Architecture Guide

FortiSASE

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Common FortiSASE use cases

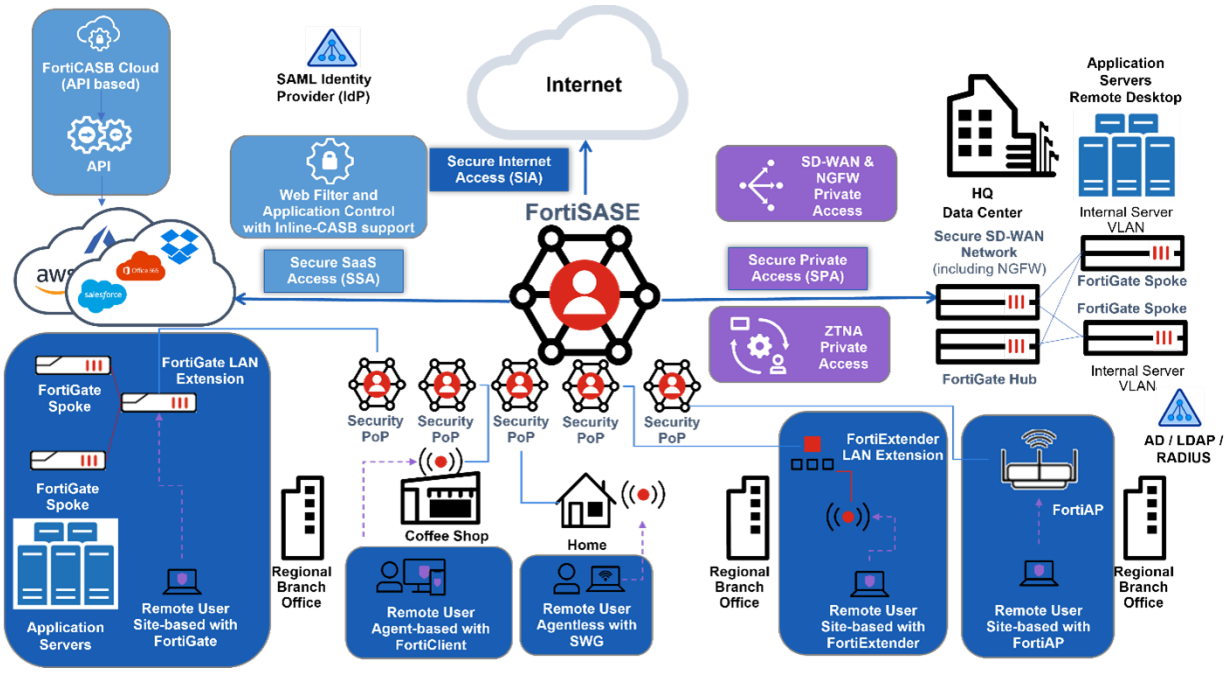
With FortiSASE, remote users (agent-based, agentless, and site-based) form secure connections to the Internet, data center, and cloud by accessing global FortiSASE security points of presence, which enforce an organization's security policies regardless of remote users' locations.

Following are examples of common FortiSASE use cases:

FortiSASE component	Use case	Description
Secure Internet access (SIA)	Agent-based remote user Internet access	Secure access to the Internet using FortiClient agent
	Agentless remote user Internet access	Secure access to the Internet using FortiSASE secure web gateway (SWG)
	Site-based remote user Internet access using FortiExtender	Secure access to the Internet using FortiExtender device as FortiSASE LAN extension
	Site-based remote user Internet access using FortiAP	Secure access to the Internet using FortiAP edge device that FortiSASE manages

FortiSASE component	Use case	Description
Secure private access (SPA)	Zero trust network access (ZTNA) private access	Access to private company-hosted TCP-based applications behind the FortiGate ZTNA application gateway for various ZTNA use cases. This access method allows for a direct (shortest) path to private resources.
	SD-WAN private access	Access to private company-hosted applications behind the FortiGate SD-WAN hub-and-spoke network. This access method extends private access for TCP- and UDP-based applications and offers data center redundancy.
	Next generation firewall (NGFW) private access	Access to private company-hosted applications behind the FortiGate NGFW. This use case extends private access for UDP-based applications and agentless remote users.
Secure SaaS access	FortiCASB SaaS access	Access to SaaS applications using FortiCASB Cloud/API
	FortiSASE Inline-CASB	Access control to SaaS applications using FortiSASE inline-CASB and SSL deep inspection on endpoint
SIA and SPA	Site-based remote users using FortiGate SD-WAN as a secure edge	Secure access to the Internet using FortiGate as FortiSASE LAN extension

Following is an example architecture of FortiSASE that incorporates all mentioned use cases:



Audience

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

About this guide

The guide is meant to provide high level insight into FortiSASE architectures for different secure access service edge use cases. You are meant to use this guide in conjunction with other technical documentation for each component that the guide lists. Where relevant, the guide lists links to the administrative guides and other technical reference guides. See More information on page 34.

For comments and feedback about this document, visit the SASE Architecture Guide for Enterprise on community.fortinet.com.

Technology used

The secure access service edge (SASE) architecture focuses on using a cloud-delivered security service that enforces secure access at the farthest edge of the network, namely, at the service edge or user endpoints. When connected to FortiSASE, remote users' traffic to the Internet, software-as-a-service (SaaS) applications, or privately hosted applications in the data center pass through a firewall-as-a-service (FWaaS) or secure web gateway (SWG) where the traffic is subject to security policies and advanced threat protection measures. For traffic redirection, remote users' endpoints rely on a software agent, remote users behind sites rely on a thin edge device, and remote users with web browser-based devices are agentless and rely on web browser proxy settings.

FortiSASE is a cloud-delivered security service that implements the described SASE architecture. The FortiSASE solution is comprised of the following features powered by FortiOS and the Fortinet Security Fabric:

- FWaaS functionality based on FortiOS Next-Generation Firewall (NGFW) features
- SWG functionality based on FortiOS explicit web proxy, captive portal, and authentication features
- FortiGuard Labs threat intelligence used by the FWaaS and the SWG
- Global Security Points of Presence (PoPs) to provide access to remote users
- Endpoint Management Service based on FortiClient EMS

Depending on the customer remote user devices and requirements, one or more of the following are required for Secure Internet Access (SIA) use cases:

- Agent-based: FortiClient software for Endpoint mode
- Agentless: Web browser-based device, low-end device, or operational technology device with support for explicit web proxy settings for SWG mode
- Site-based:
  - FortiExtender thin edge device configured for LAN extension mode
  - FortiGate device configured for LAN extension mode
  - FortiAP device configured with CAPWAP and data channel encrypted with an IPsec VPN tunnel

For ZTNA Secure Private Access (SPA) use cases involving TCP-based applications, the following components are required:

- FortiGate Next-Generation Firewall (NGFW) configured with:
  - FortiClient Cloud fabric connector
  - ZTNA access proxy
- FortiClient Agent-Based software for TCP access proxy redirection

ZTNA is limited to TCP-based applications because the FortiGate ZTNA access proxy relies on proxying connections, namely those supported by HTTP or other TCP traffic, over secure HTTPS connections with the client. Since UDP traffic is connectionless then it cannot be proxied. In addition, the FortiClient agent-based software is a requirement for ZTNA since it provides device information, user information, and security posture to FortiSASE, maintains ZTNA tags, and maintains a client certificate used for identification by the FortiGate ZTNA access proxy.

Therefore, because of the requirements to proxy TCP traffic and have FortiClient installed on endpoints, the ZTNA use case cannot be used with UDP-based applications and agentless remote users.

For SD-WAN and NGFW SPA use cases that allow seamless access to every private application (TCP and UDP), one of the following components is required:

- Existing FortiGate SD-WAN hub-and-spoke network configured using one of the SD-WAN best practice setups
- FortiGate NGFW configured as a new, standalone FortiSASE Secure Private Access (SPA) hub

For SSA use cases, FortiCASB provides cloud-based and API-based features to enable deep inspection of SaaS applications to enable detailed monitoring, analysis, and reporting features. Access to FortiCASB user-based SaaS security is included with FortiSASE per-user and per-endpoint licenses.

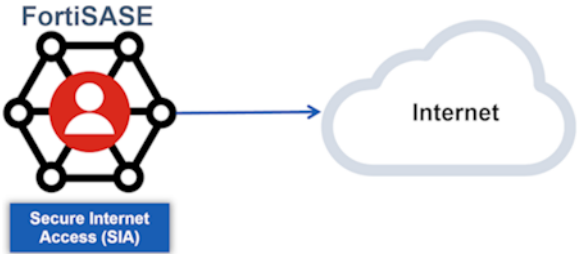
In addition, for an SSA use case, FortiSASE provides Inline-CASB functionality with web filter and application control security features. The FortiSASE Web Filter with Inline-CASB allows for restricted SaaS access from selected tenants by inspecting and modifying HTTP headers via HTTP header insertion. The FortiSASE Application Control with Inline-CASB allows for detection of SaaS application traffic and then the action of allowing, monitoring, or blocking the traffic because the CASB functionality is inline with the traffic.

