Secure Private Access Architecture Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

What is the FortiSASE Secure Private Access architecture? 4
- Intended Audience 6
- About this guide 6

Design overview 8
- Design concept and considerations 9
  - Terms, acronyms, and definitions 9
  - FortiSASE steering method implementation is required 9
  - Endpoint device and traffic type considerations 10
  - Relevant features 11
- Recommended architectures to implement SPA use cases 11

Client-initiated use cases 13
- Agent access to private applications using the IP address or domain name and security posture tags 14
  - Traffic flow 14
  - Appropriate use 15
  - Prerequisites 15
  - Considerations 15
- Agentless access to private web applications using Proxy for remote users where the installation of FortiClient is not possible 16
  - Traffic flow 16
  - Appropriate use 16
  - Prerequisites 17
  - Considerations 17
- Agentless access to private web applications using a bookmark portal for unmanaged devices 17
  - Traffic flow 18
  - Appropriate use 18
  - Prerequisites 19
  - Considerations 19
- Access to private applications using the application IP or DNS redirection from on-premise users and devices where installation of FortiClient is not feasible 19
  - Traffic flow 20
  - Appropriate use 20

Prerequisites 20
Considerations 20
Additional configurations 21
Pre-logon connectivity 21
Autoconnect tunnel connectivity 21
Server-initiated use cases 22
Server-to-Client application access 22
Traffic flow 23
Appropriate use 23
Prerequisites 23
Considerations 23
Client-to-Client application access 24
Traffic flow 24
Appropriate use 24
Prerequisites 25
Considerations 25
More information 26
4-D (Define, Design, Deploy, Demo) documentation 26
Change log 27

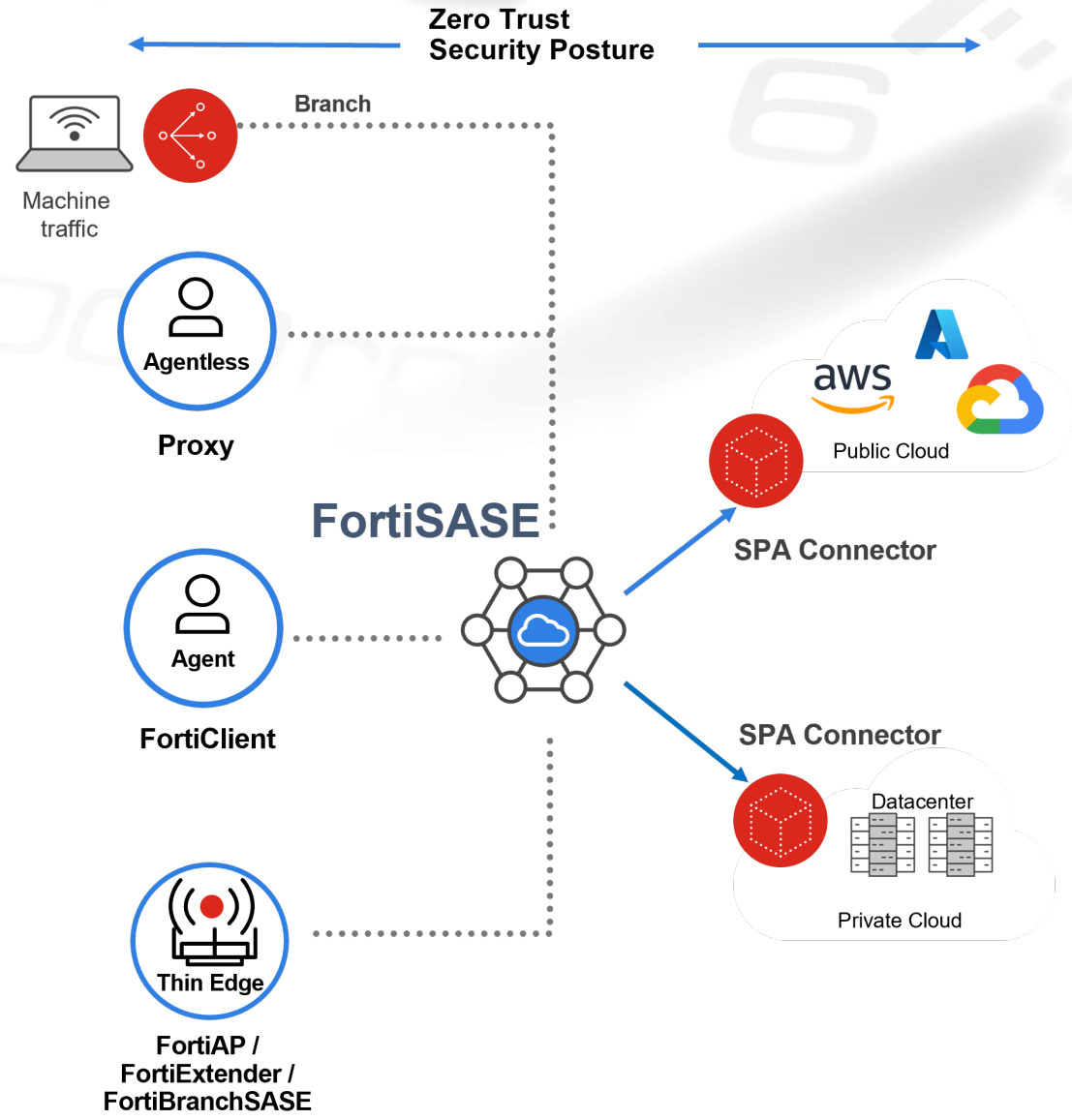
What is the FortiSASE Secure Private Access architecture?

With FortiSASE, remote users form secure connections to corporate, private applications by accessing global FortiSASE Security Points of Presence (PoPs), which enforce an organization's security policies regardless of the locations of remote users. FortiSASE Secure Private Access (SPA) enforces security when users access private applications.

FortiSASE can seamlessly integrate with the following SPA Connector options to provide secure access to private applications in the customer's data center, private cloud, or public cloud tenant:

- An existing FortiGate SD-WAN hub.
- Any existing FortiGate NGFW or DC Firewall.

SPA can leverage user identity and device context based zero-trust access to explicit applications with continuous device posture re-assessment from remote or on-premises locations.



The most common SPA use cases for FortiSASE are described as follows:

Direction of traffic flow	SPA use case	Description
Client-initiated	Agent access to private applications using the application IP address or domain name and security posture tags	This is the most common SPA use case. Remote users on supported endpoint devices use FortiClient software to steer traffic to a FortiSASE security PoP and then steer private traffic to the on-prem network over the IPsec tunnel between the FortiSASE security PoP and the SPA Connector. Applications can be accessed via either private IP addresses or domain names when DNS redirection is used. Security posture tags are used for security posture checking.

Direction of traffic flow	SPA use case	Description
	Agentless access to private web applications for remote users where the installation of FortiClient is not possible.	Remote users with web browsers supporting Proxy (formerly Secure Web Gateway or SWG) to steer web traffic to a FortiSASE security PoP and then steer private traffic to the on-prem network over the IPsec tunnel between the FortiSASE security PoP and the SPA Connector. Applications are accessed via either private IP addresses or domain names when DNS redirection is used.
	Agentless access to private web applications using a bookmark portal for unmanaged devices	Contractors or temporary remote users use browser-only solutions to access private web-based applications from a protected bookmark portal.
	Access to private applications from on-premises users and devices (servers and IoT) where installation of FortiClient is not feasible	Branch offices use a Thin Edge device including FortiAP, FortiExtender, or FortiBranchSASE, or a branch device including a FortiGate Secure Edge device or a Branch On-Ramp device to securely access private applications.
Server-initiated	Server-to-Client applications access	Private application servers securely access remote user endpoints running FortiClient software.
	Client-to-Client applications access	Remote user endpoints running FortiClient software securely access similar remote user endpoints.

