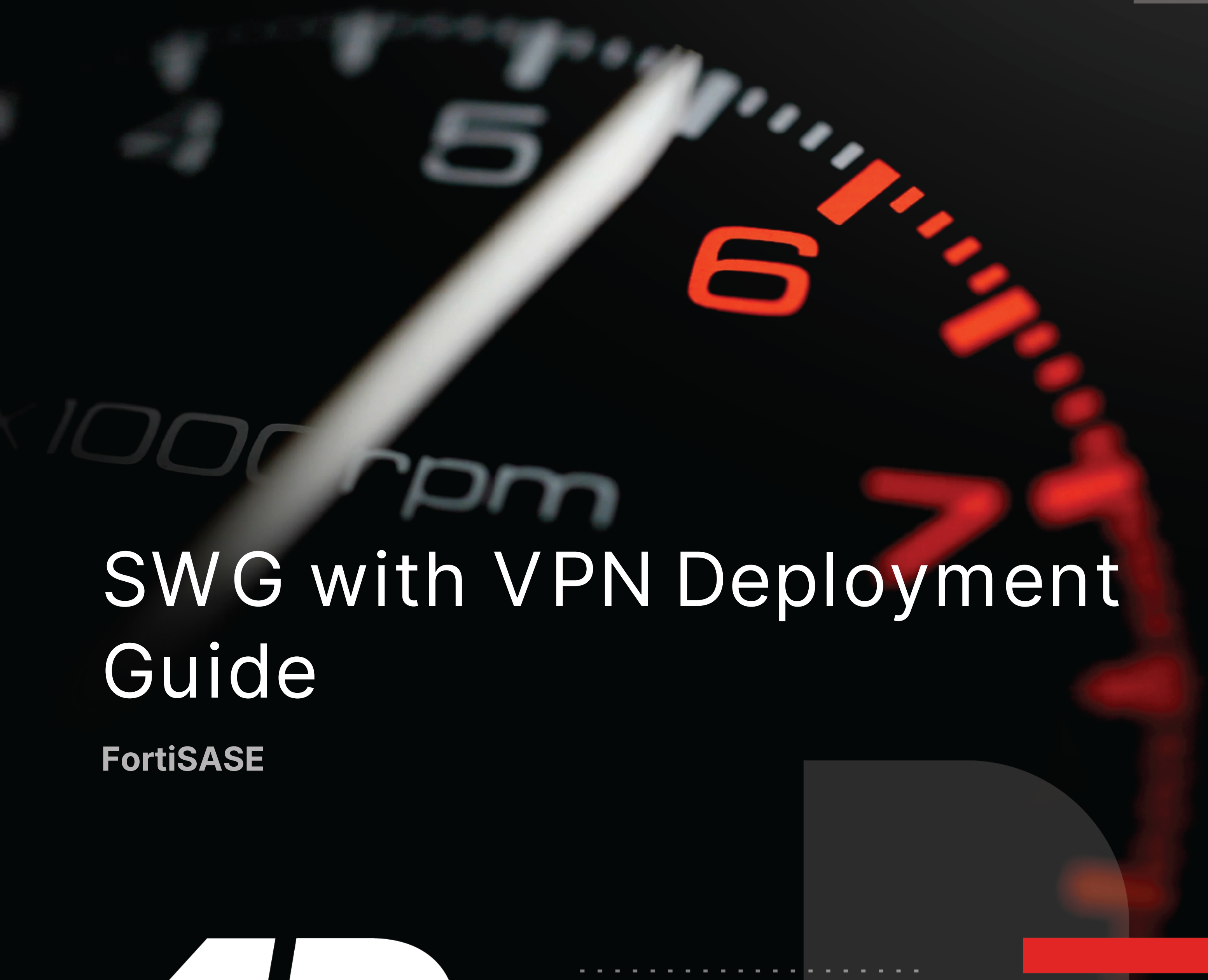
FORTINET



SWG with VPN Deployment Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change log

Date	Change description
2024-02-12	Initial release.

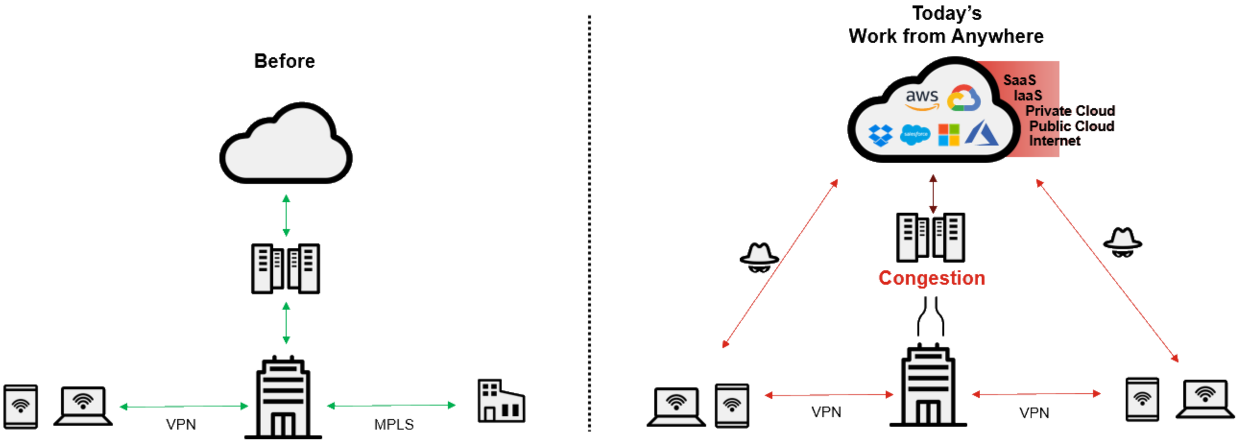
Introduction

This document describes Fortinet's recommended approach to configuring our secure web gateway (SWG) with VPN solution for FortiSASE. It covers configuration of the solution.

Executive summary

With the increased demand for a remote workforce and more applications moving to the cloud, companies must provide the network infrastructure for their employees to work securely from anywhere. While some organizations offer VPNs to securely access on-premise devices and servers, they may overlook the security of remote workers when they access cloud services on the Internet. Others may not be prepared for the amount of resources that is needed to secure all traffic coming from their remote workers using existing infrastructure.