Design overview

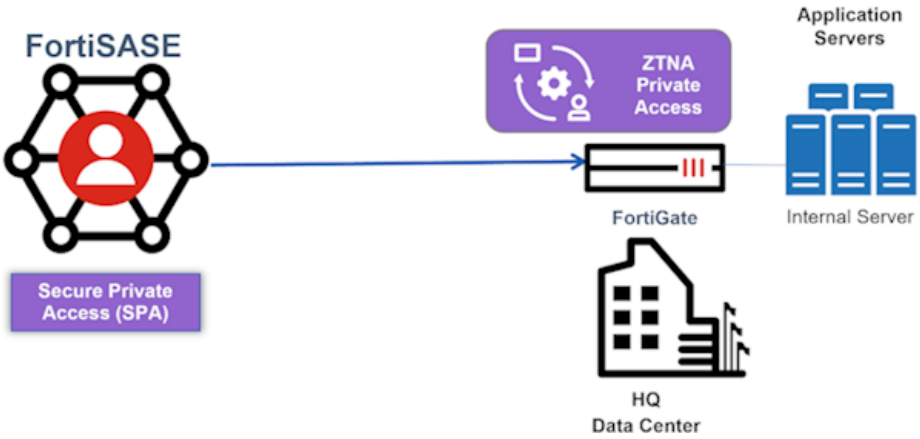
In this architecture, these are the goals for remote users that connect to FortiSASE:

- Enforce secure Internet access (SIA) when users access Internet and web-based applications
- Allow secure private access (SPA) when users access private company-hosted applications that a FortiGate next-generation firewall (NGFW) protects
- Enforce secure SaaS access (SSA) when users access SaaS applications

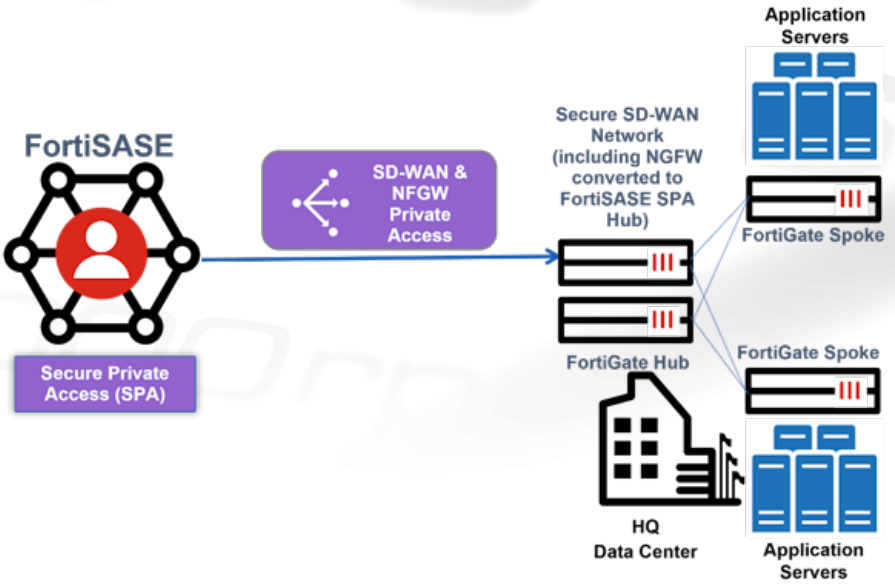
SIA extends an organization's security perimeter that an NGFW typically achieves to remote users by enforcing common security policy for Intrusion Prevention Systems and Application Control, Web and DNS filtering, and Anti-Malware, Sandboxing, and Anti-Botnet/Command and Control (C&C).



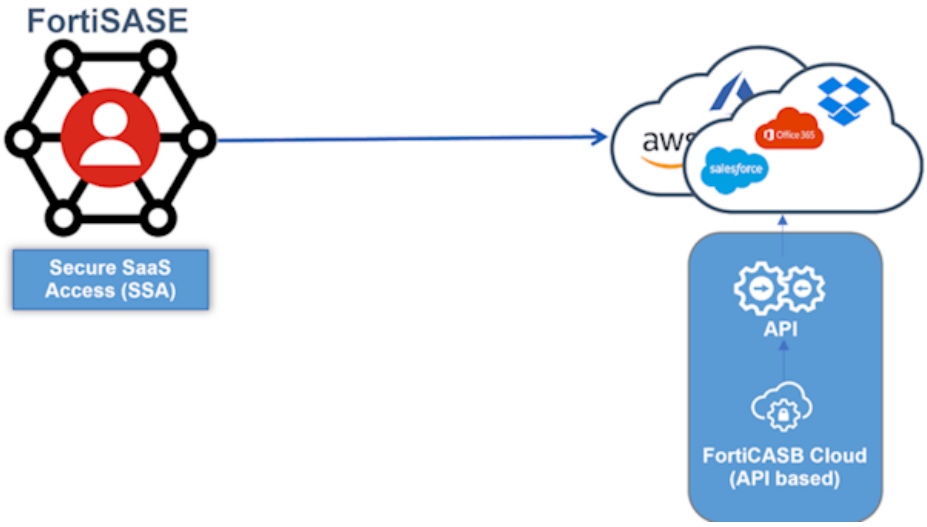
SPA using zero trust network access (ZTNA) secures private TCP-based applications, namely, leveraging FortiSASE integration with the FortiGate ZTNA access proxy. For a design overview specific to FortiGate ZTNA architecture, see the ZTNA Architecture Guide.



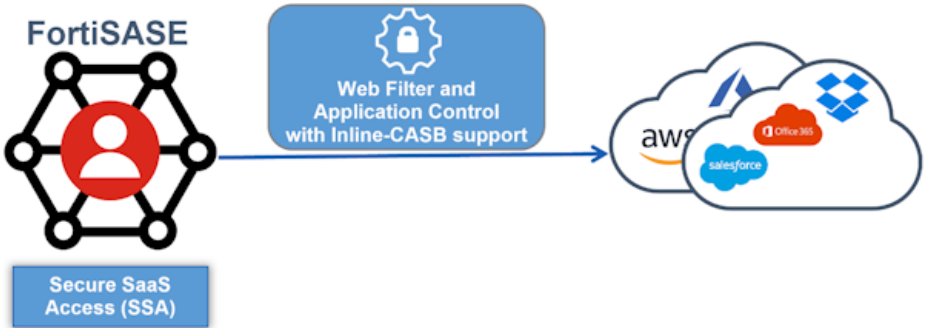
For securing private TCP-based and UDP-based applications, FortiSASE supports SPA using SD-WAN or SPA using an NGFW converted to a standalone FortiSASE SPA hub.



SSA uses FortiCASB for advanced API-based deep inspection of cloud activity to provide monitoring, analysis, and reporting features that alert network administrators of any suspicious user activity, threats, or security policy violations. Insights that FortiCASB determines can then be acted upon by network administrators to enhance FortiSASE security features and settings to block and mitigate such detected activity.



SSA can also use FortiSASE Inline-CASB functionality, which enforces security policies inline with the traffic used to access cloud applications. Therefore, unlike API-based CASB solutions, which rely on out-of-band traffic, using inline-CASB functionality, FortiSASE can block remote user access to cloud-based applications.



Design concept and considerations

All use cases related to each other

By default, all traffic from FortiSASE remote users is being tunneled to FortiSASE, which makes all the use cases (SIA, SPA, SSA) related to each other. Therefore, in most use cases, traffic must pass through FortiSASE before being destined for the Internet and private resources.

As exceptions, for ZTNA, traffic does not pass through FortiSASE. Instead, traffic is destined directly to private resources protected by the FortiGate ZTNA access proxy for ZTNA use cases.

Considerations for secure Internet access use cases

Consider the use case that your remote users will use to access FortiSASE and consider that this use case depends on the capabilities of their devices to support FortiClient agent-based software and web proxy settings. Also, consider whether you would like to distribute the capability of accessing FortiSASE on each device or if you would like to centralize this capability to a FortiExtender device.