Optionally, remote user endpoints can be configured with pre-logon connectivity. This feature allows onboarding of remote users who have never logged in to their domain-joined Windows endpoints to access the corporate Active Directory (AD) server. These endpoints are preconfigured for pre-logon connectivity.

Moreover, remote user endpoints are configured with autoconnect tunnel connectivity that makes use of automatically connecting to a Security PoP, remembering the login password, and enforcing an always-up tunnel connection.

- With Windows endpoints, the remember password feature works with OAuth authentication and SAML authentication with IdP support for persistent sessions.
- With MacOS endpoints, the remember password feature works with SAML authentication with IdP support for persistent sessions.

Intended Audience

Mid-level network and security architects in companies of all sizes and verticals should find this guide helpful.

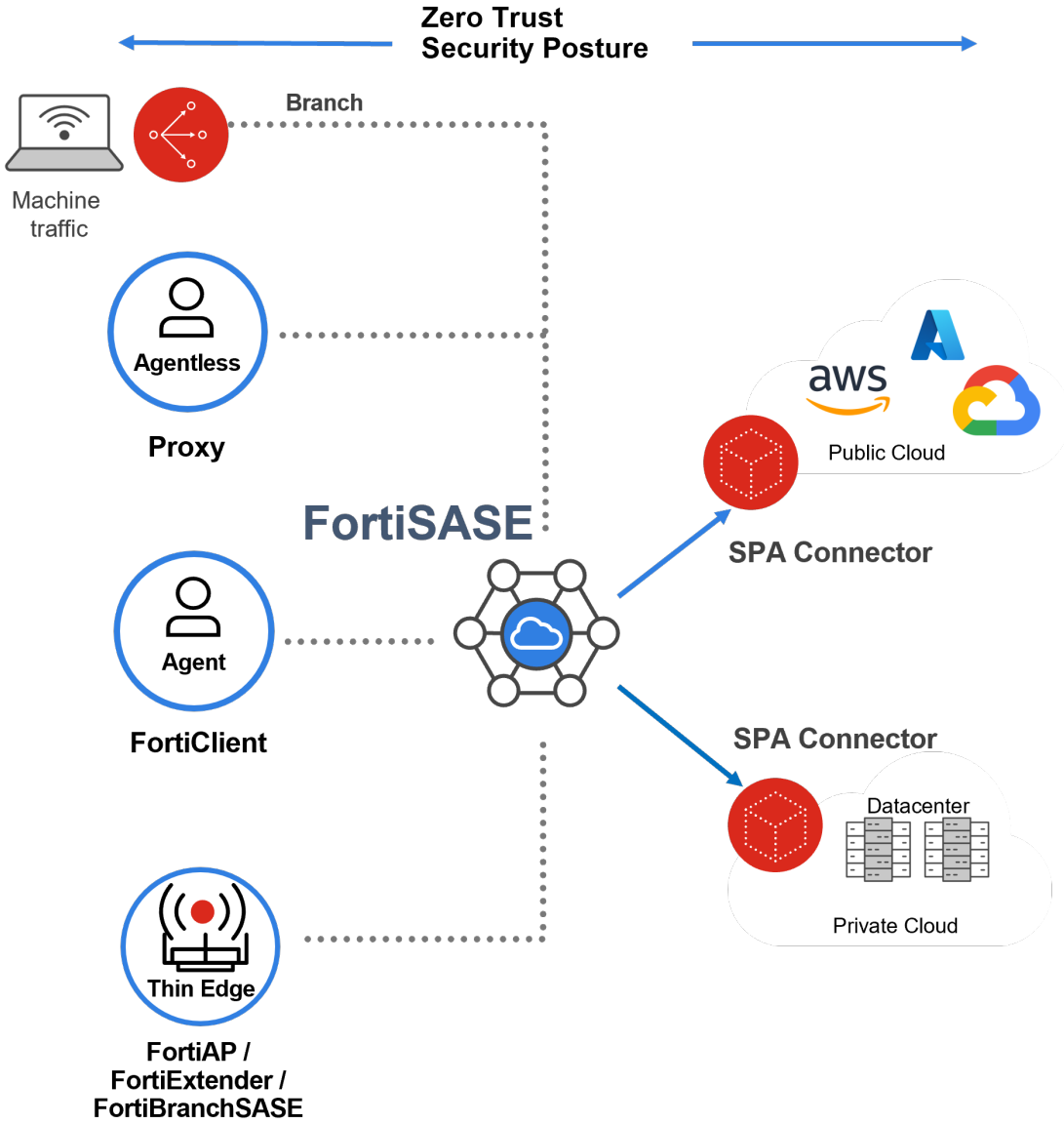
About this guide

This guide is meant to provide high level insight into FortiSASE architectures for secure access service edge (SASE), namely, Secure Private Access (SPA) use cases and relevant features. It is meant to be used in conjunction with other

technical documentation for each of the components listed in the guide. Where relevant, links to the administrative guides and other technical reference guides will be listed. See More information on page 26.

Design overview

In this architecture, the design goal is to enforce secure private access (SPA) when users access private applications.



Design concept and considerations

Terms, acronyms, and definitions

Acronym	Definition	Description
-	Agent	FortiClient agent software running on a supported endpoint platform.
DEM	Digital Experience Monitoring	End to End Digital Experience Monitoring includes Last-mile monitoring of each cloud location, first mile monitoring of the user's local network, and real-time endpoint monitoring. In the context of SPA, DEM is used for monitoring the reachability of private applications behind SPA Connectors.
SIA	Secure Internet access	FortiSASE use case to describe secure remote user access to Internet and web-based applications.
SPA	Secure private access	FortiSASE use case to describe secure remote user access to private applications.
-	SPA Connector	Hardware or software connector deployed in a corporate data center, private cloud, or public cloud tenant that FortiSASE integrates with to provide secure access to private applications.
SSA	Secure SaaS access	FortiSASE use case to describe secure remote user access to SaaS applications.
Security PoP	Security Point-of-Presence	A location with FortiSASE security capabilities that a remote user connects to. Typically, this location is geographically close to the remote user.
-	Steering method	Method for steering traffic from remote users to FortiSASE. Supported steering methods include agent, agentless, IPsec with routing, and IPsec with explicit proxy.
ZTNA	Zero trust network access	For endpoints using FortiClient, user identity and device context based zero-trust access to explicit applications with continuous device posture re-assessment from remote or on-premises locations.

FortiSASE steering method implementation is required

All traffic from FortiSASE end users must be steered to FortiSASE.

Several flexible steering methods are used to steer or redirect network traffic from the user edge to FortiSASE. These steering methods can be used to securely access Internet, private, and SaaS destinations or applications, respectively, and therefore used to implement FortiSASE SIA, SPA, and SSA use cases.

