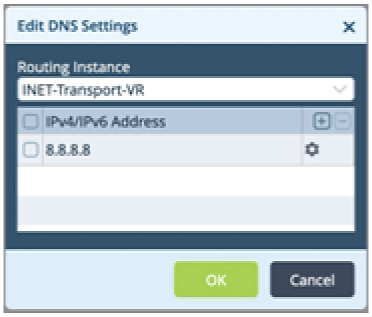
10. Select Networking > DNS > Settings, and then click the ✎ icon.



DNS Settings

Routing Instance : INET-Transport-VR
Forwarders : 8.8.8.8

11. In the Edit DNS Settings popup window, in the Routing Instance field, select a WAN interface on the CPE. This interface is used to source DNS lookups. In this example, we select NET-Transport-VR. Then, click the ⊞ Add icon to add a DNS server, and enter the IP address of the DNS server. In this example, we use 8.8.8.8. Finally, click OK. You can add additional DNS servers if required.

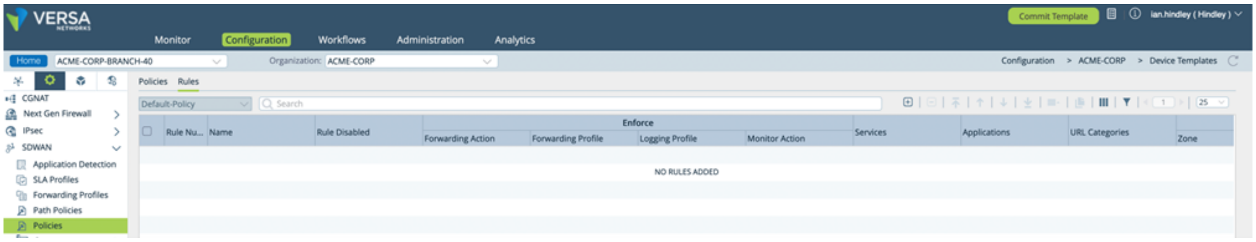


Edit DNS Settings

Routing Instance: INET-Transport-VR

□ IPv4/IPv6 Address
□ 8.8.8.8

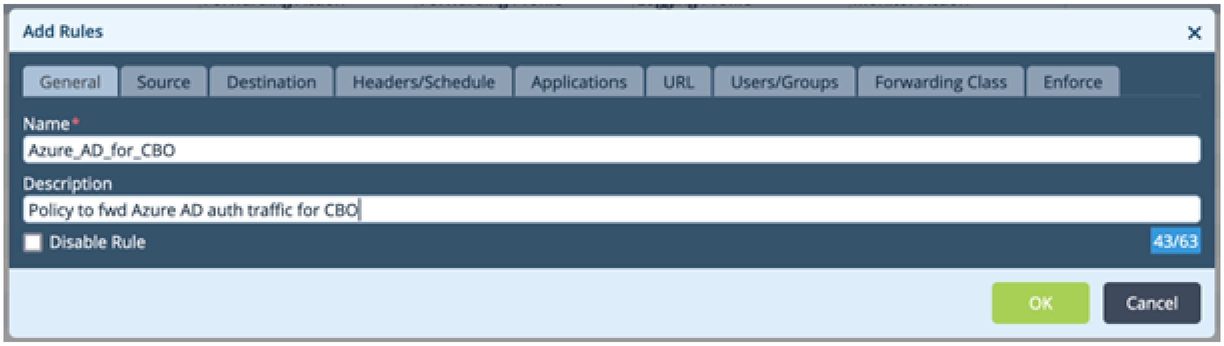
12. Select Services > SD-WAN > Policies > Rules, and then click the ⊞ Add icon.



□	Rule Nu...	Name	Rule Disabled	Enforce				Services	Applications	URL Categories	Zone
				Forwarding Action	Forwarding Profile	Logging Profile	Monitor Action				

NO RULES ADDED

13. In the Add Rules popup window, select the General tab. Enter a name for the rule, and optionally enter a description.