This deployment guide looks at how FortiSASE SWG can provide secure direct Internet access for remote workers while supporting existing network infrastructure for accessing internal company resources through VPNs.



Intended audience

This guide is intended for a technical audience, including system and network architects, design engineers, network engineers, and security engineers who want to deploy FortiSASE SWG to secure their remote workers while integrating with existing network infrastructure.

The solution in this guide is targeted at small- and medium-sized organizations and enterprises.

This guide assumes that the reader is familiar with basic concepts of applications, networking, routing, security, and proxies, and has a basic understanding of network and data center architectures. For implementation with FortiOS, a working knowledge of FortiOS VPN is ideal.

About this guide

The deployment guide serves the purpose of going through the design and deployment steps involved in deploying a specific architecture. Readers should first evaluate their environments to determine whether the architecture and design that this guide outlines suits them.

Where appropriate, reviewing supplementary material in product admin guides, example guides, cookbooks, release notes, and other documents is recommended.

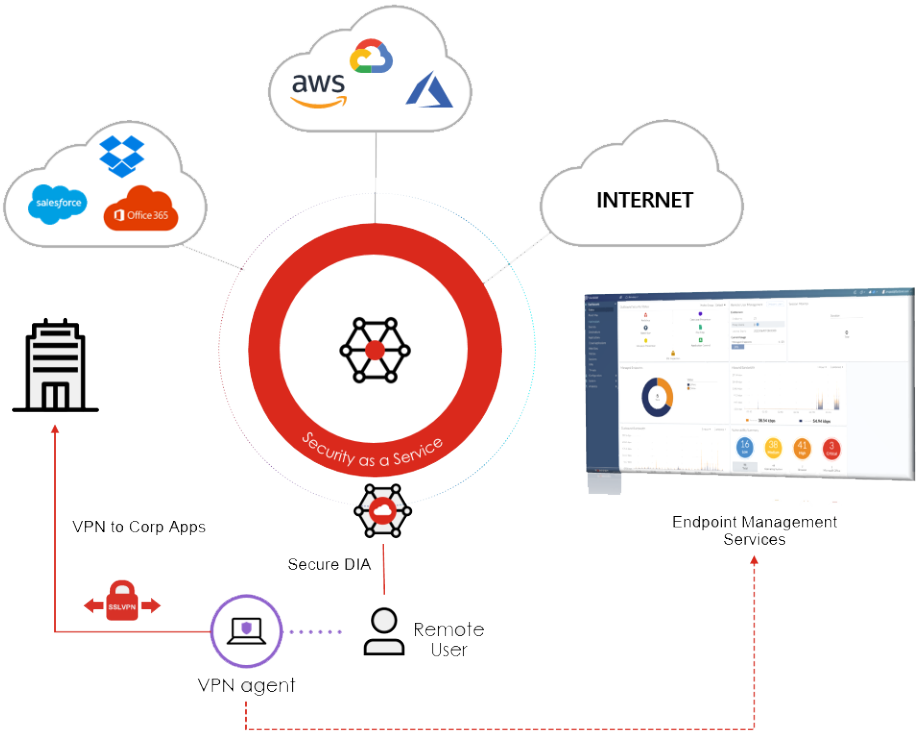
Solution overview

The FortiSASE solution offers several modes for remote clients to connect. Primarily, users can connect using FortiClient VPN in endpoint mode or forward traffic from their PC to the gateway in secure web gateway/proxy mode.

The use case that this guide discusses uses the latter mode to securely proxy traffic to the FortiSASE gateway to secure Internet traffic. FortiSASE exempts traffic destined for the corporate network through IPsec or SSL VPN from being proxied. This allows existing corporate traffic to remain undisrupted while adding security to traffic that remote users access through direct Internet access.

Since there are many FortiSASE gateways deployed in different geographic locations, remote users can connect to the nearest gateway with the least latency. This provides scalability to organizations that cannot build out infrastructure in different locations.

While this solution works with any VPN and security vendors, the deployment guide demonstrates a scenario where a FortiGate is securing the corporate office. Optionally, you can use endpoint management services to deploy FortiClient to protect endpoints and provide Zero Trust posture check.

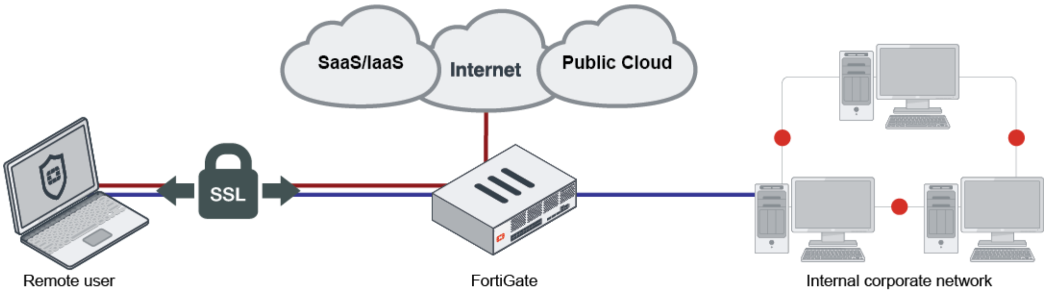


Design overview

Use cases and topology

SSL VPN networking

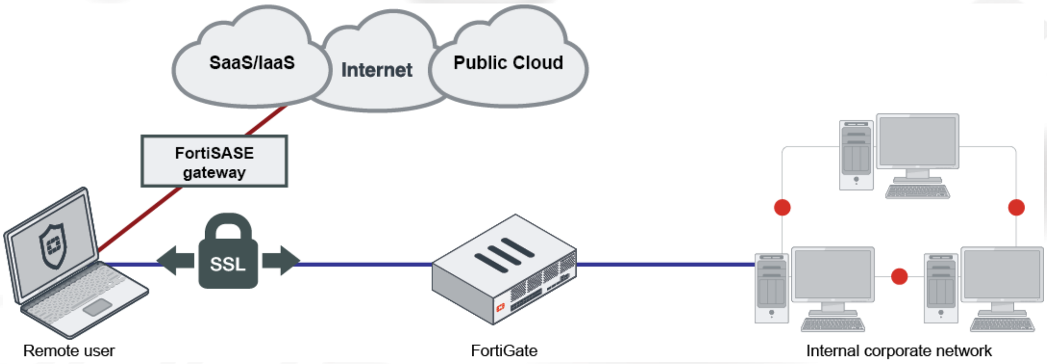
In the current deployment, an organization has deployed an existing teleworking solution using FortiGate SSL VPN. The deployment uses tunneling mode to tunnel all traffic through the FortiGate, including access to the Internet and cloud applications.