Steering Method	Destinations		
Agent	Internet and web-based applications	Private applications via SPA Connector	SaaS applications via CASB
IPsec with routing			
IPsec with explicit proxy			
Agentless			
Use case	Secure Internet Access (SIA)	Secure Private Access (SPA)	Secure SaaS Access (SSA)

SIA is to be distinguished from the other main use cases for FortiSASE including:

- Secure Private Access (SPA) enforces security when users access private applications.
- Secure SaaS Access (SSA) enforces security when users access SaaS applications.

The secure private access (SPA) and secure SaaS access (SSA) use cases depend on one or more steering methods to be implemented because traffic must be steered to FortiSASE first before being destined for the internet, private resources, or SaaS applications. Therefore, one or more of the steering methods must be implemented in a FortiSASE deployment.

As exceptions, for zero trust network access (ZTNA) and steering bypass destinations, traffic does not pass through FortiSASE. For ZTNA use cases, traffic is destined directly to private resources that the FortiGate ZTNA application gateway protects. For steering bypass destinations, traffic is destined directly for the internet or SaaS applications, bypassing FortiSASE protections. These use cases are outside of the scope of this guide.

Endpoint device and traffic type considerations

The following table summarizes the endpoint device and traffic type characteristics of each SPA architecture:

Direction of traffic flow	SPA use case	Traffic Type
Client-initiated	Agent access to private applications using the IP address or domain name and security posture tags on page 14	All protocols
	Agentless access to private web applications using Proxy for remote users where the installation of FortiClient is not possible on page 16	Web (HTTP and HTTPS)
	Agentless access to private web applications using a bookmark portal for unmanaged devices on page 17	Web (HTTPS only)
	Access to private applications using the application IP or DNS redirection from on-premise users and devices where installation of FortiClient is not feasible on page 19	All protocols
Server-initiated	Server-to-Client application access on page 22	All protocols
	Client-to-Client application access on page 24	All protocols

Relevant features

SPA architectures are used with these FortiSASE features to secure access to private applications:

Feature	Description
Advanced Threat Detection with FortiGuard Security Services	Powered by FortiOS and FortiGuard, FortiSASE provides next-generation firewall (NGFW) capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System (DNS) security. Security efficacy matches that of a FortiGate Firewall. All the security services like AV, IPS, Web Filtering, DLP are enabled by the FortiGuard AI/ML powered security.
Authentication and Captive Portal	Support for SAML based authentication and seamless integration with third party identity providers such as Microsoft Entra ID and Okta can be integrated along with support for native FortiAuthenticator Cloud. Support is also available for local, LDAP, and RADIUS. FortiSASE supports a captive portal that enforces user authentication for endpoints connected behind edge devices that attempt to access private applications.
Autoconnect tunnel connectivity	Remote user endpoints can enforce autoconnect tunnel connectivity that makes use of automatically connecting to a Security PoP, remembering the login password, and enforcing an always-up tunnel connection.
Digital Experience Monitoring (DEM)	End to End Digital Experience Monitoring includes Last-mile monitoring of each cloud location, first mile monitoring of the user's local network, and real-time endpoint monitoring. In the context of SPA, DEM is used for monitoring the reachability of private applications behind SPA Connectors.
DNS redirection	For remote users, FortiSASE must be configured to use an internal DNS server to resolve internal hostnames for private applications.
Pre-logon connectivity	For endpoints using agent access, FortiSASE allows onboarding of remote users who have never logged in to their domain-joined Windows endpoints to access the corporate Active Directory (AD) server. Endpoints are preconfigured with machine certificates for pre-logon authentication.
Security posture tags	For endpoints using agent access, FortiSASE leverages user identity and device context based zero-trust access using security posture tags to explicit applications with continuous device posture re-assessment from remote or on-premises locations.

Recommended architectures to implement SPA use cases

The recommended architectures used to implement these use cases in FortiSASE are described as follows:

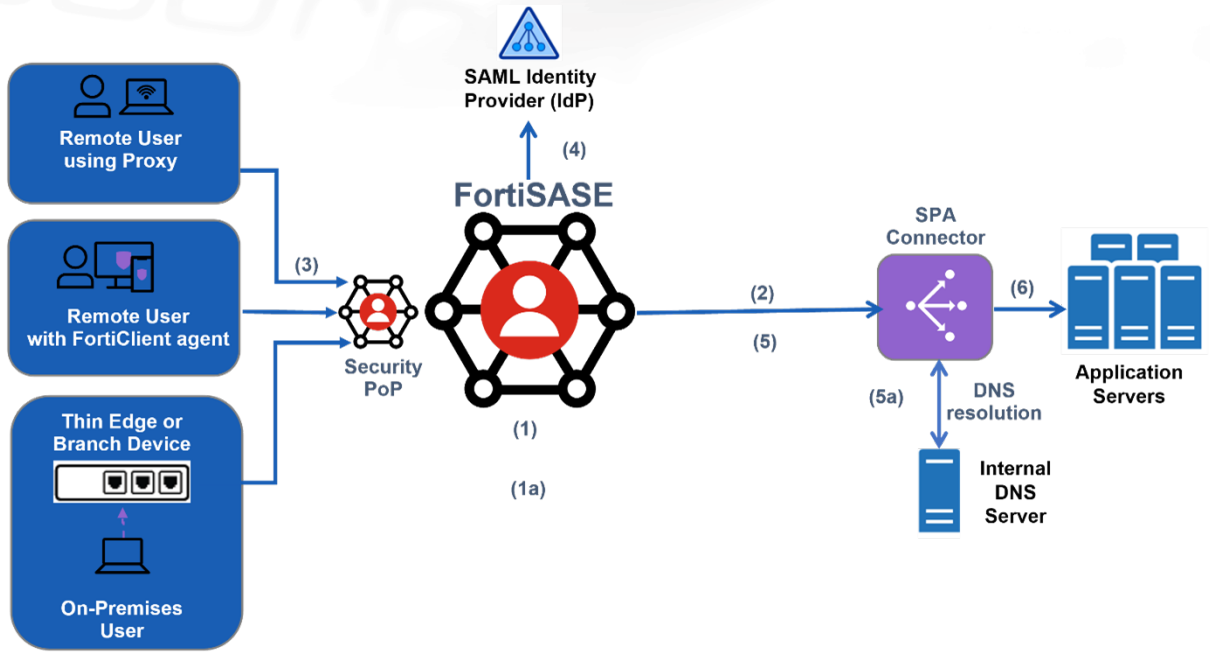
SPA use case	Description	Recommended Architecture
Agent access to private applications using the IP address or domain name and security posture tags on page 14	Remote users on supported endpoint devices use FortiClient software to steer traffic to a FortiSASE security PoP and then steer private traffic to the on-prem network over the IPsec tunnel between the FortiSASE security PoP and the SPA Connector.	FortiClient with SPA Connector