Add Rules

Name*
Azure_AD_for_CBO

Description
Policy to fwd Azure AD auth traffic for CBO

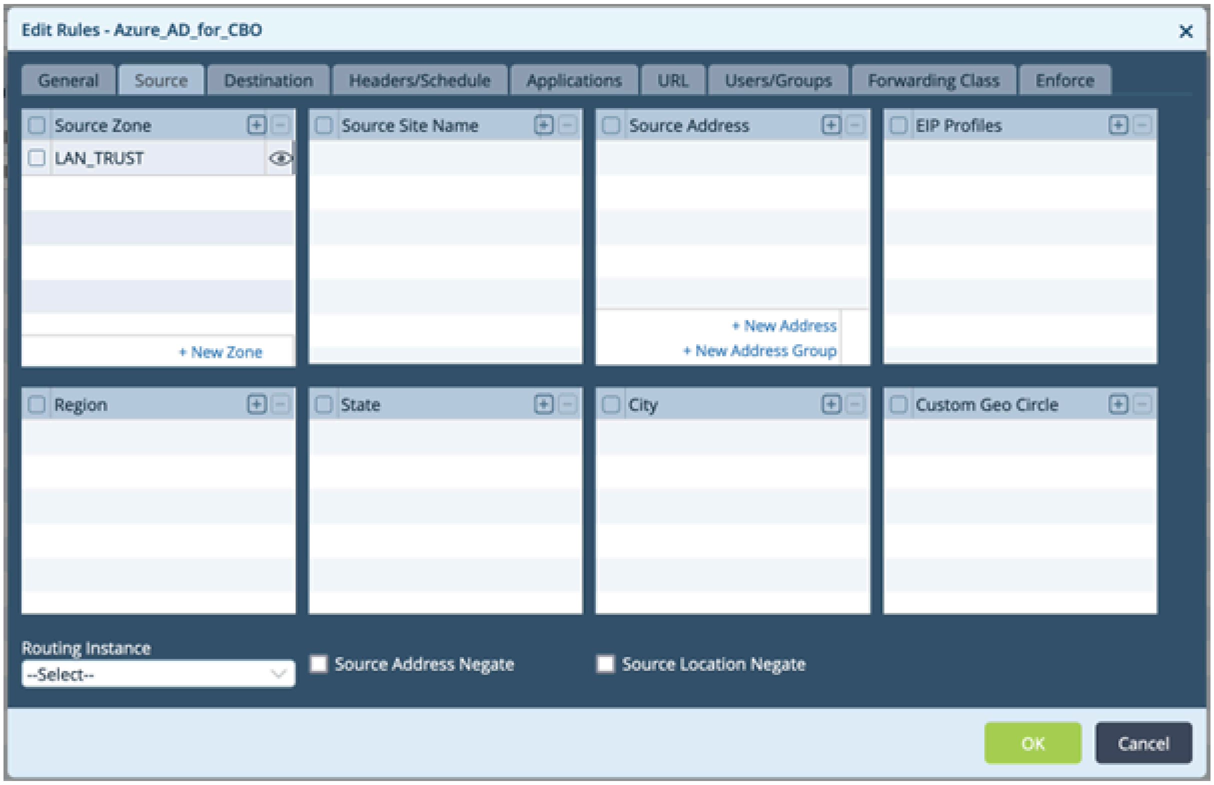
□ Disable Rule

43/63

In this example, the source zone is specified in order to filter matching traffic. Depending on your requirements, this step may need amending to meet your specific use case or skipped altogether. In this example, the LAN_TRUST zone is associated with the LAN interface port of the CPE.

14. In this example, we configure the source zone so that we can filter matching traffic. Depending on your requirements, you may need to modify this step or skip it altogether. In this example, we associate the

    LAN_TRUST zone with the LAN interface port of the CPE. To do this, select the Source tab. Then, click the ⊞ Add icon in the Source Zone table and select LAN_TRUST.



Edit Rules - Azure_AD_for_CBO

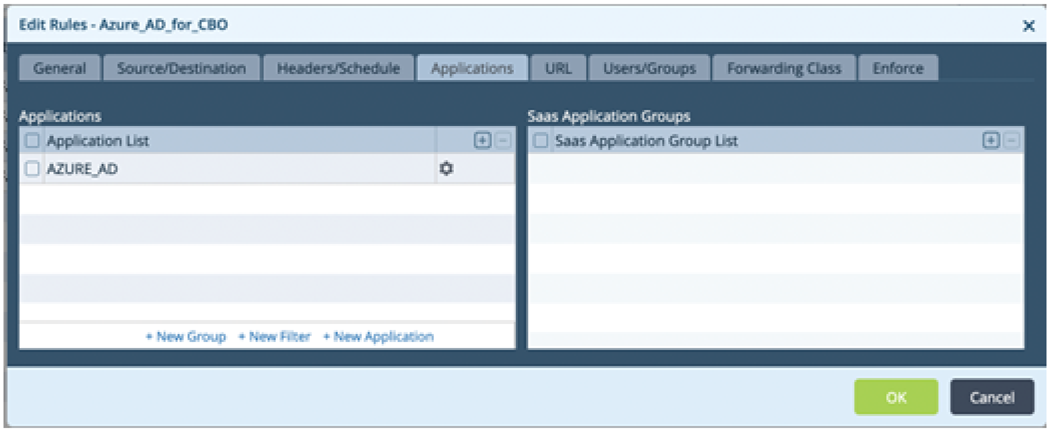
□ Source Zone
□ LAN_TRUST

Routing Instance
--Select--

□ Source Address Negate

□ Source Location Negate

15. Select the Applications tab. In the Applications table, click the ⊞ Add icon and select the custom application you created earlier, here, AZURE_AD.