The VPN solution can use security vendors other than Fortinet.

FortiSASE SWG with SSL VPN

To offload security for remote workers' direct Internet access connection, you can use FortiSASE. In particular, connecting to FortiSASE in secure web gateway mode provides an agentless way to connect while still securely proxying traffic to the FortiSASE gateway. Instead of tunneling all traffic to the corporate gateway, this solution uses split tunneling to tunnel only traffic destined to the corporate network. As a result, remote users can access the Internet through FortiSASE gateways dedicated to securing Internet access while offloading bandwidth and resources taken up on the corporate firewall for scanning remote Internet traffic.



Design concept and considerations

Proxy configuration

This solution's design uses FortiSASE secure web gateway mode, which involves configuring and hosting a proxy autoconfiguration (PAC) file for respective endpoints to connect to the FortiSASE gateway. FortiSASE provides a preconfigured PAC file hosted on the FortiSASE server for use. You can download and customize the PAC to exclude the SSL VPN gateway and internal networks from being proxied. The customer server must host the custom PAC file.

Once the PAC file is hosted, you must configure endpoint computers to enable the proxy server and point to the PAC file to retrieve the proxy settings. On a Windows machine, configuring proxy settings at the operating system (OS) level is recommended so that all traffic is proxied. On other OSes where there is no option to configure proxy settings at the OS level, you can configure the browser to point to the PAC file.

To centrally manage proxy settings on endpoints, customers should consider using group policy management for Windows or other centralized management systems like mobile device management.

User configuration

You configure users on FortiSASE for endpoints to authenticate and connect to the FortiSASE gateway. If SAML SSO is enabled on FortiSASE, you cannot configure an LDAP or RADIUS connection. When designing the solution, consider where users are defined in your organization and use one of the following methods to integrate it with FortiSASE:

User type	Integration method
LDAP	**1.** Configure an LDAP connection. **2.** Import users and groups from the LDAP server to FortiSASE.
RADIUS	**1.** Configure a RADIUS connection. **2.** Import users and groups from the RADIUS server to

User type	Integration method
	FortiSASE.
Single sign on (SSO)	Configure an SSO connection, with FortiSASE as the service provider and another service, such as Azure Active Directory, as the identity provider.

See Authentication Sources and Access for information on authentication methods.

VPN configuration

This solution assumes that customers already have VPN gateways configured to secure traffic to their internal corporate network. Some organizations may also have configured their corporate firewall to forward and scan all traffic as the example demonstrates. In this case, to prevent all traffic from being sent over the corporate firewall, you should enable split tunneling so that only traffic destined to the corporate network is sent to the VPN gateway. FortiSASE proxies and scans other traffic.

Endpoint management

For added security, organizations may also use FortiClient EMS to provide endpoint management, security, and Zero Trust endpoint posture check. It is assumed that customers who are already using on-premise EMS or FortiClient Cloud will continue using their solution to manage endpoints. No changes to endpoint management are necessary.

Deployment overview

This section consists of the following:

- Product prerequisites on page 10
- Deployment plan on page 10

Product prerequisites

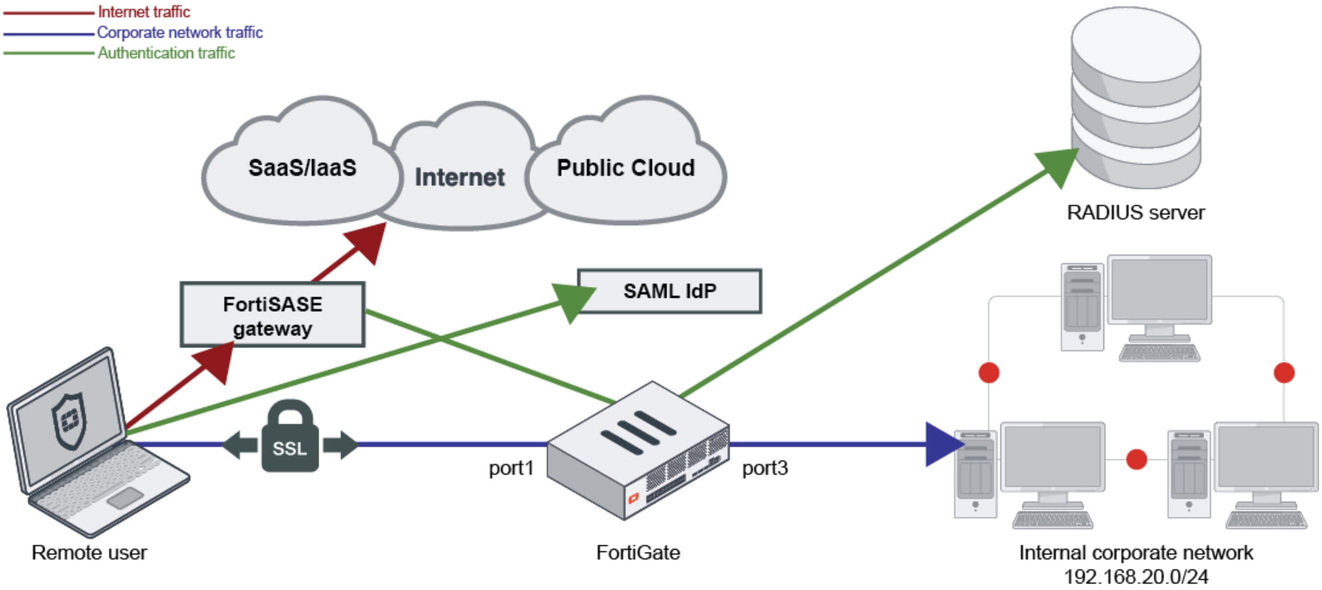
Customers should obtain enough FortiSASE Secure Web Gateway seats to support the number of remote endpoints that will use this service.