The following table summarizes the characteristics of each SIA use case:

Secure Internet Access Use Case	Distributed or Centralized	Device Support	Protocol Support	Software required for automated configuration
Agent-based using FortiClient (Previously known as Endpoint Mode)	Distributed	Devices that support FortiClient agent-based software	All protocols	Mobile device management (MDM) tool
Agentless using Explicit Web Proxy Settings (Previously known as SWG mode)	Distributed	Devices that support web browser with web proxy functionality	HTTP/HTTPS only	Windows Group Policy Objects (GPOs) or Microsoft System Center Configuration Manager (SCCM)
Site-based using FortiExtender (previously known as Thin Edge mode) or FortiGate	Centralized	All devices	All protocols	None. Requires configuration of FortiExtender or FortiGate and FortiSASE

Depending on your user requirements, the SIA use cases can be used in isolation or combined. Typically, for simplicity in design, deployment, and maintenance, each group of users with similar endpoint devices would be covered by a single SIA use case.

The main components used to support each SIA use case are found within the FortiSASE platform itself. Therefore, any supporting remote user access functionality is enabled on FortiSASE with the appropriate licensing and corresponding configuration achieved using the FortiSASE GUI. In addition, bandwidth usage for remote users is not unlimited on FortiSASE, so this requirement must also be taken into consideration when considering bandwidth licensing. See the FortiSASE Ordering Guide for licensing details.

Selecting security PoPs and analytics PoP

Initializing FortiSASE prompts you to select multiple security points-of-presence (PoPs) that your remote users will use to access FortiSASE and a single Analytics PoP that FortiSASE will use for log storage.

Consider the geographical locations of all your remote users and select PoPs that are near to your remote users and that would also provide adequate coverage for remote users who may travel or work outside of the central locations of your organization.

For organizations with log storage privacy/compliance requirements such as GDPR, ensure that you choose the log storage location that allows your organization to meet such requirements.

Design components

Consider the components of a SASE solution and align them to the existing network and security infrastructure. Review any changes that may be necessary to prepare for the SASE implementation.

SASE Component	Existing infrastructure
Secure Internet Access	Ensure endpoints (agent-based, agentless remote users) and FortiExtender devices (site-based remote users) can access the Security PoPs from everywhere. Consider the bandwidth requirements of the remote users and their applications and obtain the corresponding bandwidth licensing. The remote user connectivity methods used by the SIA use cases are also used by the SPA use cases and the SSA use cases.
Security and Analytics PoPs	Consider selecting Security PoPs that are geographically near to your remote users. Review log storage privacy requirements (such as GDPR) and consider choosing the log storage location or Analytics PoP that meets these requirements.
Remote Authentication Source	Consider the type of remote authentication source (LDAP, RADIUS, or SAML Identity Providers such as Azure AD or Okta) that you will use to control network access for devices and users on your network. When SAML identity providers (IdPs) are involved, FortiSASE will act as a service provider (SP). Ensure that appropriate users and groups are created in the remote authentication source that align with your security goals. Authentication can be applied to FortiClient agent-based and SWG agentless access.
Security Profiles	Consider the security features that will extend the enterprise security perimeter for remote users including IPS and Application Control, Web and DNS filtering, anti-malware, sandboxing, anti-botnet/command-and-control. Consider the specific settings within the security features that are sufficient to secure your remote users.
VPN Policies	Consider the common security policy used to extend the enterprise security perimeter for agent-based remote users and site-based remote users. Consider which specific security features and user groups you will configure in individual policies.

SASE Component	Existing infrastructure
SWG Policies	Consider the common security policy used to extend the enterprise security perimeter for agentless remote users. Consider which specific security features and user groups you will configure in individual policies.
Secure Private Access	For private access to TCP-based applications consider deploying the ZTNA use case. Ensure that the ZTNA design components (FortiClient, FortiClient EMS, FortiOS ZTNA access proxy, SAML IdPs) and their requirements are considered. See the ZTNA Architecture Guide for details. For broader and seamless access to every private application (TCP and UDP), consider deploying the SD-WAN and NGFW SPA use cases. Ensure that the SD-WAN hubs are remotely accessible for SD-WAN overlay interconnectivity with FortiSASE PoPs.
Secure SaaS Access	For FortiCASB use cases, ensure that you have purchased the proper per-user and per-endpoint FortiSASE licensing to obtain access to this cloud-based service.

Design examples

We can consider an example architecture for an organization that would like to extend the security perimeter to remote users for SIA, has multiple applications hosted internally, and makes use of multiple SaaS applications from a variety of providers.

This organization has the following security goals and the corresponding SASE solution for each of these goals:

Security Goal	SASE Solution
Ensure Secure Internet Access to remote users with endpoints such as workstations and mobile devices	Secure Internet Access for agent-based remote users using FortiClient and the FortiSASE FWaaS
Ensure Secure Internet Access to remote users for web traffic only, or for endpoints based on web browsers such as Chromebooks	Secure Internet Access for agentless remote users using explicit web proxy on web browsers and the FortiSASE SWG service
Ensure Secure Internet Access for sites using a thin-edge device	Secure Internet Access for site-based remote users using FortiExtender as a LAN extension to FortiSASE
Ensure Secure Internet Access for sites using a FortiGate device while providing Secure Private Access to private resources behind the FortiGate	Secure Internet Access for site-based remote users using FortiGate as a LAN extension to FortiSASE
Ensure Secure Internet Access for sites using a FortiAP edge device	Secure Internet Access for site-based remote users using FortiAP managed by FortiSASE
Control direct access to internal networks for TCP-based applications such as web applications or remote desktop	Secure Private Access using FortiGate ZTNA access proxies, FortiClient, and FortiSASE Endpoint Management Service
Allow seamless access to internal networks behind existing FortiGate SD-WAN networks for TCP-based and UDP-based applications	Secure Private Access using SD-WAN
Allow seamless access to internal networks behind newly deployed FortiGate NGFW for TCP-based and UDP-based applications	Secure Private Access using NGFW

Security Goal	SASE Solution
Allow seamless access to internal networks behind existing FortiGate SD-WAN networks for TCP-based and UDP-based applications using Fabric Overlay Orchestrator	SPA using NGFW and Fabric Overlay Orchestrator
Monitor, analyze, and report on suspicious user activity, threats, and policy compliance for SaaS applications using API-based deep inspection	Secure SaaS Access using FortiCASB
Restrict tenant access to SaaS applications using FortiSASE Web Filter with Inline-CASB and SSL deep inspection. Allow, monitor, or block SaaS traffic access using FortiSASE Application Control with Inline-CASB and SSL deep inspection	Secure SaaS Access using FortiSASE Inline-CASB

This section focuses on each of the individual FortiSASE use cases and the corresponding designs and topologies deployed in those use cases. Note that these individual topologies can be combined if FortiSASE use cases are combined based on your security goals and requirements.

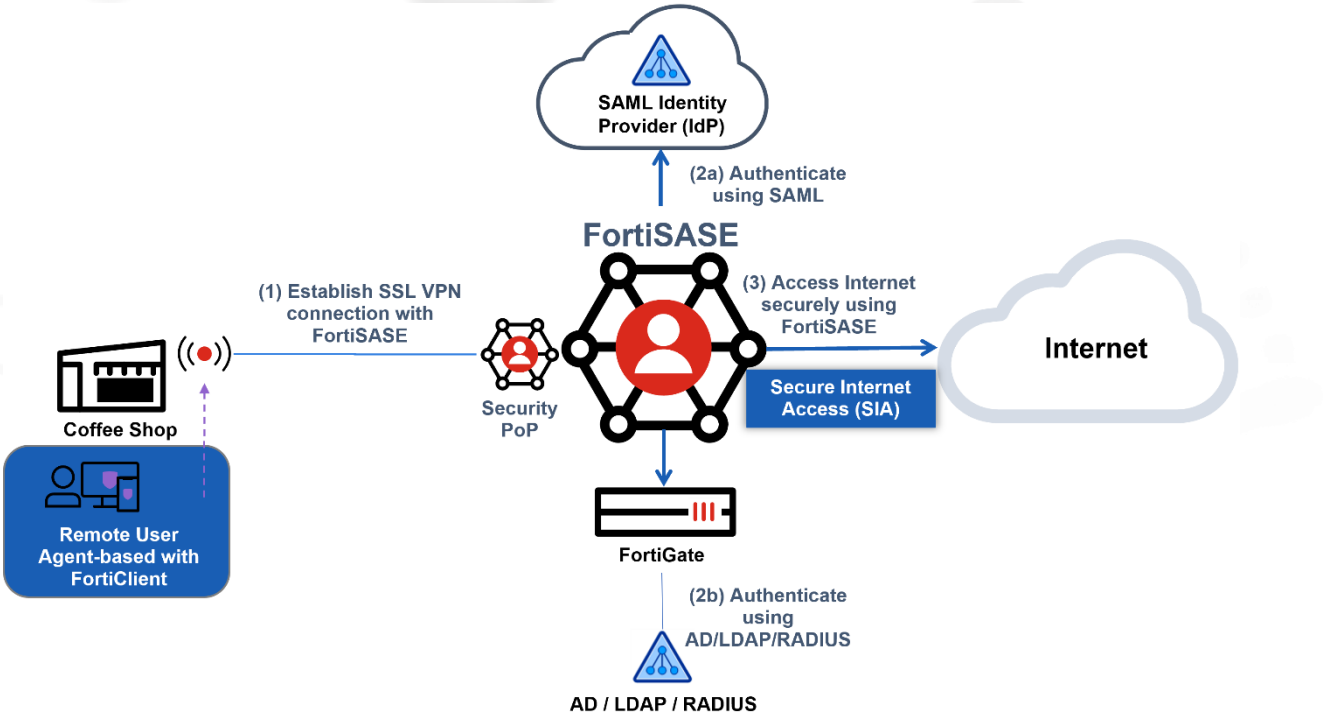
SIA for agent-based remote users

Secure Internet access (SIA) for agent-based remote users is the most typical use case, which involves installing and configuring FortiClient on supported endpoints including Windows, macOS, and Linux endpoints. In this use case, the FortiSASE firewall as a service (FWaaS) comes between the endpoint and the Internet. Because FortiClient essentially sets up a full-tunnel SSL VPN with the FWaaS, agent-based SIA secures all Internet traffic and protocols using VPN policies. Each endpoint connects to a security point of presence.