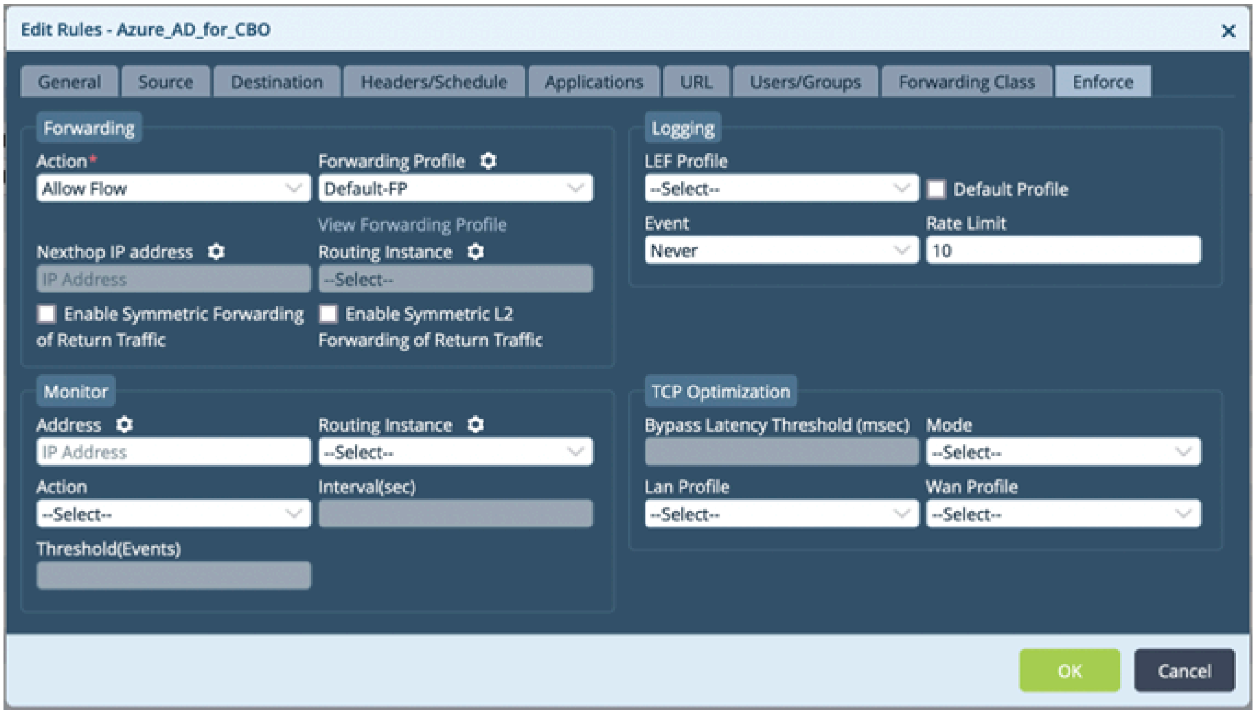
Applications

□ Application List
□ AZURE_AD

Saas Application Groups

□ Saas Application Group List

16. Select the Enforce tab, and then select the appropriate forwarding profile.
In this example, we select the default forwarding profile. However, you can choose a forwarding profile appropriate for your use case. For example, you could use a low-latency or low packet loss profile toward the data center, headquarters, or equivalent for CBO. For more information, see Configure SD-WAN Traffic Steering.
In this example, the forwarding profile, together with the originator of the default route, ensures that traffic sourced from the LAN_TRUST zone and destined for any of the four URLs is forwarded across the network to ACME-CORP-HQ for CBO.



Forwarding
Action* Allow Flow
Forwarding Profile Default-FP
Nexthop IP address: IP Address
Routing Instance: --Select--
□ Enable Symmetric Forwarding of Return Traffic
□ Enable Symmetric L2 Forwarding of Return Traffic

Logging
LEF Profile --Select--
□ Default Profile
Event Never
Rate Limit 10

Monitor
Address: IP Address
Routing Instance: --Select--
Action: --Select--
Interval(sec)
Threshold(Events)

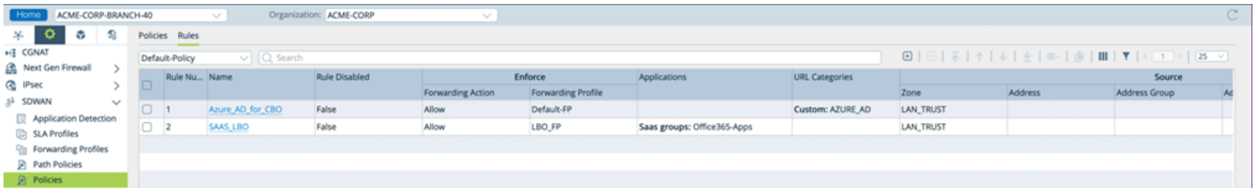
TCP Optimization
Bypass Latency Threshold (msec)
Mode --Select--
Lan Profile --Select--
Wan Profile --Select--

17. Click OK. The main pane displays the configured SD-WAN traffic-steering policies. The following screenshot shows two SD-WAN traffic-steering policies:

    - Azure_AD_for_CBO is the policy we created in the steps above. The purpose of this policy is to forward URLs related to Azure AD, using the forwarding profile and in conjunction with the default route, to break out to the internet centrally. Because the WAN IP addresses of the central site are trusted within the Azure Active Directory environment, end users connected to branches associated with this device template bypass MFA.
    - SAAS_LBO is an example policy for SaaS-destined traffic that breaks out to the internet at the local branch. In

this example, the policy matches on the predefined application group named Office365-Apps. The policy references a forwarding profile that ensures that a route lookup is not performed. In the example here, the profile is called LBO_FP. By avoiding a route lookup, traffic does not follow the default route to ACME-CORP-HQ. Instead, it is broken out locally to the internet.