Deployment plan

This outlines the major steps to deploy this solution. Go to Deployment procedures on page 11 for detailed configuration steps:

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed. See Provisioning your FortiSASE instance on page 11.
2. Configure users. See Configuring SSO SAML users on page 12 and Configuring RADIUS users on page 13.
3. Configure Secure Web Gateway policies to apply desired scanning and filtering for your users. See Configuring security profiles and SWG policies on page 14.
4. Download the proxy autoconfiguration (PAC) file from the FortiSASE portal. Customize the file to exclude SSL VPN gateway and internal corporate networks. See Downloading and customizing the PAC file on page 15.
5. Host the PAC file on an externally accessible server. See Hosting the custom PAC file on page 16.
6. Configure proxy settings on endpoints to point to the PAC file. See Configuring proxy settings on endpoints on page 16.
7. Modify your SSL VPN gateway to enable split tunneling. See Modifying your SSL VPN gateway to enable split tunneling on page 17.

Deployment procedures



You can use the following procedures to migrate an SSL VPN teleworking solution to one that secures remote direct Internet access connections with FortiSASE Secure Web Gateway as the topology diagram illustrates.

Provisioning your FortiSASE instance

Ensure that you have purchased the contract to provision FortiSASE Secure Web Gateway (SWG).

To provision your FortiSASE instance:

1. From the Fortinet Support site, register your FortiSASE contract.
2. Once registered, go to *Services > Cloud Services > FortiSASE* to provision your FortiSASE instance.
3. When provisioning, select the geographic location for your security sites and logging.
4. Once provisioned, the FortiSASE dashboard displays your entitlement in the Remote User Management widget. The number of SWG users that the widget lists is the number of users that are entitled to use this service in SWG mode. Go to *System > SWG Configuration*. Toggle *Enable* to on, then click *OK*. The

GUI may take a few minutes to reload to display SWG configuration options in the menu.

Configuring SSO SAML users

Depending on the authentication source, the user configuration steps differ. This example shows configuring single sign on (SSO) users and user groups against an Azure Active Directory (AD) identity provider (IdP).

For configuring other authentication sources, see Authentication Sources and Access. When SSO is configured, other user types do not work.

To configure the SSO SAML configuration:

1. Go to *Configuration > SWG User SSO*.
2. In step one, *Configure Identity Provider*, collect the URLs on FortiSASE and enter them into the respective fields in the SSO settings of the respective Azure AD enterprise application.

FortiSASE SAML field	Azure AD Basic SAML Configuration field
Entity ID	Identifier (Entity ID)
Assertion Consumer Service (ACS) URL	Reply URL (Assertion Consumer Service URL)
Portal (Sign On) URL	Sign on URL
Single Logout Service (SLS) URL	Logout Url (Optional)

   Click *Next*.
3. In step two, *Configure Service Provider*, collect the URLs from the Azure AD enterprise application *Single sign-on > Set up <application name>*. Enter them into the respective fields in FortiSASE.

Azure AD > *Set up <application name>* fields	FortiSASE SAML field
Login URL	IdP Single Sign-On URL
Azure AD Identifier	IdP Entity ID
Logout URL	IdP Single Log-Out URL

   Click *Next*.
4. With claims mapping, you can specify the identifier for the username and group name attributes in Azure. The default configuration uses username and group respectively, which matches the attribute names in Azure. If you need custom names, modify them here.
5. Enable and configure *SAML Group Matching* if you only want Azure AD users of a certain group to be allowed to authenticate. Otherwise, leave this setting disabled. You can further define more granular groups when you configure user group settings.
6. FortiSASE requires the IdP certificate is required. Configure the IdP certificate:
7. Download the certificate from Azure AD enterprise application > *Single sign-on > SAML Signing Certificate*. Download Certificate (Base64).
   a. On the *IdP Certificate* dropdown list, click *Create*.
   b. In the *Import Remote Certificate* slide-in, upload the certificate from Azure.
   c. Enter a unique name for the certificate, then click *OK*.
   d. Select the certificate, then click *Next*.

8. Review your settings. The click *Submit* to apply.
9. Upon successful configuration, FortiSASE prompts for instructions to onboard users. Follow the steps under *SWG Users* to download the SWG certificate for usage on the client. The certificate package contains the built-in certificate authority certificate for the FortiSASE instance. This must be installed in the certificate store on the client to trust the certificate chain for pages that FortiSASE has signed.

To configure an SSO user group:

1. Go to *Configuration > Users*.
2. Click *Create*. Select *User Group*, and click *Next*.
3. In the *Name* field, enter the desired name.
4. Under *Remote Groups*, click *Create*.
5. From the *Remote Server* dropdown list, select the SAML server that you created.
6. In the *Groups* field, enter the names of the group(s) that you will allow access on FortiSASE. This is the group object ID of the user group defined on Azure.
7. Click *OK* to finish. Click OK again to create the user group. You can apply this new user group to your SWG policies.

Configuring RADIUS users

Depending on the authentication source, the user configuration steps differ. The example shows configuring a RADIUS server and user groups. For configuring other authentication sources, see Authentication Sources and Access.

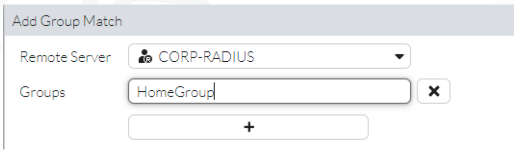
If Secure Web Gateway (SWG) user single sign on (SSO) is configured, RADIUS user configuration does not take effect. If you plan to use RADIUS, first delete your SWG user SSO configuration.

To configure the RADIUS server:

1. Go to *Configuration > RADIUS*.
2. Click *Create* to add a new RADIUS server.
   a. Configure the RADIUS server settings:
   b. Enter the desired server name.
   c. Do not enable *Include All Users* unless you want all users on the RADIUS server to be allowed access to FortiSASE.
   d. Click *Next*.
   e. In the *Primary Server > IP/Name* field, enter the primary server IP address or fully qualified domain name.
   f. In the *Primary Server > Secret* field, enter the primary server secret.
   g. If your organization has a redundant RADIUS server, enter its information in the *Secondary Server* section.
3. Click *Test Connection*.
4. Do one of the following:
   a. If the connection succeeds, click *Next*.
   b. If the connection does not succeed, try again. Confirm your RADIUS server allows traffic from the FortiSASE gateway IP address. This may require sniffing for traffic on port 1812.
5. Review and submit the settings.