You can achieve authentication for users in this use case by configuring the authentication source as Active Directory/LDAP or RADIUS or as a SAML identity provider.

You can automate initial configuration of endpoints using a mobile device management (MDM) tool. End user deployment involves entering an invitation code into FortiClient and then using a username and password to log into the Secure Internet Access SSL VPN tunnel to FortiSASE.

A typical topology for deploying this example design is as follows:



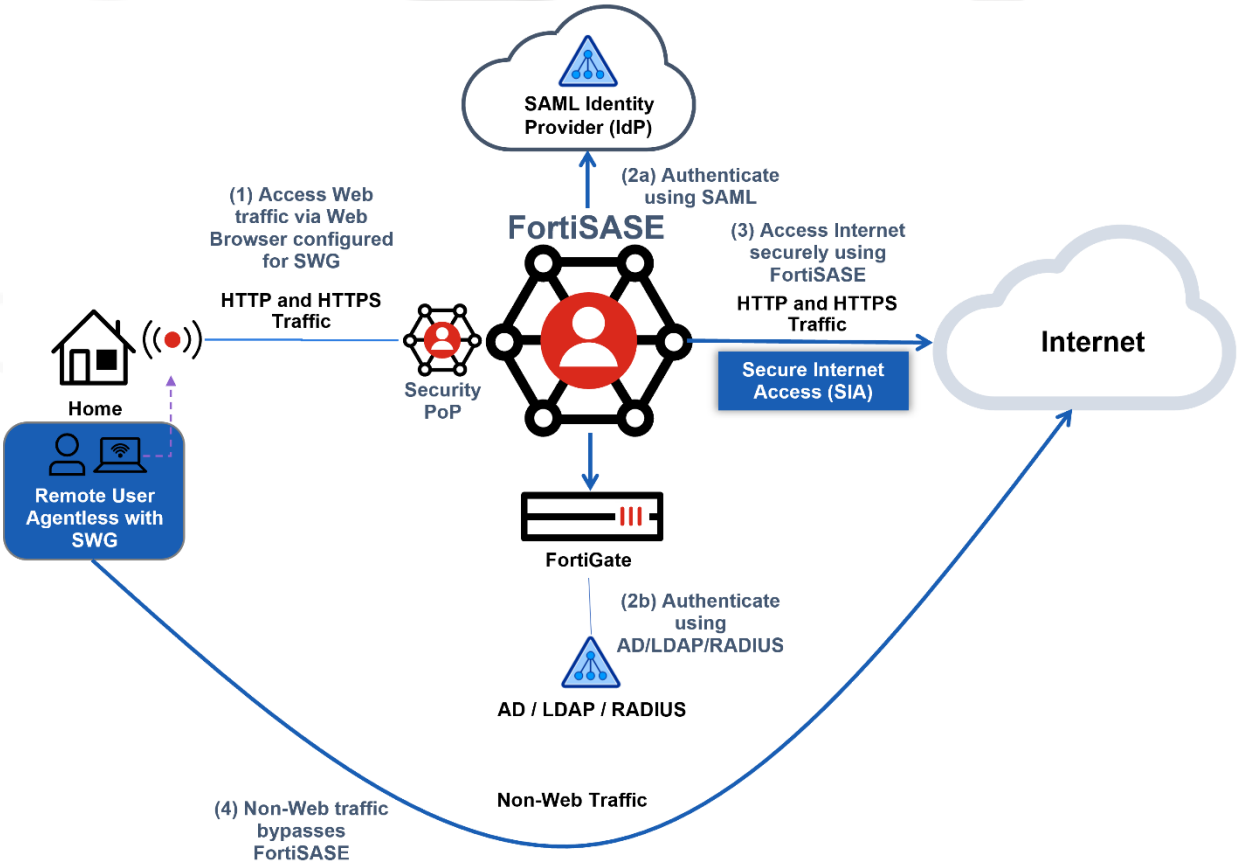
SIA for agentless remote users

SIA for agentless remote users involves setting up a web browser, or of a browser-based device using a proxy auto-configuration (PAC) file to use the FortiSASE SWG service as an explicit web proxy. The web browser will redirect HTTP and HTTPS traffic to the SWG, which secures user web traffic by implementing SWG security policies. All other non-web traffic will bypass FortiSASE and will be forwarded to the Internet directly.

You can achieve authentication for users in this use case by configuring the authentication source as Active Directory/LDAP or RADIUS or as a SAML identity provider.

Initial configuration of the proxy settings for web browsers can be automated using Windows Group Policy Objects (GPOs) or Microsoft System Center Configuration Manager (SCCM).

A typical topology for deploying this example design is as follows:

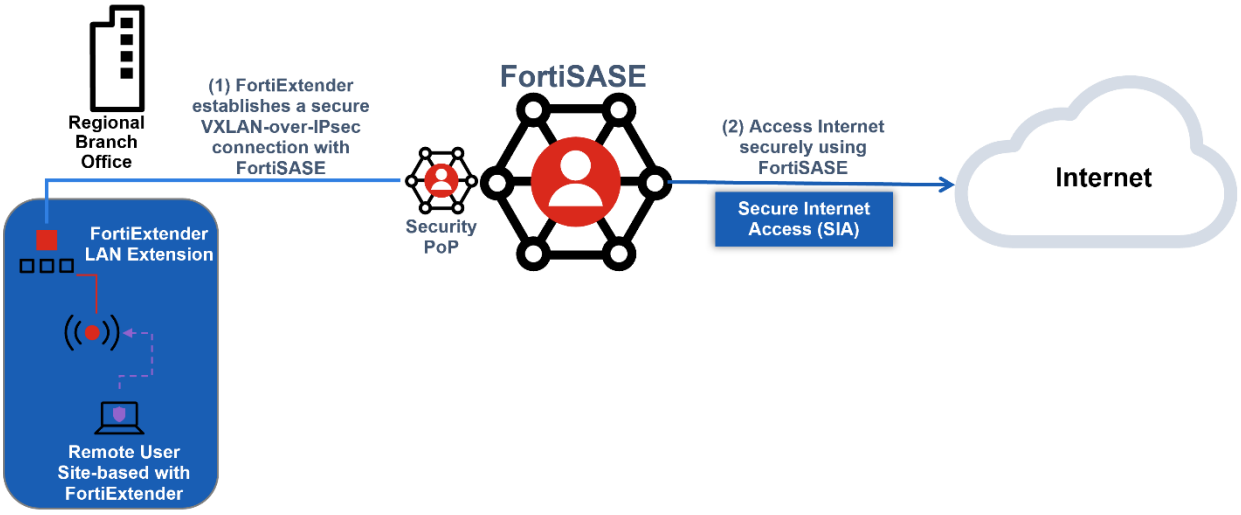

SAML Identity Provider (IdP)
(2a) Authenticate using SAML
FortiSASE
(1) Access Web traffic via Web Browser configured for SWG
HTTP and HTTPS Traffic
Security PoP
(3) Access Internet securely using FortiSASE
HTTP and HTTPS Traffic
Secure Internet Access (SIA)
Internet
Home
Remote User Agentless with SWG
FortiGate
(2b) Authenticate using AD/LDAP/RADIUS
AD / LDAP / RADIUS
Non-Web Traffic
(4) Non-Web traffic bypasses FortiSASE

SIA for site-based remote users using FortiExtender

SIA for site-based remote users involves configuring a FortiExtender as a LAN extension by setting up a VXLAN-over-IPsec tunnel between the FortiExtender and FortiSASE. This creates a Layer 2 network between FortiSASE and the network behind the remote FortiExtender. In this SIA use case, because the FortiExtender is responsible for centralizing site connectivity to the FortiSASE FWaaS, the endpoints only need to be configured in their IP settings to forward traffic to the FortiExtender as the default gateway. For details, see FortiExtender as FortiSASE LAN extension.