Note that the order of policy rules is important. In this example, if the rules were the other way around in the screenshot below, all Microsoft 365 including Azure AD traffic would break out locally. Therefore, it is important to consider the order of the rules for successful deployment.



	Rule Nu...	Name	Rule Disabled	Enforce		Applications	URL Categories	Source			Ac
				Forwarding Action	Forwarding Profile			Zone	Address	Address Group	
□	1	Azure_AD_for_CBO	False	Allow	Default-FP		Custom: AZURE_AD	LAN_TRUST			
□	2	SAAS_LBO	False	Allow	LBO_FP	Saas groups: Office365-Apps		LAN_TRUST			

18. To apply the site-to-site configuration to the VOS branch, follow the normal process to commit the template.

Configure Azure Active Directory

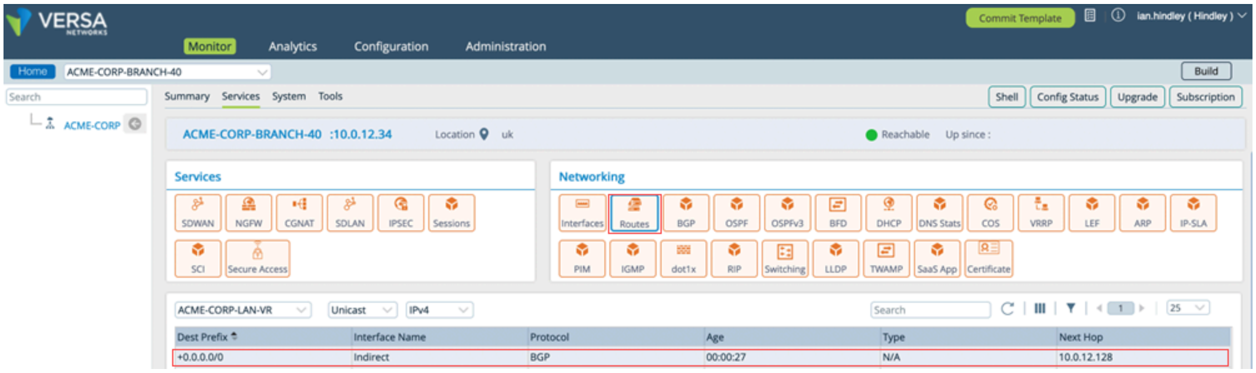
To configure Azure Active Directory, refer to your vendor's support site for configuration instructions. For example, see https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates.

Verification

After you configure the Secure SD-WAN CBO and LBO, and after you configure Azure Active Directory, verify that the SD-WAN traffic-steering rules are properly directing traffic.

Verify ACME-CORP-BRANCH-40

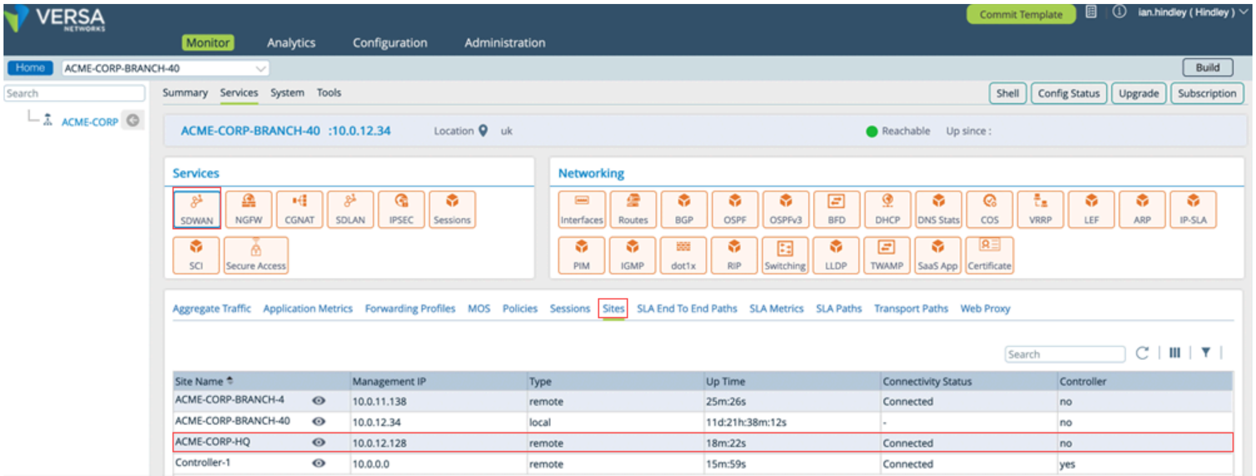
Before testing, we can see a default route is learned through ACME-CORP-HQ (10.0.12.128). This route is used for all internet access, including Azure Active Directory authentication.