To configure a RADIUS user group:

1. Go to *Configuration > Users*.
2. Click *Create*.
3. Configure the RADIUS user group(s):
   a. In the *Name* field, enter the desired name.
   b. Under *Remote Groups*, click *Create*.
   c. From the *Remote Server* dropdown list, select the RADIUS server that you created.
   d. In the *Groups* field, enter the group names of the group(s) that will be allowed access on FortiSASE.



Remote Server: CORP-RADIUS

Groups: HomeGroup

4. Click *OK*.
5. Click *OK* again.
6. A slide-in appears with instructions on how to onboard an end user. Follow the steps under *SWG Users* to download the SWG certificate for usage on the client. The certificate package contains the built-in certificate authority certificate for the FortiSASE instance. This must be installed in the certificate store on the client to trust the certificate chain for pages that FortiSASE has signed.
7. Click *Close*.

Configuring security profiles and SWG policies

FortiSASE has a default security profile configured, which is applied to the Allow-All Secure Web Gateway (SWG) policy. When all users, sources, and destinations require the same scanning and protection, maintaining only one default security profile suffices. However, if different users, sources, or destinations require different protection, create different profile groups for each group of users.

The default SWG policies block any traffic destined for Botnet and C&C servers but allow the rest. Consider your user base and design your SWG policies carefully. FortiSASE matches policies from top down, so add more restrictive policies at the top and less restrictive policies at the bottom.

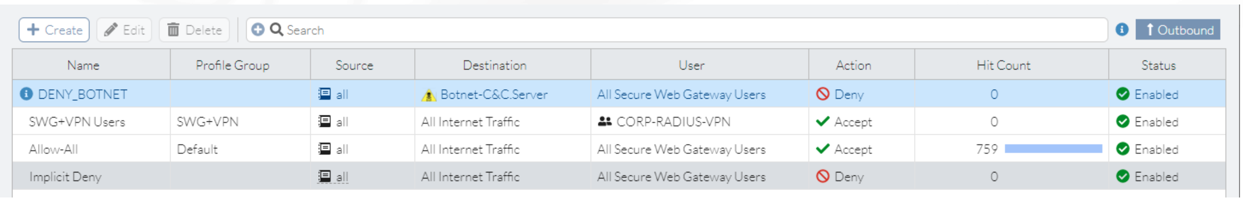
To configure a new security profile:

1. Go to *Configuration > Security*.
2. On the top-right, click the dropdown list beside *Profile Group*, then click *Create*.
3. In the *Create Profile Group* slide-in, enter a name for the new profile.
4. In *Initial Configuration*, select whether to use a basic initial configuration or base the profile on an existing profile.
5. Click *OK*.
6. On the top-right, click the dropdown list again, and select your newly created profile.
7. Edit the profile as desired. See Security for details.

To create an SWG policy:

1. Go to *Configuration > SWG Policies*.
2. Click *Create*.

3. Configure the SWG policy:
   a. In the *Name* field, enter the desired policy name.
   b. For *Action*, select *ACCEPT*.
   c. In the *Source* field, specify source subnet(s) as desired.
   d. In the *User* field, specify the user group used for your remote users.
   e. In the *Destination* field, specify destination subnet(s) as desired.
   f. In the *Profile Group* field, specify the profile that you created.
   g. In the *Log Allow Traffic* field, select *All Sessions*.
4. Click *OK*.
5. Move the new policy above the Allow-All policy.



Name	Profile Group	Source	Destination	User	Action	Hit Count	Status
DENY_BOTNET		all	Botnet-C&C.Server	All Secure Web Gateway Users	Deny	0	Enabled
SWG+VPN Users	SWG+VPN	all	All Internet Traffic	CORP-RADIUS-VPN	✓ Accept	0	Enabled
Allow-All	Default	all	All Internet Traffic	All Secure Web Gateway Users	✓ Accept	759	Enabled
Implicit Deny		all	All Internet Traffic	All Secure Web Gateway Users	Deny	0	Enabled

Downloading and customizing the PAC file

The *System* > *SWG Configuration* page displays the Secure Web Gateway (SWG) servers, port, and hosted proxy autoconfiguration (PAC) file. You can download the predefined PAC file to customize.

PAC files contain rules for the proxy client to follow to route traffic to the proxy server, which in this case is the FortiSASE SWG. By default, it contains the servers in regions that you have selected when provisioning the FortiSASE instance.

This example customizes the PAC file to exclude corporate networks and the corporate SSL VPN gateway from being forwarded to the FortiSASE SWG server:

```
function FindProxyForURL(url, host)
{
//
//Bypass proxy for internal hosts
//
if (isInNet(host, "0.0.0.0", "255.0.0.0")||
    isInNet(host, "127.0.0.0", "255.0.0.0") ||
           isInNet(host, "169.254.0.0", "255.255.0.0") ||
    isInNet(host, "192.168.20.0", "255.255.255.0") ||
    isInNet(host, "64.206.157.136", "255.255.255.255"))
{
return "DIRECT";
}
//
//Bypass proxy for the Corporate SSLVPN Gateway
//
if (dnsDomainIs(host, ”Corp_SSLVPN_GW"))
{
return "DIRECT";
}

return "PROXY 0ni8tgf4-0hdw554o-sslgateway-fos001-region6.edge.prod.fortisase.com:10447;
DIRECT";
}
```

Hosting the custom PAC file

Once you have modified the proxy autoconfiguration (PAC) file, you should host it on a web server that is externally accessible. The PAC file does not require user authentication to access. However, any user that is pointing to the PAC file will be subject to authentication by FortiSASE when it accesses the Internet.