Therefore, for this SIA use case, individual workstation or device setup is minimized because FortiClient does not need to be installed on endpoints and web browser-based endpoint do not require explicit web proxy settings to be configured.

A typical topology for deploying this example design is as follows:



SIA for site-based remote users using FortiAP

FortiAP edge device support is a controlled General Availability feature that requires a separate FortiSASE subscription license per FortiAP. FortiAP 231F and 431F devices running FortiAP firmware 7.2.4 and above are supported.

Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each FortiAP. To enable this feature for your tenant after it has been licensed accordingly, the FortiSASE security points of presence must run a feature release environment. If you require this support for your FortiSASE instance and already have the proper licenses, contact FortiCare Support.

Secure Internet access (SIA) for site-based remote users using FortiAP involves configuring FortiSASE as the wireless controller managing a FortiAP device. A CAPWAP tunnel is established between FortiSASE and the FortiAP device.

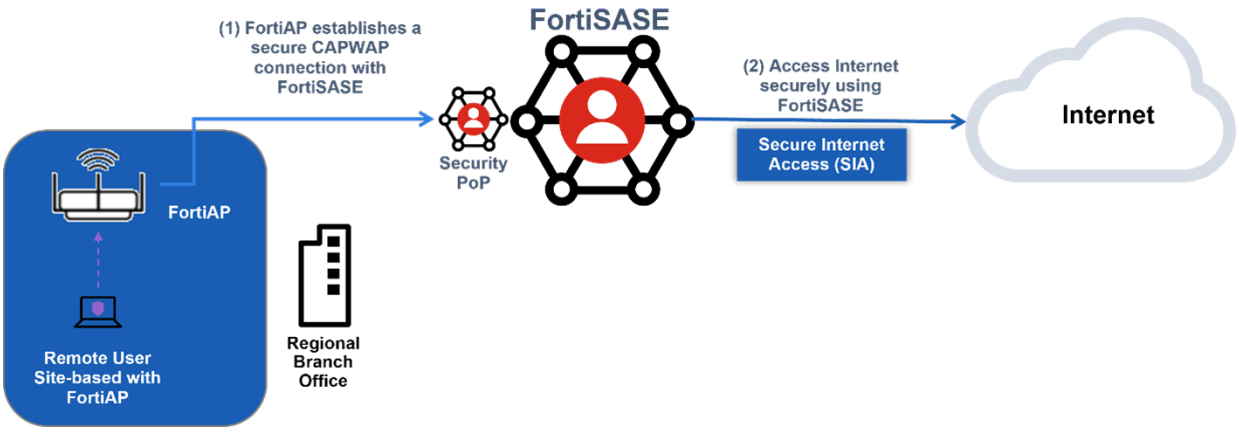
There are two channels inside the CAPWAP tunnel:

- Control channel for managing traffic, which is always encrypted by DTLS.
- Data channel for carrying client data packets, which you can configure to be encrypted or not.

For FortiSASE to manage a FortiAP, the data channel is encrypted using an IPsec VPN tunnel between FortiSASE and the FortiAP that carries CAPWAP data packets.

Therefore, this SIA use case minimizes individual workstation or device setup because FortiClient does not need to be installed on endpoints and web browser-based endpoints do not require explicit web proxy setting configuration.

A typical topology for deploying this example design is as follows:



Site-based remote users using FortiGate SD-WAN as a secure edge

FortiGate SD-WAN as a secure edge is a controlled General Availability feature that requires a separate FortiSASE subscription license per FortiGate. All FortiGate F-series and G-series desktop platforms running FortiOS 7.4.2 and above can support FortiSASE Secure Edge connectivity.

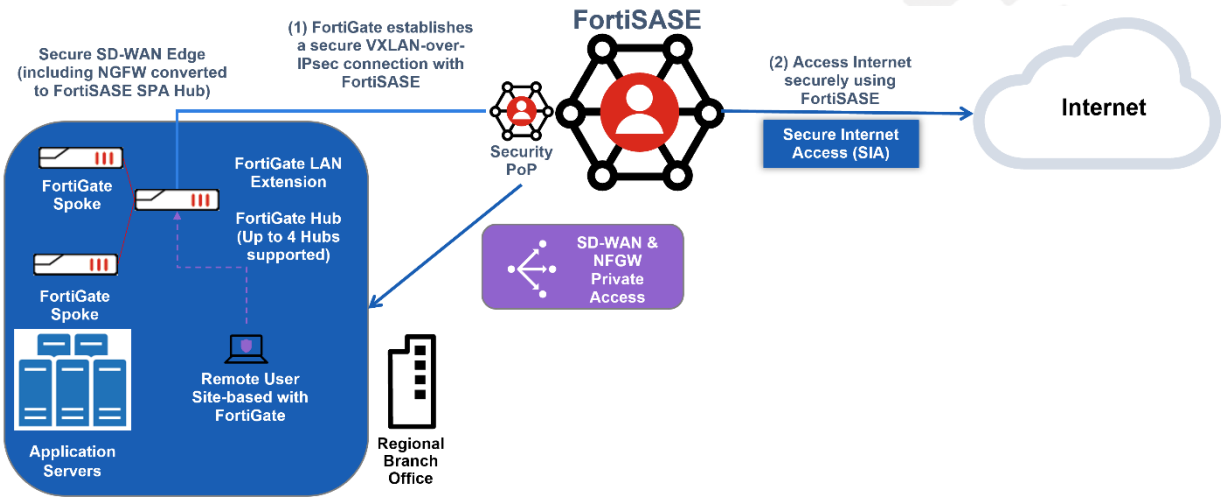
Contact your Fortinet Sales/Partner representative to purchase a FortiSASE subscription license for each FortiGate and to enable this feature for your tenant after it has been licensed accordingly.

You can configure a FortiGate SD-WAN device as a LAN extension by setting up a VXLAN-over-IPsec tunnel between the FortiGate and FortiSASE. This creates a layer 2 network between FortiSASE and the network behind the remote FortiGate. In this use case, because the FortiGate is responsible for centralizing its remote users' site connectivity to the FortiSASE FWaaS, the endpoints only need to be configured in their IP settings to forward traffic to the FortiGate as the default gateway. For more details, see FortiGate LAN extension.

Therefore, for this use case, individual workstation or device setup is minimized because FortiClient does not need to be installed on endpoints and web browser-based endpoint do not require explicit web proxy settings to be configured.

Also, for this use case, FortiSASE can be configured using Secure Private Access (SPA) support as described later, to allow other FortiSASE remote users to access private resources behind the FortiGate device configured as either an SD-WAN hub or an NGFW converted to an SPA hub.

A typical topology for deploying this example design is as follows:



Secure private access using ZTNA

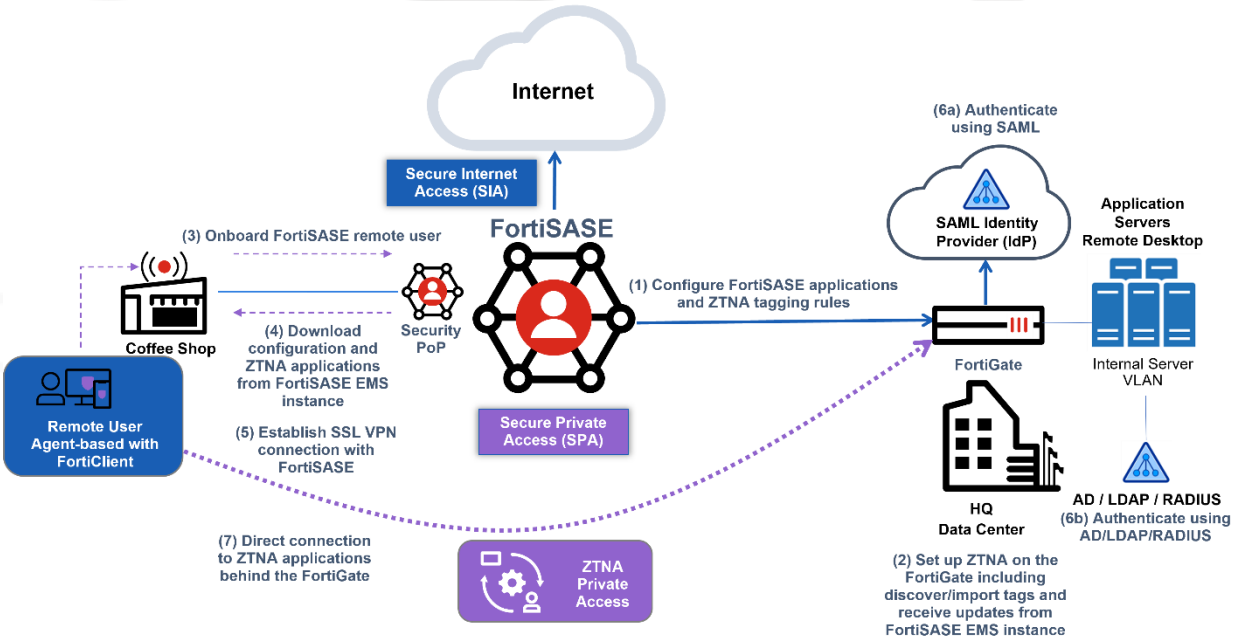
FortiSASE agent-based remote users can securely access private resources, namely, TCP-based applications using ZTNA. This use case offers a direct (shortest) path to private resources and per-session user authentication thus offering greater performance and security. ZTNA has the following requirements:

- A FortiGate must be located at an organization's headquarters data center (on-premises, private cloud, or public cloud) and configured as a ZTNA access proxy that controls access to resources behind the FortiGate.
- Remote users must be agent-based with FortiClient installed.