ACME-CORP-BRANCH-40 :10.0.12.34 Location uk Reachable Up since :

Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+0.0.0.0/0	Indirect	BGP	00:00:27	N/A	10.0.12.128

To confirm that the next hop 10.0.12.128 is ACME-CORP-HQ, select Services > SD-WAN and then select the Sites tab, as shown in the screenshot below. Note that the Management IP address in the screenshot below is equivalent to the Next-Hop IP address in the screenshot above.

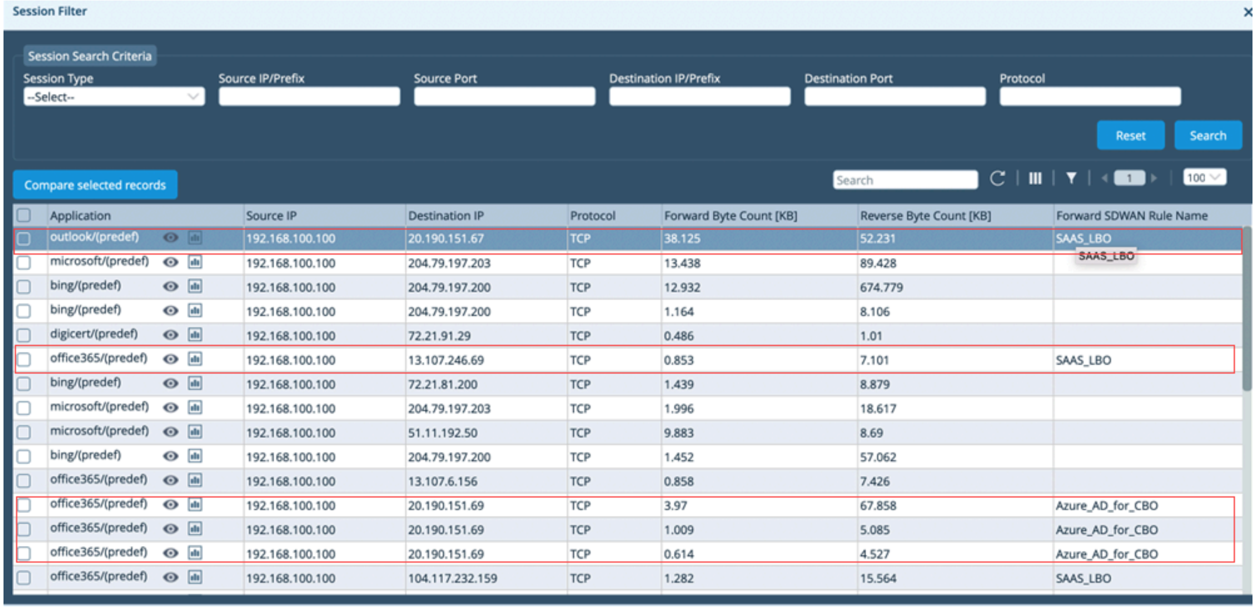


ACME-CORP-BRANCH-40 :10.0.12.34 Location uk Reachable Up since :

Site Name	Management IP	Type	Up Time	Connectivity Status	Controller
ACME-CORP-BRANCH-4	10.0.11.138	remote	25m:26s	Connected	no
ACME-CORP-BRANCH-40	10.0.12.34	local	11d:21h:38m:12s	-	no
ACME-CORP-HQ	10.0.12.128	remote	18m:22s	Connected	no
Controller-1	10.0.0.0	remote	15m:59s	Connected	yes

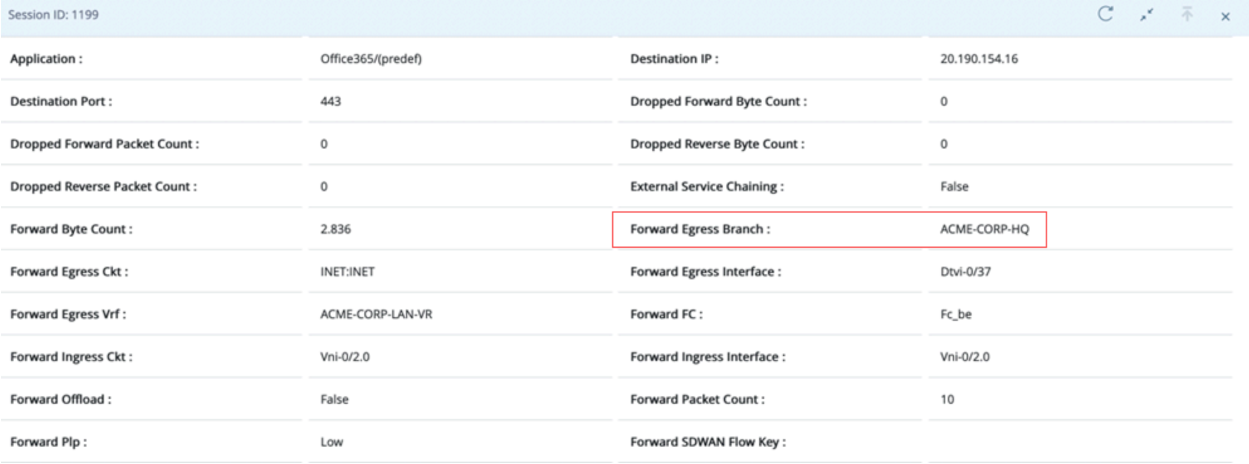
Now, we create an end user session on a Windows PC to one of the URLs in the SD-WAN traffic-steering policy that we created earlier. We can monitor information related to this session from the Versa Director Monitor tab.