SPA use case	Description	Recommended Architecture
Agentless access to private web applications using Proxy for remote users where the installation of FortiClient is not possible on page 16	Remote users with web browsers supporting Proxy (formerly Secure Web Gateway or SWG) to steer web traffic to a FortiSASE security PoP and then steer private traffic to the on-prem network over the IPsec tunnel between the FortiSASE security PoP and the SPA Connector.	Proxy with SPA Connector
Agentless access to private web applications using a bookmark portal for unmanaged devices on page 17	Contractors or temporary remote users use browser-only solutions to access private web-based applications from a protected bookmark portal.	Agentless ZTNA with SPA Connector
Access to private applications using the application IP or DNS redirection from on-premise users and devices where installation of FortiClient is not feasible on page 19	Branch offices use a Thin Edge device including FortiAP, FortiExtender, or FortiBranchSASE, or a branch device including a FortiGate Secure Edge device or a Branch On-Ramp device to securely access private applications.	Thin Edge or Branch device with SPA Connector, with or without DNS redirection
Server-to-Client application access on page 22	Private application servers securely access remote user endpoints running FortiClient software.	SPA Connector with Server-to-Client policies
Client-to-Client application access on page 24	Remote user endpoints running FortiClient software securely access similar remote user endpoints.	SPA Connector with Client-to-Client policies

Client-initiated use cases

Most private access applications involve steering application traffic from a client to a server. With FortiSASE, the client is typically either a FortiSASEremote user with a FortiClient agent installed or an on-premises user whose traffic is steered to FortiSASE. Moreover, the server is typically a private application server reachable from an SPA Connector in either a data center, private cloud, or public cloud tenant.

The common SPA client-initiated use cases are described below.



The overall configuration and traffic flow are as follows:

1. Configure FortiSASE to connect to the SPA Connector and to allow client-to-server traffic using a private access policy.
   a. If required, configure one or more DNS redirection rules to redirect DNS requests from the FortiSASE DNS server to use the internal DNS server. The internal DNS server requires either Layer 2 or Layer 3 reachability from the SPA connector.
2. FortiSASE establishes a connection with the SPA Connector. Private application servers are now accessible by FortiSASE remote users or branch users.
3. Initiate Agent, Agentless (Proxy or Bookmark Portal), Thin Edge, or Branch connection with the FortiSASE Security PoP.
4. Authenticate using SAML IdP and upon successful authentication, establish connection with the FortiSASE Security PoP.
5. FortiSASE steers any remote user or branch user traffic destined for the private application, specifically, to the SPA Connector.
   a. If configured, a DNS redirection rule for the internal domain or internal hostname redirects the request to resolve the internal hostname of the private application server using the configured internal DNS server in the rule.
6. The SPA Connector steers traffic to the private application server. The private application server processes the request traffic and sends the response traffic back to the remote user or branch user.

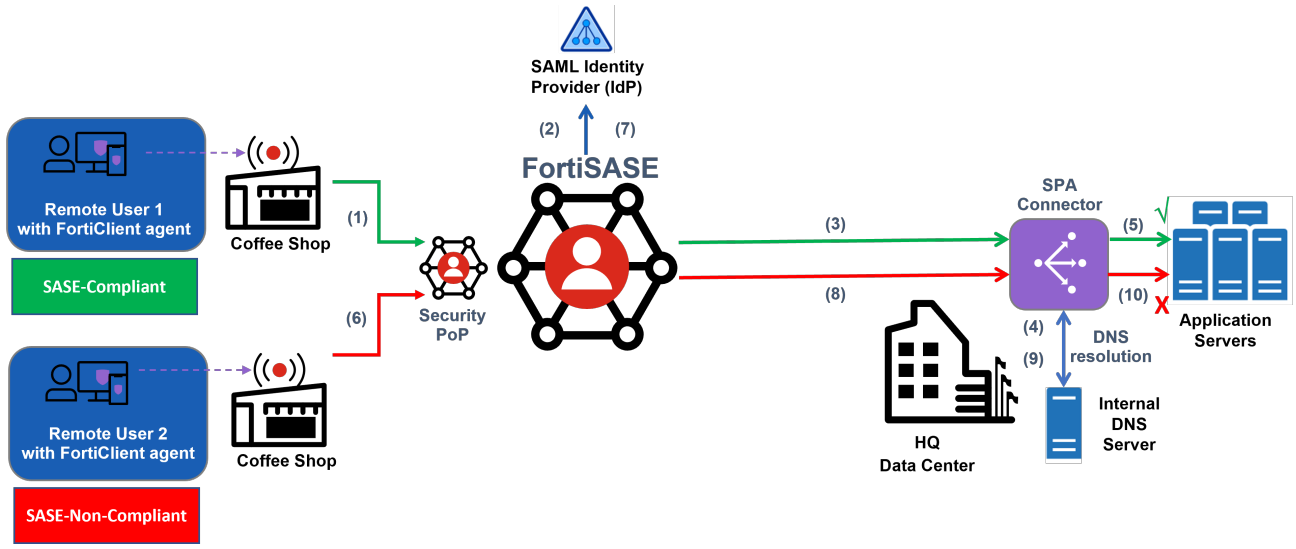
Agent access to private applications using the IP address or domain name and security posture tags

In this use case, remote users with FortiClient agent software installed initiate access to private applications using their application IP addresses, which are private IP addresses.

Alternatively, in this use case, remote agent users can access private applications using their internal hostnames, which require DNS redirection and resolution using an internal DNS server.

- Using FortiClient, the endpoint security posture is continuously evaluated and identified using a security posture tag to represent this posture.
- Security posture tags are used with private access policies to control access to private applications.
- Private access policies can be generalized or granular depending on your requirements.

In the example below, the *SASE-Compliant* security posture tag is used to represent endpoints whose security posture is deemed to be compliant with your requirements. Endpoints tagged as *SASE-Compliant* are allowed access to application servers. In contrast, the *SASE-Non-Compliant* tag is used to represent endpoints whose security posture is deemed to be non-compliant with your requirements. Endpoints tagged as *SASE-Non-Compliant* are denied access to application servers.



Traffic flow

The traffic flow for this use case is as follows:

1. Remote User 1 initiates an Agent connection with the FortiSASE Security PoP.
2. Remote User 1 authenticates using SAML IdP and upon successful authentication, establishes a tunnel with the FortiSASE Security PoP.
3. Remote User 1 sends request traffic destined for the private application and FortiSASE steers the traffic to the SPA Connector.
4. *For domain name variation of use case*: FortiSASE uses a DNS redirection rule to direct the DNS resolution of the internal hostname to the internal DNS server that is reachable from the SPA Connector.
5. FortiSASE evaluates the security posture tag.
   a. Since the security posture tag for the endpoint is *SASE-Compliant*, it is authorized to access the private application server. FortiSASE steers traffic to the private application server.

   b. The private application server processes the request traffic and sends the response traffic back to Remote User 1.
6. Remote User 2 initiates an Agent connection with the FortiSASE Security PoP.
7. Remote User 2 authenticates using SAML IdP and upon successful authentication, establishes a tunnel with the FortiSASE Security PoP.
8. Remote User 2 sends request traffic destined for the private application and FortiSASE steers the traffic to the SPA Connector.
9. *For domain name variation of use case*: FortiSASE uses a DNS redirection rule to direct the DNS resolution of the internal hostname to the internal DNS server that is reachable from the SPA Connector.
10. FortiSASE evaluates the security posture tag.
    a. Since the security posture tag for the endpoint is *SASE-Non-Compliant*, it is not authorized to access the private application server. FortiSASE drops traffic.
    b. The private application server does not receive the request traffic and the Remote User 2 application times out.

Appropriate use

FortiClient can be installed on endpoints.