ZTNA requires the FortiClient to be managed by the FortiSASE Endpoint Management Service to discover the endpoint's device information, log on user information, and security posture, and to request and obtain a client certificate from the FortiSASE Endpoint Management Service. FortiSASE Endpoint Management Service applies ZTNA tagging rules to tag the clients. FortiSASE then shares the tags and client certificate details with the FortiGate. The FortiGate ZTNA access proxy uses the client certificate to verify the client's identity and grants or denies access based on the client's ZTNA tags.

You can achieve authentication for users in this use case by configuring the authentication source as Active Directory/LDAP or RADIUS or as a SAML identity provider.

A typical topology for deploying this example design is as follows:



SPA using SD-WAN

Organizations with existing FortiGate SD-WAN deployments can provide their remote users with access to private resources using FortiSASE. This use case offers broader and seamless access to privately hosted applications, both TCP- and UDP-based.

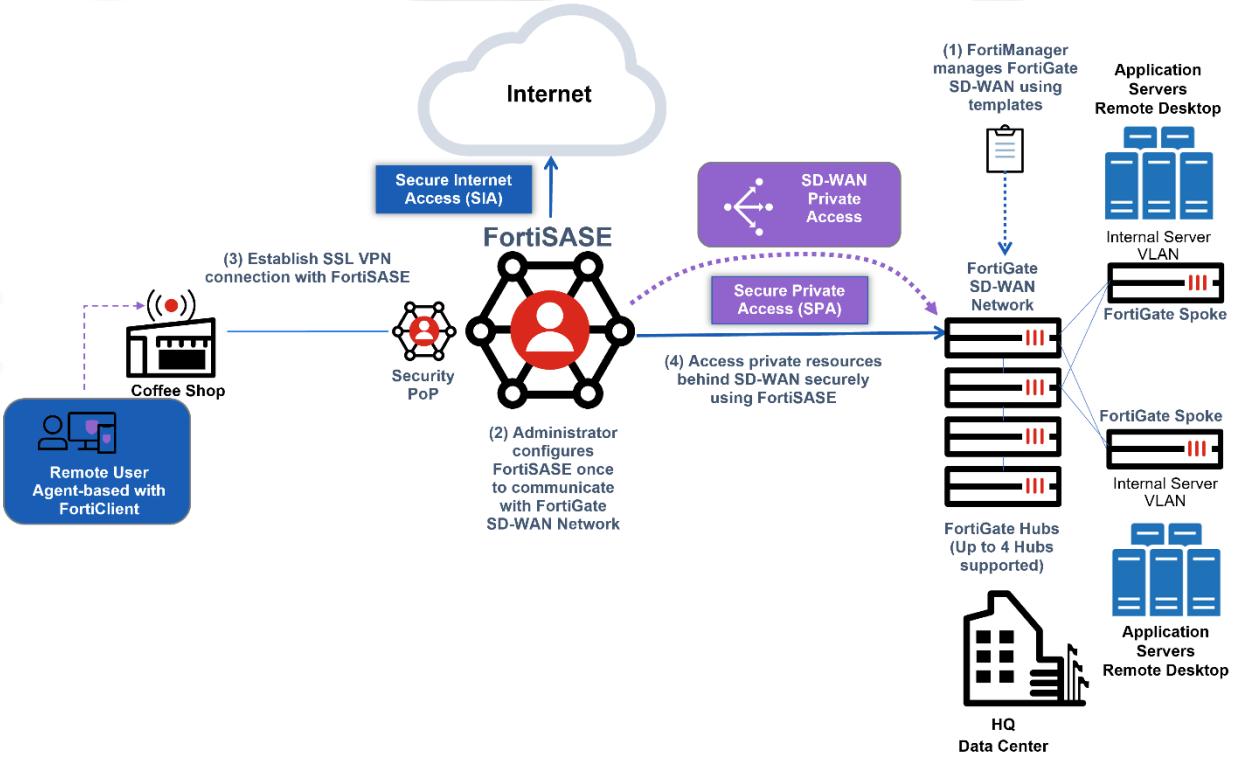
In the SD-WAN SPA use case, the Security PoPs act as spokes in the organization's SD-WAN network, relying on IPsec VPN overlays and BGP to secure and route traffic between PoPs and the networks behind an organization's SD-WAN hubs and spokes.

Existing FortiGate SD-WAN network deployments are expected to conform to Fortinet's best practices for SD-WAN architecture and deployment for the following topologies:

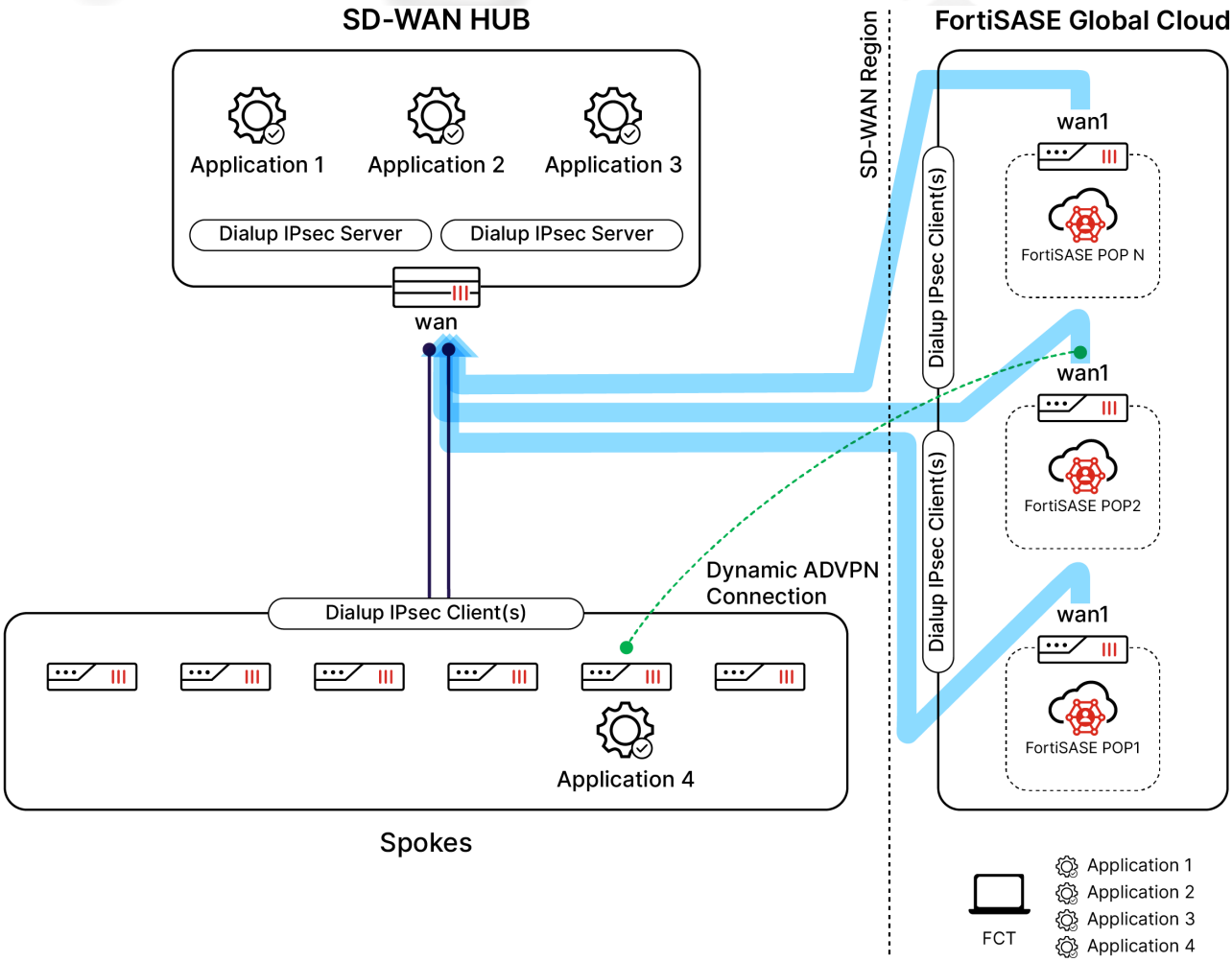
- SD-WAN with a single datacenter/hub
- SD-WAN with dual datacenters/hubs
- SD-WAN with up to four datacenters/hubs

For a list of product prerequisites, see SPA using a FortiGate SD-WAN hub.