From the Services > Sessions tab, we can see several sessions including ones that match the Azure_AD_for_CBO policy rule. This is the rule that matches on authentication URLs and forwards the traffic for CBO to ACME-CORP-HQ. In this screenshot, we also see several sessions that were LBO, because they matched the SAAS_LBO rule. This policy matched on Microsoft 365 and broke out any matches locally. The output in this screenshot also demonstrates the order of the rules is correct, because we see both CBO and LBO. If the order were the wrong way around, we would not see any CBO.



Application	Source IP	Destination IP	Protocol	Forward Byte Count [KB]	Reverse Byte Count [KB]	Forward SDWAN Rule Name
outlook/(predef)	192.168.100.100	20.190.151.67	TCP	38.125	52.231	SAAS_LBO
microsoft/(predef)	192.168.100.100	204.79.197.203	TCP	13.438	89.428	
bing/(predef)	192.168.100.100	204.79.197.200	TCP	12.932	674.779	
bing/(predef)	192.168.100.100	204.79.197.200	TCP	1.164	8.106	
digicert/(predef)	192.168.100.100	72.21.91.29	TCP	0.486	1.01	
office365/(predef)	192.168.100.100	13.107.246.69	TCP	0.853	7.101	SAAS_LBO
bing/(predef)	192.168.100.100	72.21.81.200	TCP	1.439	8.879	
microsoft/(predef)	192.168.100.100	204.79.197.203	TCP	1.996	18.617	
microsoft/(predef)	192.168.100.100	51.11.192.50	TCP	9.883	8.69	
bing/(predef)	192.168.100.100	204.79.197.200	TCP	1.452	57.062	
office365/(predef)	192.168.100.100	13.107.6.156	TCP	0.858	7.426	
office365/(predef)	192.168.100.100	20.190.151.69	TCP	3.97	67.858	Azure_AD_for_CBO
office365/(predef)	192.168.100.100	20.190.151.69	TCP	1.009	5.085	Azure_AD_for_CBO
office365/(predef)	192.168.100.100	20.190.151.69	TCP	0.614	4.527	Azure_AD_for_CBO
office365/(predef)	192.168.100.100	104.117.232.159	TCP	1.282	15.564	SAAS_LBO

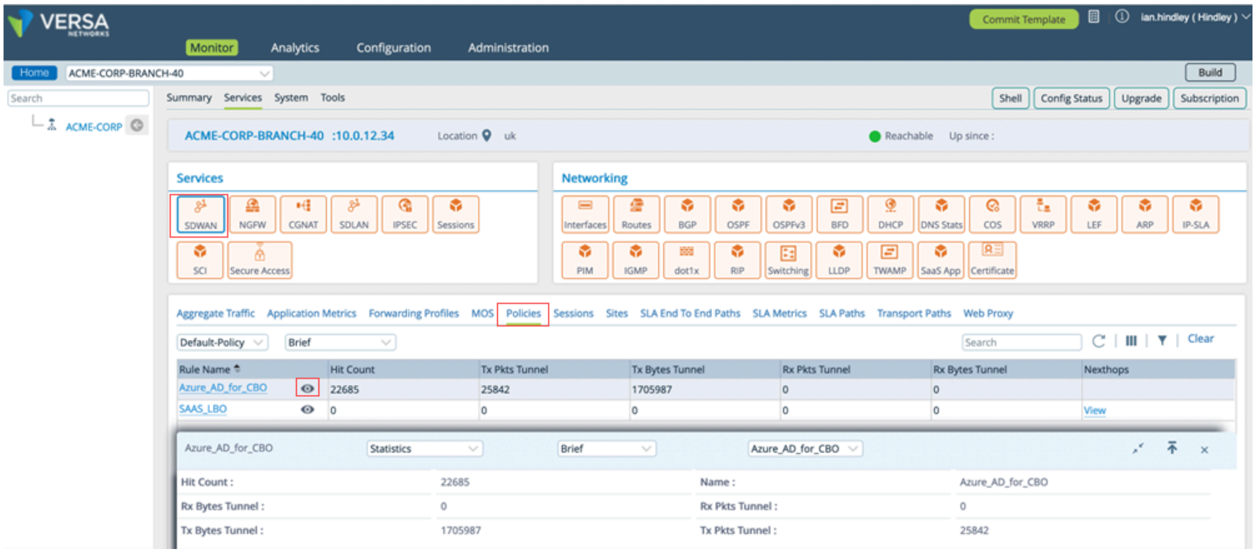
If you click the 👁 Eye icon in the session table above, you can see more session information regarding the session. As an example, for the CBO session, the Forward Egress Branch is listed as ACME-CORP-HQ for the Azure_AD_for_CBO rule. This is the correct and expected behavior, because internet breakout for Azure Active Directory traffic is through the HQ.