Private application access involves any protocol including HTTPS.

It is sufficient for the client to access the private application using its private IP address only.

For domain name variation of use case:

- Private application access works with internal hostnames resolved by an internal DNS server.
- An internal DNS server is configured and is accessible from the SPA Connector through Layer 2 or Layer 3.

Prerequisites

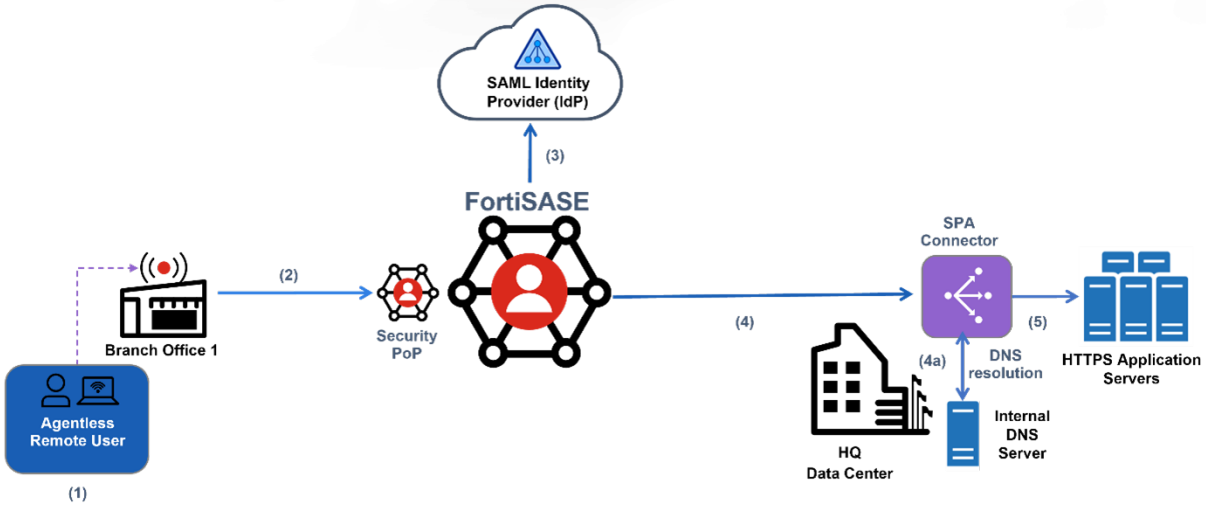
- See FortiSASE Ordering Guide for licensing details:
  - FortiSASE per-user licensing includes up to 3 devices per user and be a combination of FortiClient and Proxy devices.
  - Each SPA Connector requires a separate FortiSASE subscription license.
- Endpoints must be running on platforms supported by FortiSASE and the FortiClient agent, namely, Windows or MacOS.

Considerations

- FortiClient blocks IPv6 traffic. Only IPv4 traffic traverses through the FortiSASE tunnel.
- Using alternate VPN clients in combination with FortiSASE is not recommended nor supported.

Agentless access to private web applications using Proxy for remote users where the installation of FortiClient is not possible

In this use case, remote users with web browsers supporting Proxy (formerly Secure Web Gateway or SWG) to steer web traffic to a FortiSASE security PoP and then steer private traffic to the on-prem network over the IPsec tunnel between the FortiSASE security PoP and the SPA Connector. Applications are accessed through either private IP addresses or domain names when DNS redirection is used.



Traffic flow

The traffic flow for this use case is as follows:

1. The agentless remote user uses their web browser to access a private resource via HTTP or HTTPS using a private IP address.
   a. *For domain name variation of use case*: The agentless remote user uses their web browser to access a private resource via HTTP or HTTPS using a private domain name.
2. The web browser request is sent to FortiSASE.
3. FortiSASE prompts the remote user to authenticate with the SAML IdP. Remote users can only access web resources after successfully authenticating.
4. FortiSASE steers the HTTPS request to the SPA Connector.
5. *For domain name variation of use case*: If the private application is configured using an internal hostname, FortiSASE uses a DNS redirection rule to direct the DNS resolution of the internal hostname to the internal DNS server that is reachable from the SPA Connector.
6. The SPA Connector steers the HTTPS request to the corresponding private application server and the HTTPS response is sent back to the remote user.

Appropriate use

- Installation of FortiClient is not possible on endpoints
- Endpoints support web proxy configuration via system or web browser

- Private application access involves only web protocols including HTTP and HTTPS.
- *For domain name variation of use case*:
  - Private application access works with internal hostnames resolved by an internal DNS server.
  - An internal DNS server is configured and is accessible from the SPA Connector via Layer 2 or Layer 3.

Prerequisites

- See FortiSASE Ordering Guide for licensing details:
  - FortiSASE per-user licensing includes up to 3 devices per user and be a combination of FortiClient and Proxy devices.
  - Each SPA Connector requires a separate FortiSASE subscription license.

Considerations

- See Proxy client onboarding and Feature SIA Agentless Proxy Deployment Guide for proxy deployment details.

Agentless access to private web applications using a bookmark portal for unmanaged devices

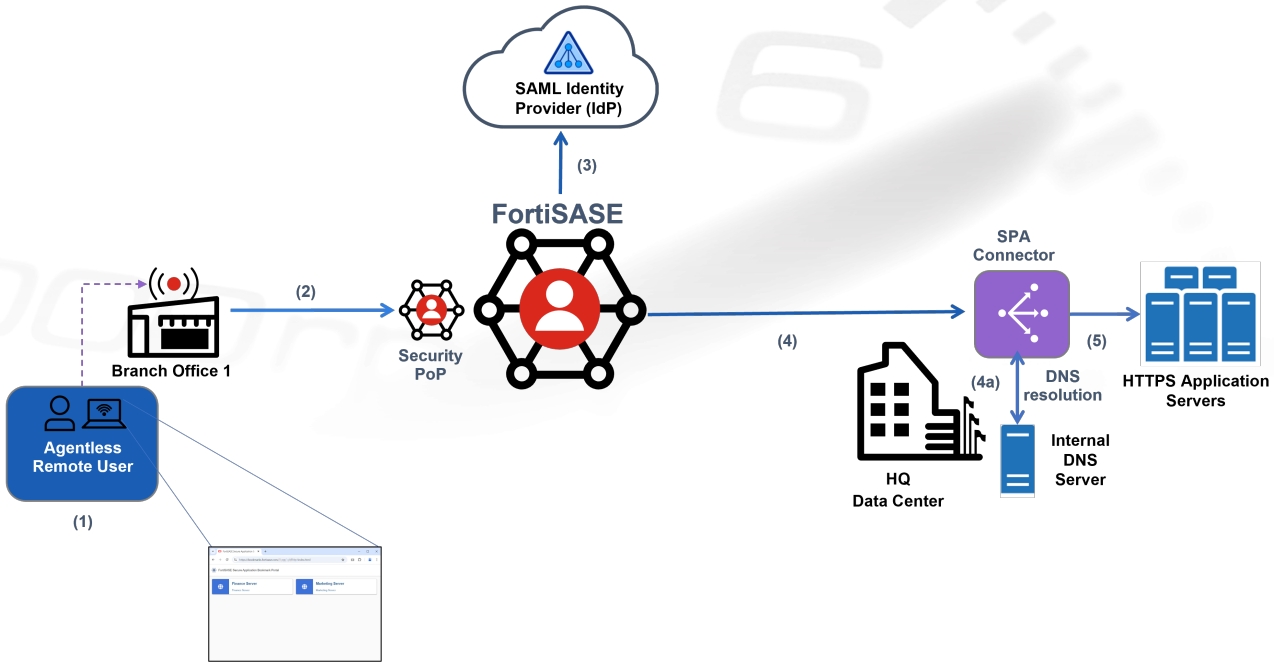
FortiSASE supports agentless ZTNA, which allows contractors or temporary remote users to access a private web-based application behind an SPA Connector without requiring an agent, simply by using a web browser.