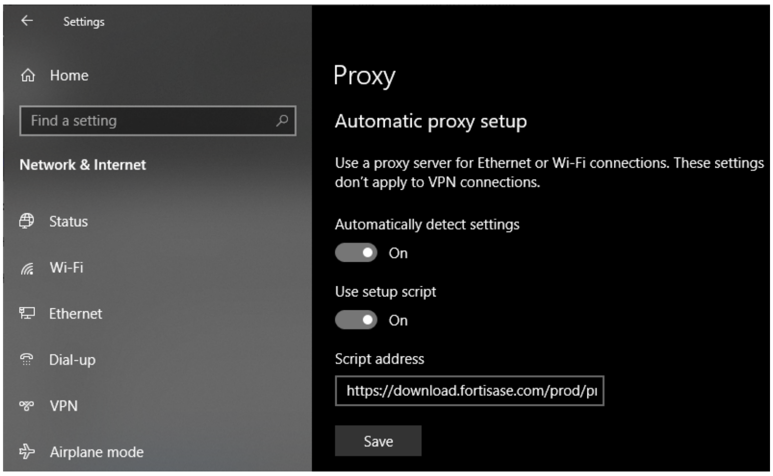
Configuring proxy settings on endpoints

Proxy settings can differ between operating systems (OS) and browsers. Refer to your OS or browser for instructions on configuring proxy settings to point to the custom proxy autoconfiguration file. In a larger environment, you can use an enterprise management system to push proxy settings to endpoints.

This example demonstrates manually configuring proxy settings on Windows 10.

To manually configure proxy settings on a Windows 10 endpoint:

1. Go to *Windows Settings > System > Proxy Settings*.
2. Enable *Use setup script*.
3. In the *Script address* field, enter the hosted PAC file URL.



Proxy

Automatic proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Automatically detect settings: On

Use setup script: On

Script address: https://download.fortisase.com/prod/pı

4. The next time that the user starts a browser session, the browser displays an authentication prompt.
5. The end user enters their FortiSASE user credentials in the prompt to authenticate.

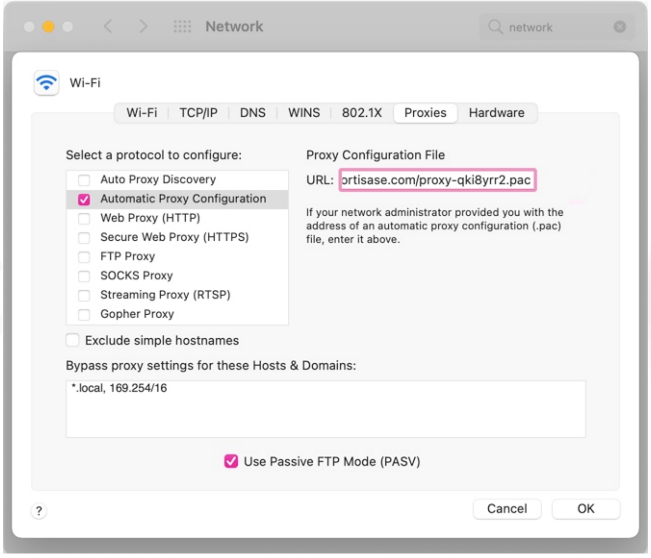
See Configuring a proxy policy for details.

This example demonstrates manually configuring proxy settings on macOS. See also Change proxy settings in Network preferences on Mac.

To manually configure proxy settings on a macOS endpoint:

1. Go to the Apple menu > *System Preferences > Network*.
2. In the list, select the Network service. For example, you may select your connected wireless SSID.
3. Click *Advanced*.
4. On the *Proxies* tab, select the protocol to configure. Enable *Automatic Proxy Configuration*, then enter the URL to your hosted PAC file.

5. Click *OK*, then apply to apply the changes.



Select a protocol to configure:

- □ Auto Proxy Discovery
- ☑ Automatic Proxy Configuration
- □ Web Proxy (HTTP)
- □ Secure Web Proxy (HTTPS)
- □ FTP Proxy
- □ SOCKS Proxy
- □ Streaming Proxy (RTSP)
- □ Gopher Proxy

Proxy Configuration File

URL: ortisase.com/proxy-qki8yrr2.pac

If your network administrator provided you with the address of an automatic proxy configuration (.pac) file, enter it above.

□ Exclude simple hostnames

Bypass proxy settings for these Hosts & Domains:

*.local, 169.254/16

☑ Use Passive FTP Mode (PASV)

6. The next time that the user starts a browser session, the browser displays an authentication prompt.
7. The end user enters their FortiSASE user credentials in the prompt to authenticate.

Modifying your SSL VPN gateway to enable split tunneling

Modify your settings on your SSL VPN gateway so that only traffic to the corporate network is tunneled to the VPN gateway. The following example modifies the FortiOS SSL VPN settings.

To modify FortiOS SSL VPN settings to enable split tunneling:

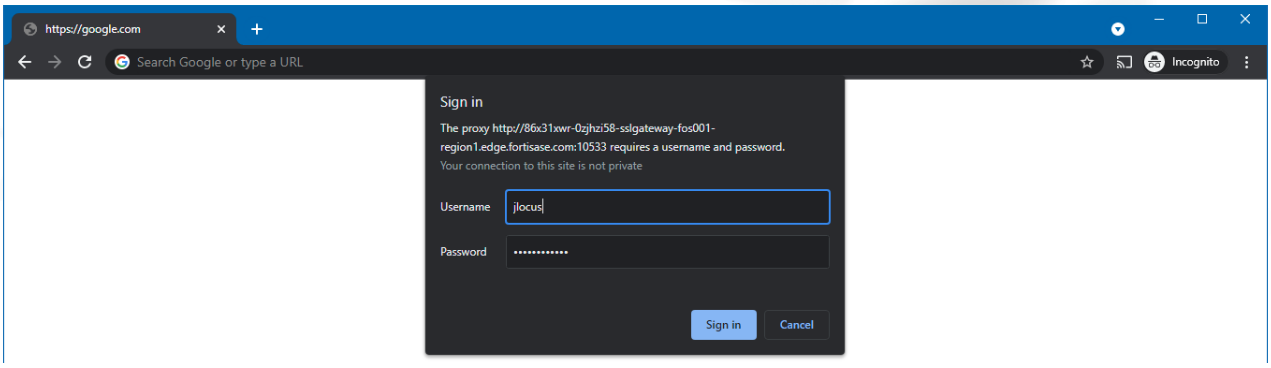
1. In FortiOS, go to *VPN > SSL-VPN Portals*.
2. Edit the portal that your remote users use.
3. Under *Tunnel Mode > Split tunneling*, select *Enabled Based on Policy Destination*.
4. Click *OK*.
5. Go to *Policy & Objects*.
6. Disable the firewall policy that allows traffic from the SSL VPN tunnel interface to WAN.
7. Edit the firewall policy that allows traffic from the SSL VPN tunnel interface to LAN.
8. Select the address of the internal network that will be allowed. Only this network will be routable on the endpoint.
9. Click *OK*.