A typical topology for deploying this example design is as follows:



FortiSASE security PoPs and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel. Therefore, the SPA use cases with FortiGate hubs only allow traffic to be initiated from FortiSASE spokes to FortiGate spokes.

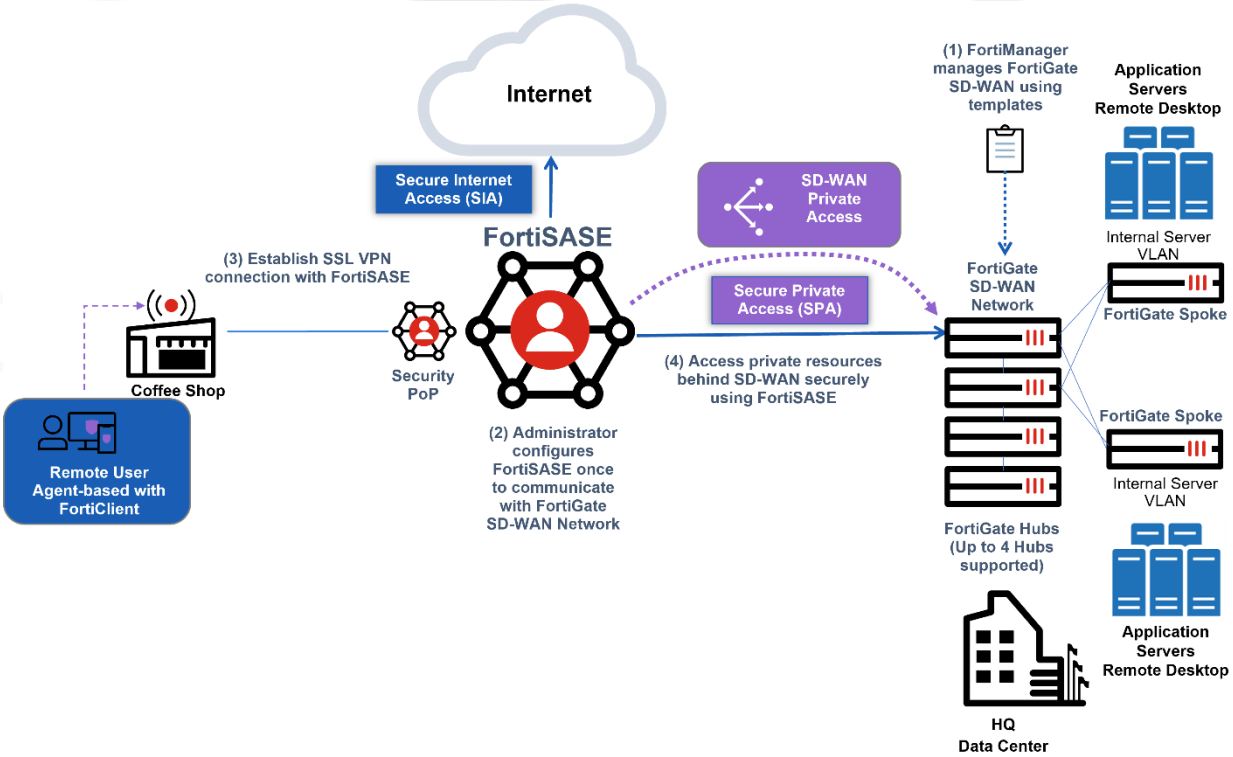
SPA using NGFW

Organizations with existing FortiGate next generation firewall (NGFW) deployments can provide their remote users using FortiSASE with access to private resources. This use case offers broader and seamless access to privately hosted applications, both TCP- and UDP-based.

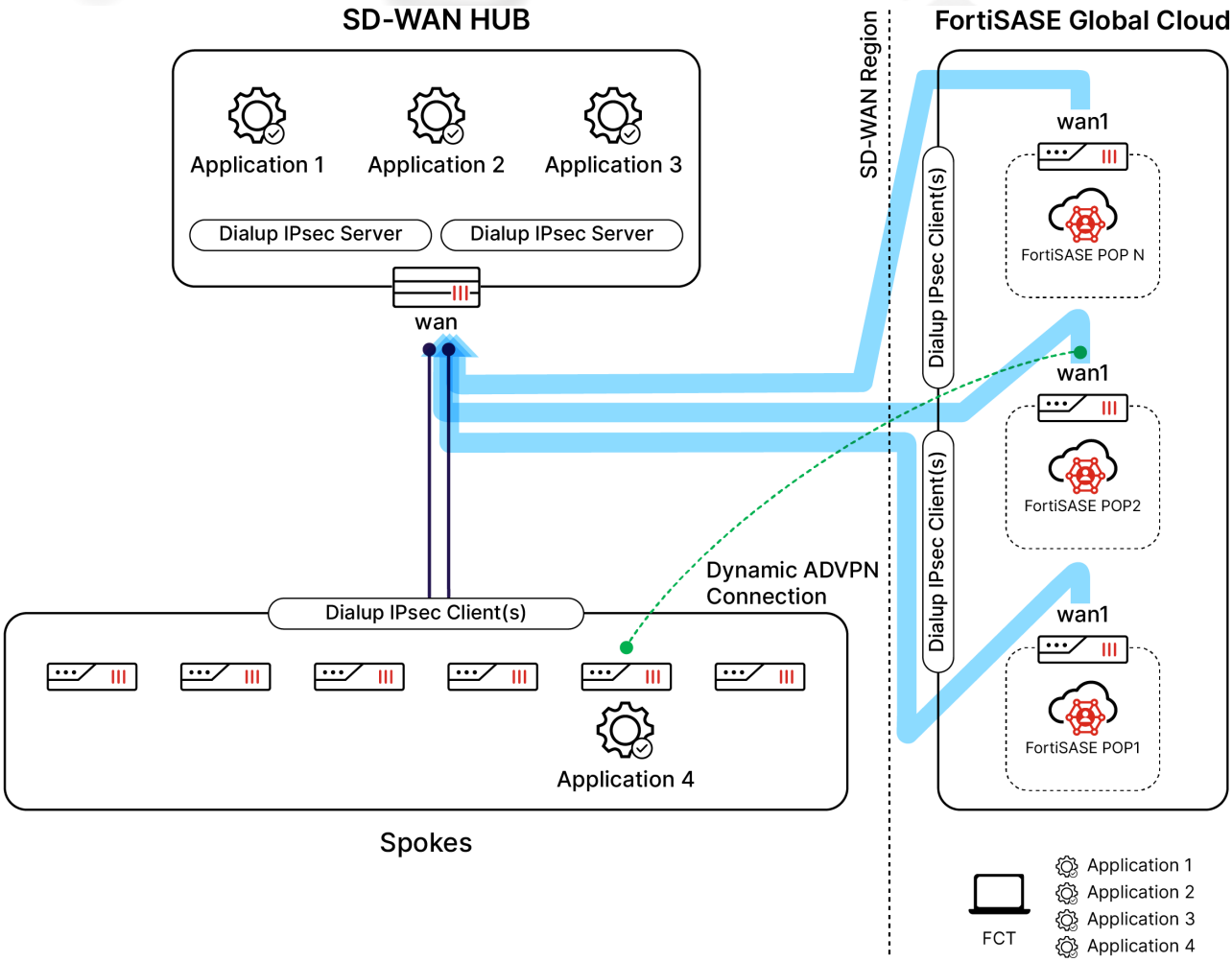
In the NGFW SPA use case, you must first convert the NGFW to a standalone IPsec VPN hub and the security points of presence (PoP) act as spokes to this hub, relying on IPsec VPN overlays and BGP to secure and route traffic between PoPs and the networks behind the organization's NGFW. This example design supports up to four hubs.

For a list of product prerequisites, see SPA using a FortiGate SD-WAN hub.

A typical topology for deploying this example design is as follows:



FortiSASE security PoPs and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel. Therefore, the SPA use cases with FortiGate hubs only allow traffic to be initiated from FortiSASE spokes to FortiGate spokes.