- FortiSASE provides an agentless ZTNA bookmark portal that you can share with contractors or temporary remote users to make it convenient for them to access private applications using agentless ZTNA.
- A private application is configured with either the private IP address or the internal hostname of the private application server. The internal hostname must be resolvable by an internal DNS server accessible by the SPA Connector.
- Each web-based application is assigned to a unique public URL using the custom public domain name associated with the FortiSASE instance so that you do not have to maintain a separate set of domain names dedicated to private web applications.

FortiSASE functions as a HTTPS reverse proxy on behalf of the private web-based applications it is protecting. Before granting access to the protected application, FortiSASE verifies:

- User identity by enforcing user authentication to a SAML IdP from within the remote user's web browser.
- Geolocation of the remote user by using geofencing.

Based on the application policy configured, FortiSASE grants access accordingly. FortiSASE provides seamless access to private applications through the unique public URL.



Traffic flow

The traffic flow for this use case is as follows:

1. The agentless remote user uses their web browser to access the bookmark portal.
2. The web browser request is sent to FortiSASE.
3. FortiSASE prompts the remote user to authenticate with the SAML IdP. Remote users can only access the bookmark portal after successfully authenticating.
4. The remote user clicks on the bookmark of the private application they would like to access. Using the unique public URL, FortiSASE steers the HTTPS request to the SPA Connector.
   a. If the private application is configured using an internal hostname, FortiSASE uses a DNS redirection rule to direct the DNS resolution of the internal hostname to the internal DNS server that is reachable from the SPA Connector.
5. The SPA Connector steers the HTTPS request to the corresponding private application server and the HTTPS response is sent back to the remote user.

Appropriate use

- Suitable for unmanaged Web browser-based solutions and remote user interaction to navigate through bookmark portal.
- Private application access is only via HTTPS.
- Private application access works with either private IP addresses or internal hostnames resolved by an internal DNS server
  - To resolve internal hostnames, an internal DNS server is configured and is accessible from the SPA Connector via Layer 2 or Layer 3

Prerequisites

- See FortiSASE Ordering Guide for licensing details:
  - FortiSASE per-user licensing includes up to 3 devices per user and be a combination of FortiClient and Proxy devices.
  - Each SPA Connector requires a separate FortiSASE subscription license.
  - Agentless ZTNA requires a FortiSASE Advanced, Professional, or Comprehensive license.
- Endpoints must be running on platforms supported by FortiSASE and the FortiClient agent, namely, Windows or MacOS.

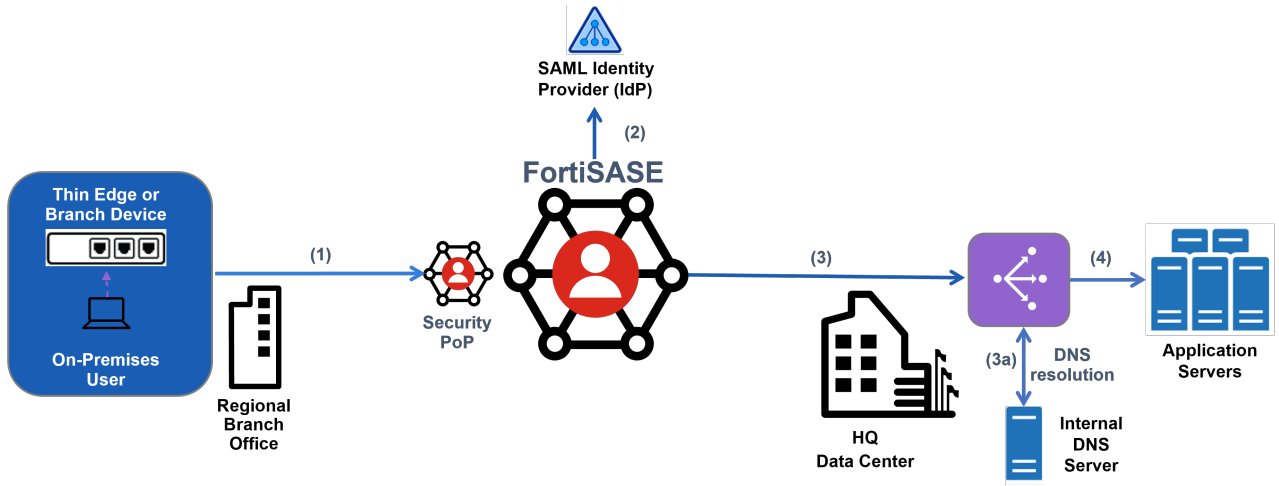
Considerations

- FortiClient blocks IPv6 traffic. Only IPv4 traffic traverses through the FortiSASE tunnel.
- Using alternate VPN clients in combination with FortiSASE is not recommended nor supported.

Access to private applications using the application IP or DNS redirection from on-premise users and devices where installation of FortiClient is not feasible

In this use case, on-premises users at branch offices are connected to a Thin Edge device (FortiExtender/FortiBranchSASE, FortiAP) or a Branch device (FortiGate Secure Edge, FortiGate or third-party IPsec device for Branch On-Ramp). These users access private applications using either their application IP addresses, which are private IP addresses, or their internal hostnames resolved using DNS redirection rules with internal DNS servers.

- A captive portal is used with a SAML IdP to provide authentication to on-premises users.
- On-premises users require direct Layer 2 or indirect Layer 3 access to the Thin Edge or Branch device.
- This use case is best for devices including servers and IOT without web browsing capabilities or where installation of FortiClient is not feasible.



Traffic flow

For this use case, the traffic flow is as follows:

1. The Thin Edge or Branch device establishes a tunnel connection with the FortiSASE Security PoP.
2. The on-premises user is presented with a captive portal and authenticates using SAML IdP. Upon successful authentication, a user session is established with the FortiSASE Security PoP.
3. FortiSASE steers any Thin Edge or Branch user traffic destined for the private application, specifically, to the SPA Connector.
   a. If configured, a DNS redirection rule for the internal domain or internal hostname redirects the request to resolve the internal hostname of the private application server using the configured internal DNS server in the rule.
4. The SPA Connector steers traffic to the private application server. The private application server processes the request traffic and sends the response traffic back to the Thin Edge or Branch user.

Appropriate use

Devices where installation of FortiClient is not feasible and require private traffic to be steered to FortiSASE.