Session ID: 1199

Application :	Office365/(predef)	Destination IP :	20.190.154.16
Destination Port :	443	Dropped Forward Byte Count :	0
Dropped Forward Packet Count :	0	Dropped Reverse Byte Count :	0
Dropped Reverse Packet Count :	0	External Service Chaining :	False
Forward Byte Count :	2.836	Forward Egress Branch :	ACME-CORP-HQ
Forward Egress Ckt :	INET:INET	Forward Egress Interface :	Dtvi-0/37
Forward Egress Vrf :	ACME-CORP-LAN-VR	Forward FC :	Fc_be
Forward Ingress Ckt :	Vni-0/2.0	Forward Ingress Interface :	Vni-0/2.0
Forward Offload :	False	Forward Packet Count :	10
Forward Plp :	Low	Forward SDWAN Flow Key :	

We can also check statistics for the Azure_AD_for_CBO rule (or the SAAS_LBO rule) by selecting SD-WAN > Policies, as shown in the screenshot below.



ACME-CORP-BRANCH-40 :10.0.12.34   Location uk   Reachable   Up since :

Default-Policy   Brief

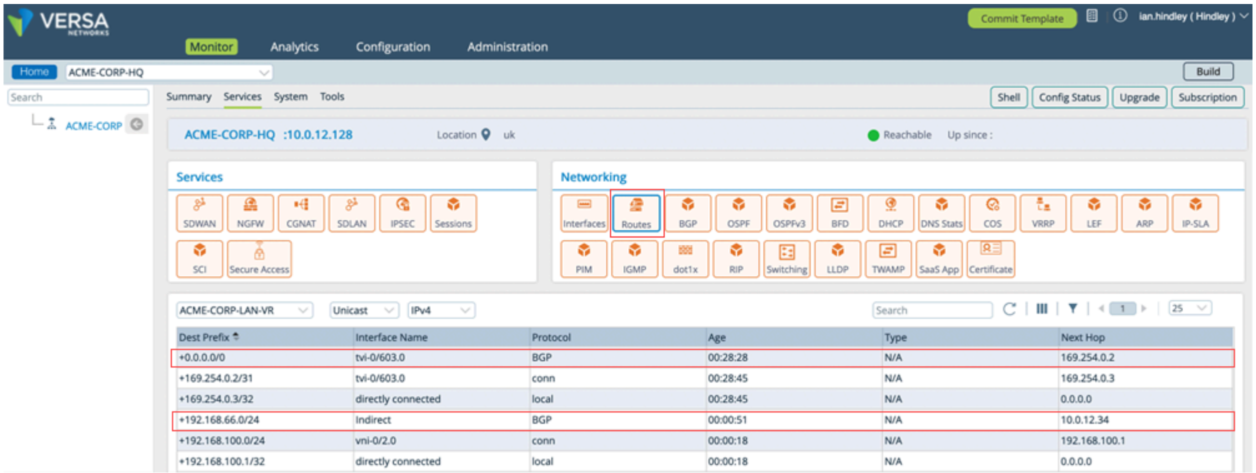
Rule Name	Hit Count	Tx Pkts Tunnel	Tx Bytes Tunnel	Rx Pkts Tunnel	Rx Bytes Tunnel	Nexthops
Azure_AD_for_CBO 👁	22685	25842	1705987	0	0	
SAAS_LBO 👁	0	0	0	0	0	View

Azure_AD_for_CBO   Statistics   Brief   Azure_AD_for_CBO

Hit Count :	22685	Name :	Azure_AD_for_CBO
Rx Bytes Tunnel :	0	Rx Pkts Tunnel :	0
Tx Bytes Tunnel :	1705987	Tx Pkts Tunnel :	25842