Testing and monitoring

The basic configuration is complete at this point. Test the connections to the Internet and corporate networks on an endpoint.

To test connection to the Internet on a Windows computer with a RADIUS user:

1. From the endpoint, open a browser.
2. Browse to a webpage.
3. An authentication prompt appears. Enter your username and password.



Sign in

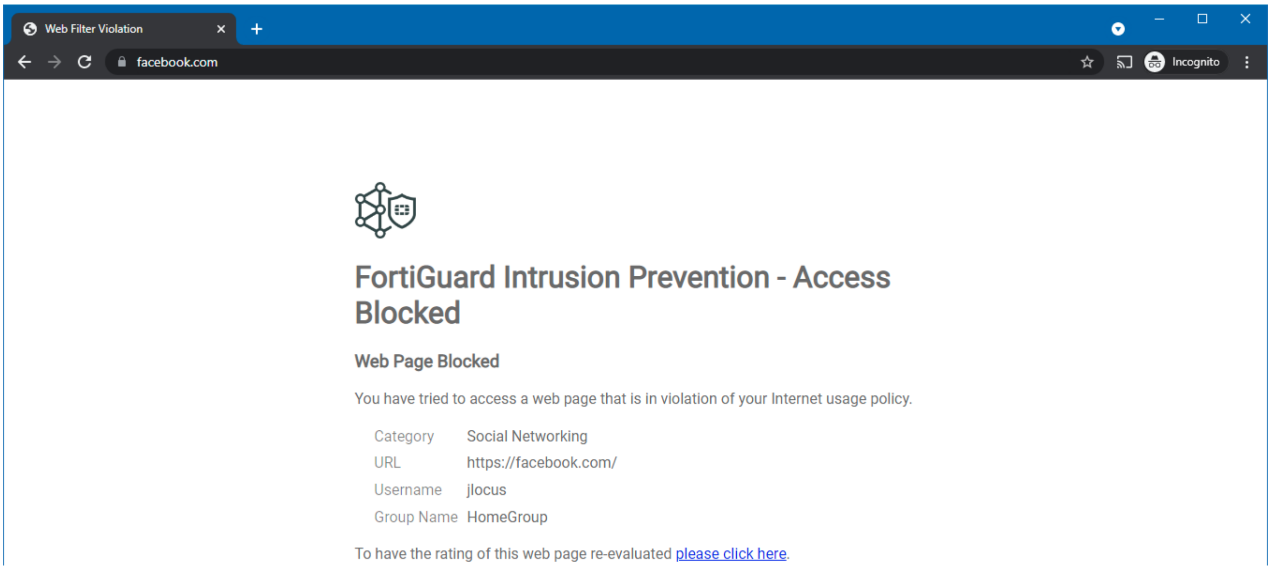
The proxy http://86x31xwr-0zjhzi58-sslgateway-fos001-region1.edge.fortisase.com:10533 requires a username and password.

Your connection to this site is not private

Username: jlocus

Password: ••••••••••••

4. Once authenticated, you can browse to any webpage. FortiSASE scans this traffic.
5. Browse to a webpage that triggers a Web Filter violation. The browser shows a message that FortiSASE is blocking the webpage.



FortiGuard Intrusion Prevention - Access Blocked

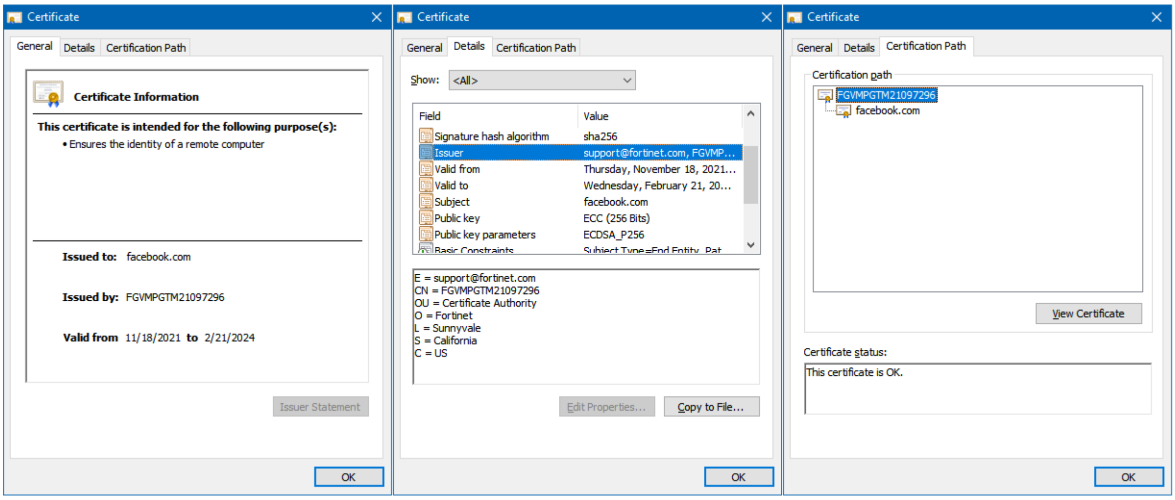
Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category	Social Networking
URL	https://facebook.com/
Username	jlocus
Group Name	HomeGroup

To have the rating of this web page re-evaluated please click here.

For the blocked webpage message to display without a certificate warning, the FortiSASE root certificate authority certificate must be installed on the endpoint. The following shows a valid certificate chain.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: facebook.com

Issued by: FGVMPGTM21097296

Valid from 11/18/2021 to 2/21/2024

Show: <All>

Field	Value
Signature hash algorithm	sha256
Issuer	support@fortinet.com, FGVMP...
Valid from	Thursday, November 18, 2021...
Valid to	Wednesday, February 21, 20...
Subject	facebook.com
Public key	ECC (256 Bits)
Public key parameters	ECDSA_P256
Basic Constraints	Subject Type=End Entity, Pat

```
E = support@fortinet.com
CN = FGVMPGTM21097296
OU = Certificate Authority
O = Fortinet
L = Sunnyvale
S = California
C = US
```