Private application access involves any protocol including HTTPS

Private application access works with either private IP addresses or internal hostnames resolved by an internal DNS server

To resolve internal hostnames, an internal DNS server is configured and is accessible from the SPA Connector via Layer 2 or Layer 3

Prerequisites

- See FortiSASE Ordering Guide for licensing details:
  - FortiSASE per-user licensing includes up to 3 devices per user and be a combination of FortiClient and Proxy devices.
  - Each SPA Connector requires a separate FortiSASE subscription license.
  - Each Thin Edge device requires a separate FortiSASE subscription license.
  - Branch On-Ramp enables customers to connect FortiGate or third-party IPsec devices for connectivity to FortiSASE.
    - IPsec service connections require the FortiSASE instance to have these licenses applied:
      - Advanced or Comprehensive license
      - Branch On-Ramp Location subscription license corresponding to the Advanced or Comprehensive license

Considerations

- FortiSASE supports a maximum of 1024 FortiExtender devices combined that you can configure as FortiSASE edge devices.
- FortiSASE supports a maximum of 240 FortiAP devices that you can configure as FortiSASE edge devices.
- FortiAP devices can be connected to FortiSASE using FortiZTP.
- FortiSASE supports a maximum of 16 FortiGate and FortiWiFi devices combined that you can configure as FortiSASE edge devices.

- Multiple branch devices can establish IPsec connections with the Branch On-Ramp location and number of IPsec connections can be increased through add-on licensing.
  - A maximum of 20 On-Ramp locations are supported by FortiSASE in the cloud.
    - Each location supports 1 Gbps of shared bandwidth.
    - Each location can have a maximum of 2000 tunnels.

Additional configurations

Pre-logon connectivity

Pre-logon connectivity is typically useful to onboard remote users who have never logged in to their Windows machines, where the user's Windows machines are domain-joined to their organizational Active Directory (AD) environment.

Initial user login to domain-joined Windows machines using user AD credentials requires real-time connectivity to the AD server. You can provide connectivity to the AD server via pre-logon tunnels.

This initial onboarding workflow is as follows:

1. Upon bootup, using a pre-logon tunnel, a Windows machine self-authenticates and connects to a gateway using its machine certificates.
2. Once Windows machines establish pre-logon tunnels, they can access the AD server.
3. Users can then log in to the Windows machine using their AD credentials.
4. After login to the Windows machine, the pre-logon tunnel connection disconnects.
5. Users then can connect to FortiSASE automatically or manually depending on FortiSASE endpoint management configuration.
6. For subsequent user logins to Windows machines, users can then use their locally cached Windows AD credentials.
7. Windows administrators must have already staged the domain-joined Windows machines with a preconfigured FortiClient installer with the proper supported FortiClient version, along with machine certificates before shipping devices to users.

Autoconnect tunnel connectivity

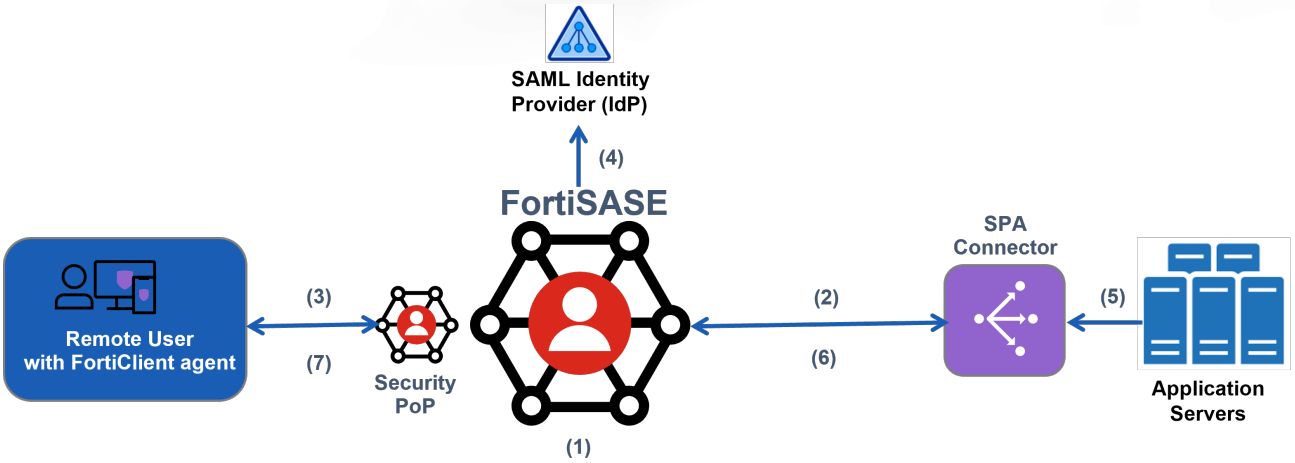
To ensure agent tunnel connectivity without the remote user having to manually enter their credentials, FortiSASE relies on various autoconnect mechanisms:

- Agent tunnels using OAuth
  - OAuth support is currently limited to remote users using SSL-based tunnels.
  - OAuth support is currently limited to Entra ID as the IdP and Windows endpoints installed with FortiClient agent software.
- In the endpoint profile when the endpoint is configured to automatically connect to the Security PoP, the remember password feature along with autoconnect and always-up features are enabled.
  - When using SAML authentication, the remember password feature relies on persistent sessions being configured in the IdP.
  - If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each tunnel connection attempt.

Server-initiated use cases

Some private applications require traffic to be initiated by servers and destined for clients. With FortiSASE, servers refer to private application servers reachable using the SPA Connector. Remote users with the FortiClient agent installed are supported as clients reachable by private application servers.

- Server-initiated use cases include client-to-client traffic such as for SIP applications, or server-to-client traffic such as remote desktop and device management applications.
- Server-initiated use cases support using the private IP addresses of agent remote users.

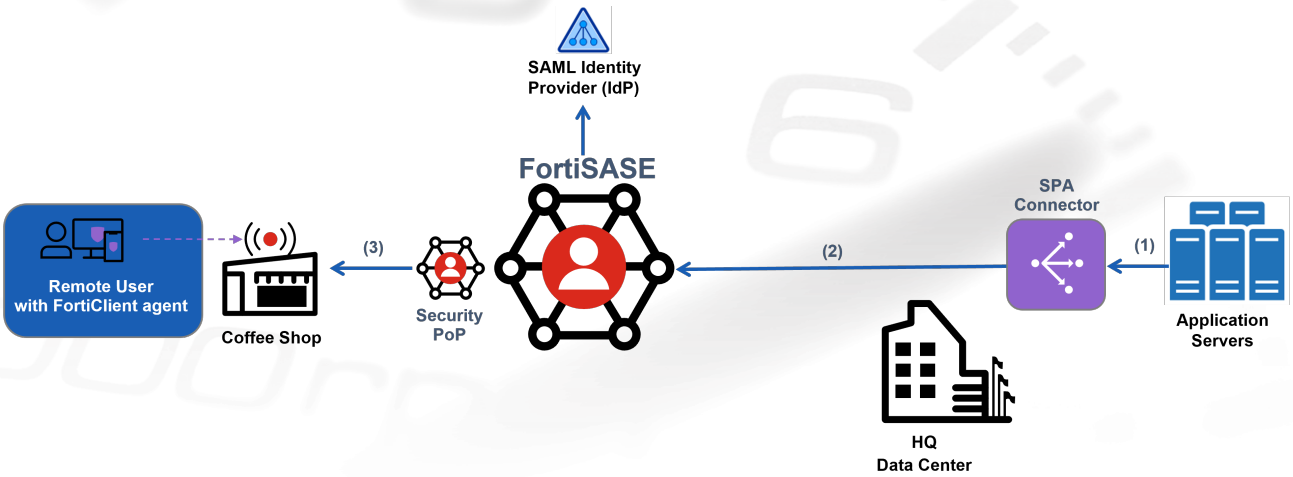


The overall configuration and traffic flow are as follows:

1. Configure FortiSASE to connect to the SPA Connector and to allow server-to-client communication using a private access policy.
2. FortiSASE establishes a connection with the SPA Connector. Private application servers are now accessible by FortiSASE remote users. FortiSASE remote users are now accessible by private application servers.
3. Initiate the Agent connection with the FortiSASE Security PoP.
4. Authenticate using SAML IdP and upon successful authentication, establish connection with the FortiSASE Security PoP.
5. The private application server initiates a request destined for a remote user using its private IP address.
6. The SPA Connector steers the request destined for the remote user to FortiSASE
7. FortiSASE steers traffic to the remote user. The remote user processes the request traffic and sends the response traffic back to the private application server.