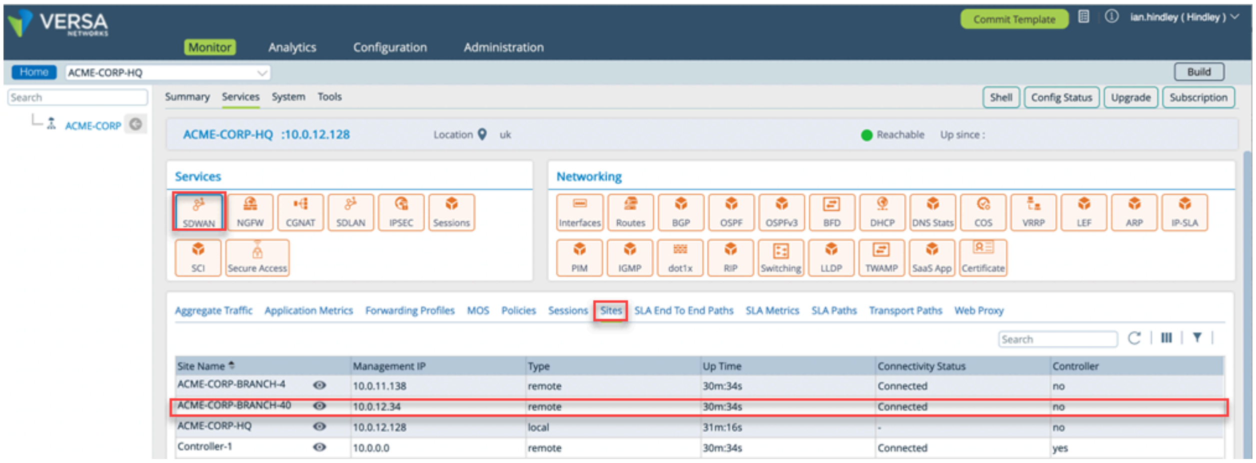
Verify ACME-CORP-HQ

Before testing, we can see a default route is learned through a split tunnel on the ACME-CORP-HQ device. This route is learned from BGP, and it is used for all internet access, including Azure Active Directory authentication. Additionally, we can see a subnet for the LAN range used on ACME-CORP-BRANCH-40 (192.168.66.0/24) with a next hop of 10.0.12.34. These two pieces of information ensure that we have connectivity between ACME-CORP-BRANCH-40 and the internet.



Dest Prefix	Interface Name	Protocol	Age	Type	Next Hop
+0.0.0.0/0	tvi-0/603.0	BGP	00:28:28	N/A	169.254.0.2
+169.254.0.2/31	tvi-0/603.0	conn	00:28:45	N/A	169.254.0.3
+169.254.0.3/32	directly connected	local	00:28:45	N/A	0.0.0.0
+192.168.66.0/24	Indirect	BGP	00:00:51	N/A	10.0.12.34
+192.168.100.0/24	vni-0/2.0	conn	00:00:18	N/A	192.168.100.1
+192.168.100.1/32	directly connected	local	00:00:18	N/A	0.0.0.0

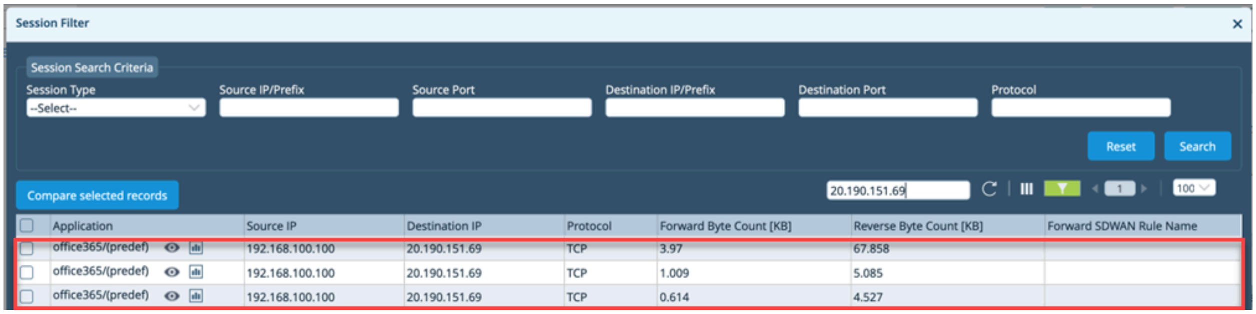
To confirm that 10.0.12.34 is ACME-CORP-BRANCH-40, select select Services > SD-WAN and then select the Sites tab, as shown in the screenshot below. Note that the Management IP address in the screenshot below is equivalent to the Next-Hop IP address in the screenshot above.



Site Name	Management IP	Type	Up Time	Connectivity Status	Controller
ACME-CORP-BRANCH-4	10.0.11.138	remote	30m:34s	Connected	no
ACME-CORP-BRANCH-40	10.0.12.34	remote	30m:34s	Connected	no
ACME-CORP-HQ	10.0.12.128	local	31m:16s	-	no
Controller-1	10.0.0.0	remote	30m:34s	Connected	yes

Now, we create an end user session on a Windows PC to one of the URLs in the SD-WAN traffic-steering policy that we created earlier. The source branch is ACME-CORP-BRANCH-40. We can monitor information related to this session from the Versa Director Monitor tab.

From the Services > Sessions tab, we can see several sessions including ones that match the Azure_AD_for_CBO policy rule on ACME-CORP-BRANCH-40. This is the rule that matches on authentication URLs and forwards the traffic for CBO to ACME-CORP-HQ. (Unlike ACME-CORP-BRANCH-40, we created no SD-WAN rules on ACME-CORP-HQ. As a result, the Forward SD-WAN Rule Name column is blank). The Forward and Reverse Byte Count columns confirm there is bidirectional traffic between the user and the server.



□	Application	Source IP	Destination IP	Protocol	Forward Byte Count [KB]	Reverse Byte Count [KB]	Forward SDWAN Rule Name
□	office365/(predef)	192.168.100.100	20.190.151.69	TCP	3.97	67.858	
□	office365/(predef)	192.168.100.100	20.190.151.69	TCP	1.009	5.085	
□	office365/(predef)	192.168.100.100	20.190.151.69	TCP	0.614	4.527	

Supported Software Information

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

Additional Information

Configure Direct Breakout to the Internet
Configure SD-WAN Traffic Steering
System Application Cache
VOS Release Notes for Release 21.1