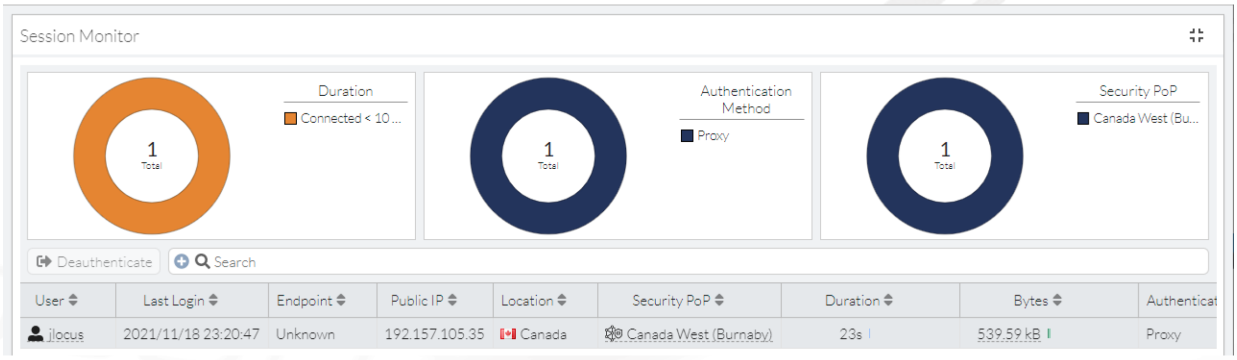
Certification path

- FGVMPGTM21097296
  - facebook.com

Certificate status:

This certificate is OK.

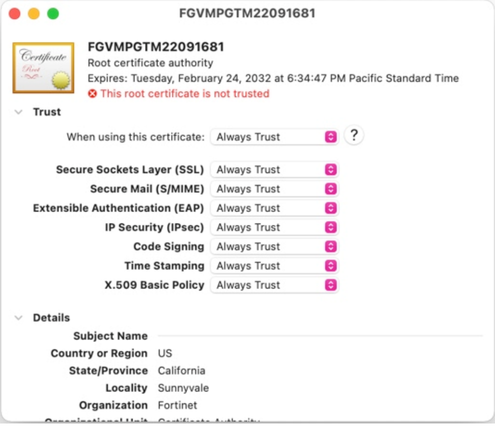
6. In FortiSASE, go to *Session Monitor* to see the logged in user.



User	Last Login	Endpoint	Public IP	Location	Security PoP	Duration	Bytes	Authenticat
jlocus	2021/11/18 23:20:47	Unknown	192.157.105.35	Canada	Canada West (Burnaby)	23s	539.59 kB	Proxy

To test connection to the Internet on a macOS computer with an Azure Active Directory (AD) user:

1. From the endpoint, open a browser.
2. Browse to a webpage. The page redirects to a Microsoft login page to perform single sign on.
3. Log in using your Azure AD credentials.
4. Once authenticated, you can browse to any webpage. FortiSASE scans this traffic.
5. To properly browse any HTTPS websites, you must install the FortiSASE root certificate on the endpoint. Double-click the FortiSASE certificate that the administrator provided during onboarding. In the *Keychain* field, select *System*, then click *Add*.
6. When you view the certificate, the root certificate appears as not trusted. Expand the *Trust* section. In the *When using this certificate* field, select *Always Trust*.



FGVMPGTM22091681

FGVMPGTM22091681
Root certificate authority
Expires: Tuesday, February 24, 2032 at 6:34:47 PM Pacific Standard Time
This root certificate is not trusted

Trust

When using this certificate:	Always Trust
Secure Sockets Layer (SSL)	Always Trust
Secure Mail (S/MIME)	Always Trust
Extensible Authentication (EAP)	Always Trust
IP Security (IPsec)	Always Trust
Code Signing	Always Trust
Time Stamping	Always Trust
X.509 Basic Policy	Always Trust

Details

Subject Name	
Country or Region	US
State/Province	California
Locality	Sunnyvale
Organization	Fortinet
Organizational Unit	Certificate Authority

7. Save the configuration and add the certificate to the system keychain.
8. You can connect to HTTPS websites without seeing a warning. Browse to an HTTPS website, then go to *Session Monitor* in FortiSASE to see the logged in user.

To test connection to the corporate network:

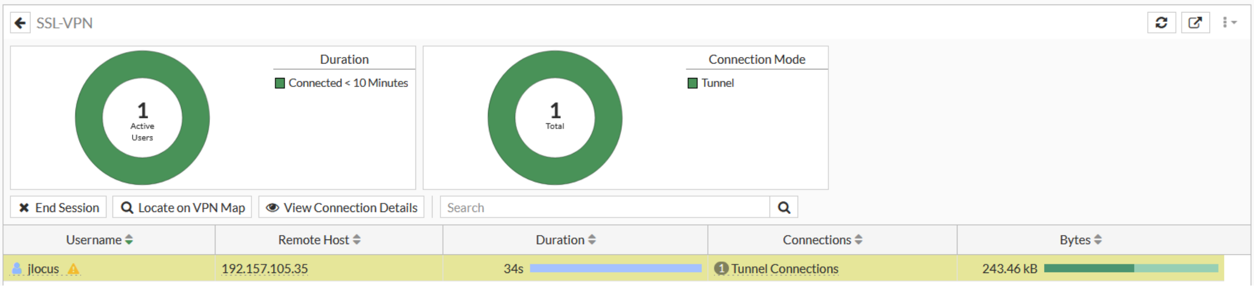
1. On the endpoint, connect to the SSL VPN gateway using the VPN client (FortiClient). In this scenario, the SSL VPN user and FortiSASE user is from the same source.
2. Once VPN connects, verify the routes from Windows Command Prompt:

```
> route print
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.10.1     10.10.10.25     60
        10.10.10.0    255.255.255.0         On-link     10.10.10.25    316
    10.212.134.200  255.255.255.255         On-link  10.212.134.200    257
```

```
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.20.0    255.255.255.0  10.212.134.201  10.212.134.200      1
```

The corporate network (192.168.20.0/24) is routed through the SSL VPN interface.

3. In FortiOS, go to *Firewall > Network Dashboard > SSL-VPN* widget to see the logged in VPN user.



Username	Remote Host	Duration	Connections	Bytes
jlocus	192.157.105.35	34s	1 Tunnel Connections	243.46 kB

4. From the endpoint, connect to an internal resource on the corporate network. The connection succeeds.

www.fortinet.com