Server-to-Client application access

In this use case, a private application server requires access to a remote user with the FortiClient agent. This use case is commonly used for remote desktop and device management applications.



Traffic flow

For this use case, we consider that these conditions have already been met:

- The remote user with FortiClient agent has successfully authenticated and established a connection with a FortiSASE Security PoP.
- FortiSASE has established a connection with the SPA Connector.

In this use case, the traffic flow occurs as follows:

1. The private application server initiates a request destined for a remote user using its private IP address.
2. The SPA Connector steers the request destined for the remote user to FortiSASE
3. FortiSASE steers traffic to the remote user. The remote user processes the request traffic and sends the response traffic back to the private application server.

Appropriate use

- FortiClient can be installed on endpoints.
- Access between private application server and remote user involves any protocol including HTTPS.
- It is sufficient for the client to access the private application using its private IP address only.

Prerequisites

- See FortiSASE Ordering Guide for licensing details:
  - FortiSASE per-user licensing includes up to 3 devices per user and be a combination of FortiClient and Proxy devices.
  - Each SPA Connector requires a separate FortiSASE subscription license.
- Endpoints must be running on platforms supported by FortiSASE and the FortiClient agent, namely, Windows or MacOS.

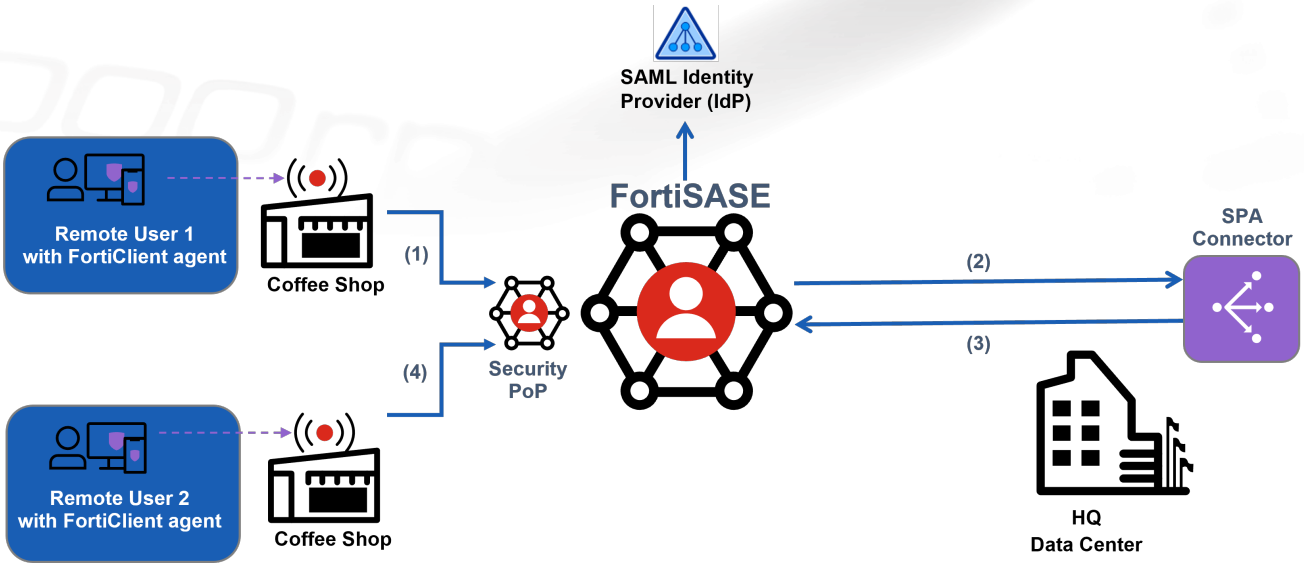
Considerations

- FortiClient blocks IPv6 traffic. Only IPv4 traffic traverses through the FortiSASE tunnel.
- Using alternate VPN clients in combination with FortiSASE is not recommended nor supported.

Client-to-Client application access

Traffic can travel directly between endpoints by traversing the SPA Connector.

All Security PoPs establish connections with the SPA Connector. By having client-to-client traffic traverse the SPA Connector, connectivity is ensured, regardless of the Security PoP that each remote user is connected to.



Traffic flow

For this use case, we consider that these conditions have already been met:

- The remote user with FortiClient agent has successfully authenticated and established a connection with a FortiSASE Security PoP.
- FortiSASE has established a connection with the SPA Connector.

In this use case, the traffic flow occurs as follows:

1. Remote User 1 sends a request destined for Remote User 2. Since all traffic is steered to FortiSASE, this request is also steered to FortiSASE.
2. FortiSASE steers the Remote User 1 traffic to the SPA Connector.
3. The SPA Connector determines the Remote User 1 traffic destination is not for one of its local subnets and steers the remote user traffic back to FortiSASE.
4. FortiSASE steers the Remote User 1 traffic to Remote User 2, which processes the request traffic and sends the response traffic back to Remote User 1 using the same path in the opposite direction.

Appropriate use

- FortiClient can be installed on endpoints.
- Access between private application server and remote user involves any protocol including HTTPS.
- It is sufficient for a client to access another client using its private IP address only.

Prerequisites

- See FortiSASE Ordering Guide for licensing details:
  - FortiSASE per-user licensing includes up to 3 devices per user and be a combination of FortiClient and Proxy devices.
  - Each SPA Connector requires a separate FortiSASE subscription license.
- Endpoints must be running on platforms supported by FortiSASE and the FortiClient agent, namely, Windows or MacOS.
- Additional configuration is required on the SPA Connector to ensure proper steering between clients and to resolve any conflicts between FortiSASE remote user subnets and SPA Connector local subnets.

Considerations

- FortiClient blocks IPv6 traffic. Only IPv4 traffic traverses through the FortiSASE tunnel.
- Using alternate VPN clients in combination with FortiSASE is not recommended nor supported.

More information

4-D (Define, Design, Deploy, Demo) documentation

- 4-D Resources: Secure Access Service Edge
- 4-D FortiSASE Concept Guide
- 4-D FortiSASE Secure Internet Access Architecture Guide
- 4-D FortiSASE Feature SPA Deployment Guide using BGP per Overlay

Change log

Date	Change description
2026-03-13	Initial release.

www.fortinet.com

72-261-1131306-20250313