SPA using NGFW and Fabric Overlay Orchestrator

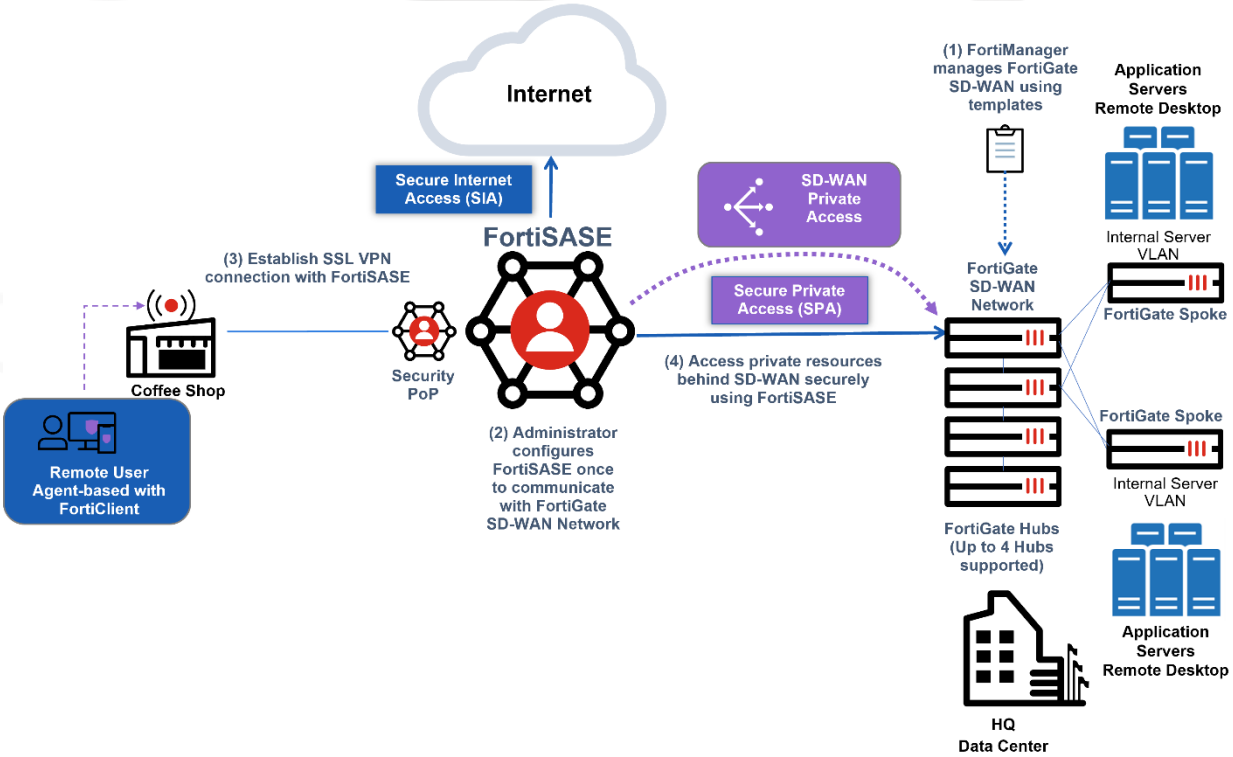
Organizations that have resources behind a newly deployed FortiGate next generation firewall (NGFW) standalone site or behind a newly deployed FortiGate NGFW in a data center and are not configured with SD-WAN enabled can provide their FortiSASE remote users with access to private resources.

Scenarios involving a FortiGate NGFW converted to a FortiSASE secure private access (SPA) hub or involving an existing FortiGate SD-WAN hub allow broader and seamless access to privately hosted TCP- and UDP-based applications.

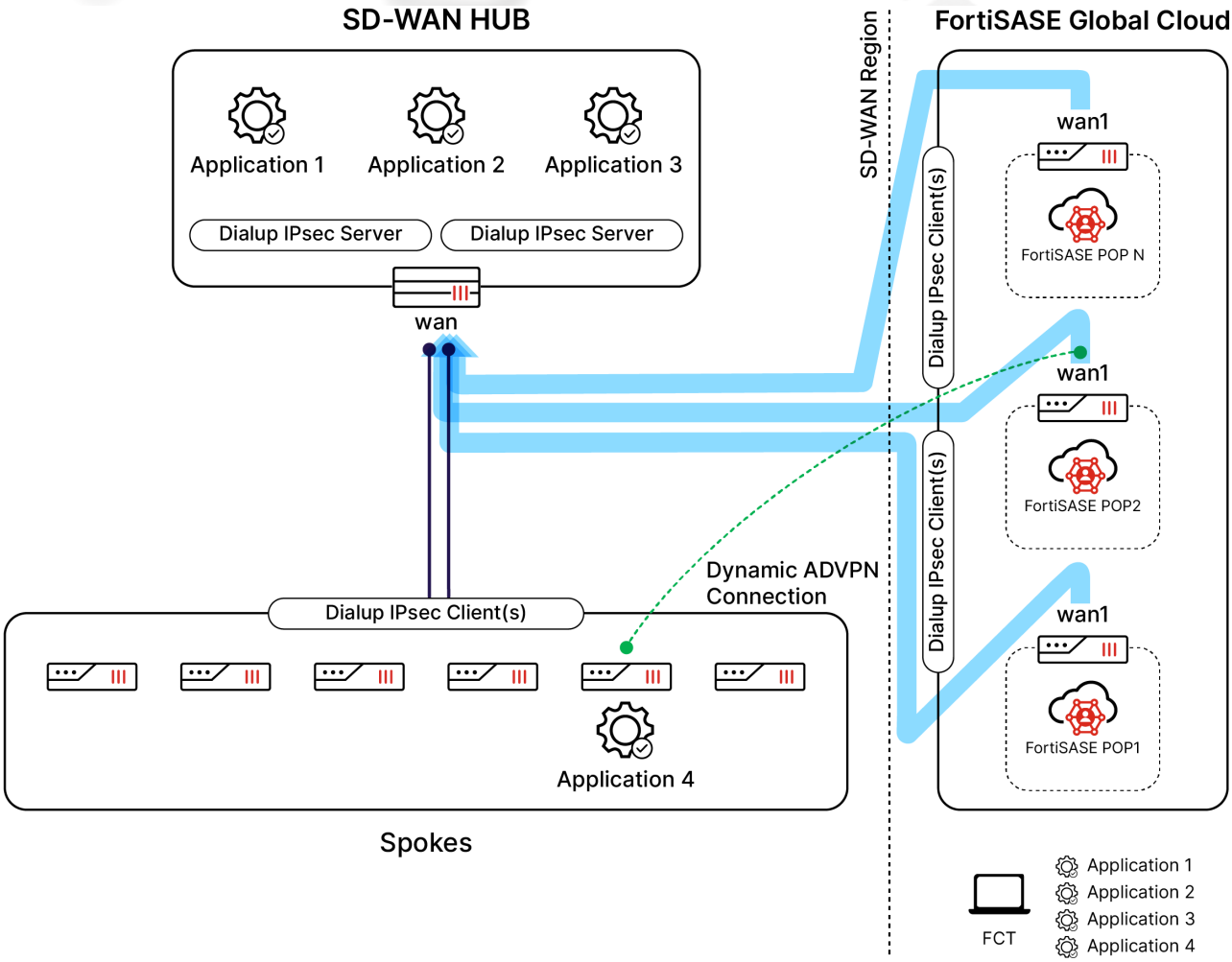
In the NGFW SPA use case, you must first convert the newly deployed NGFW to a FortiSASE SPA hub. Starting in FortiOS 7.2.4, you can accomplish this using Fabric Overlay Orchestrator. After configuring FortiSASE to communicate with this hub, the FortiSASE security points-of-presence (PoPs) act as spokes to this hub, relying on IPsec VPN overlays and iBGP to secure and route traffic between PoPs and the networks behind the organization's NGFW.

For a list of product prerequisites, see SPA using a FortiSASE SPA hub with Fabric overlay orchestrator.

A typical topology for deploying this example design is as follows:



FortiSASE PoPs and the organization's FortiGate hubs form a traditional hub-and-spoke topology that supports the Fortinet autodiscovery VPN (ADVPN) configuration. ADVPN is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels, known as shortcut tunnels, between each other to avoid routing through the topology's hub device.



FortiSASE remote users may access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels. If a private resource is behind an organization's spoke device, they may connect directly to that resource through an on-demand, direct, and dynamic ADVPN tunnel. Therefore, the SPA use cases with FortiGate hubs only allow traffic to be initiated from FortiSASE spokes to FortiGate spokes.

Secure SaaS access using FortiCASB

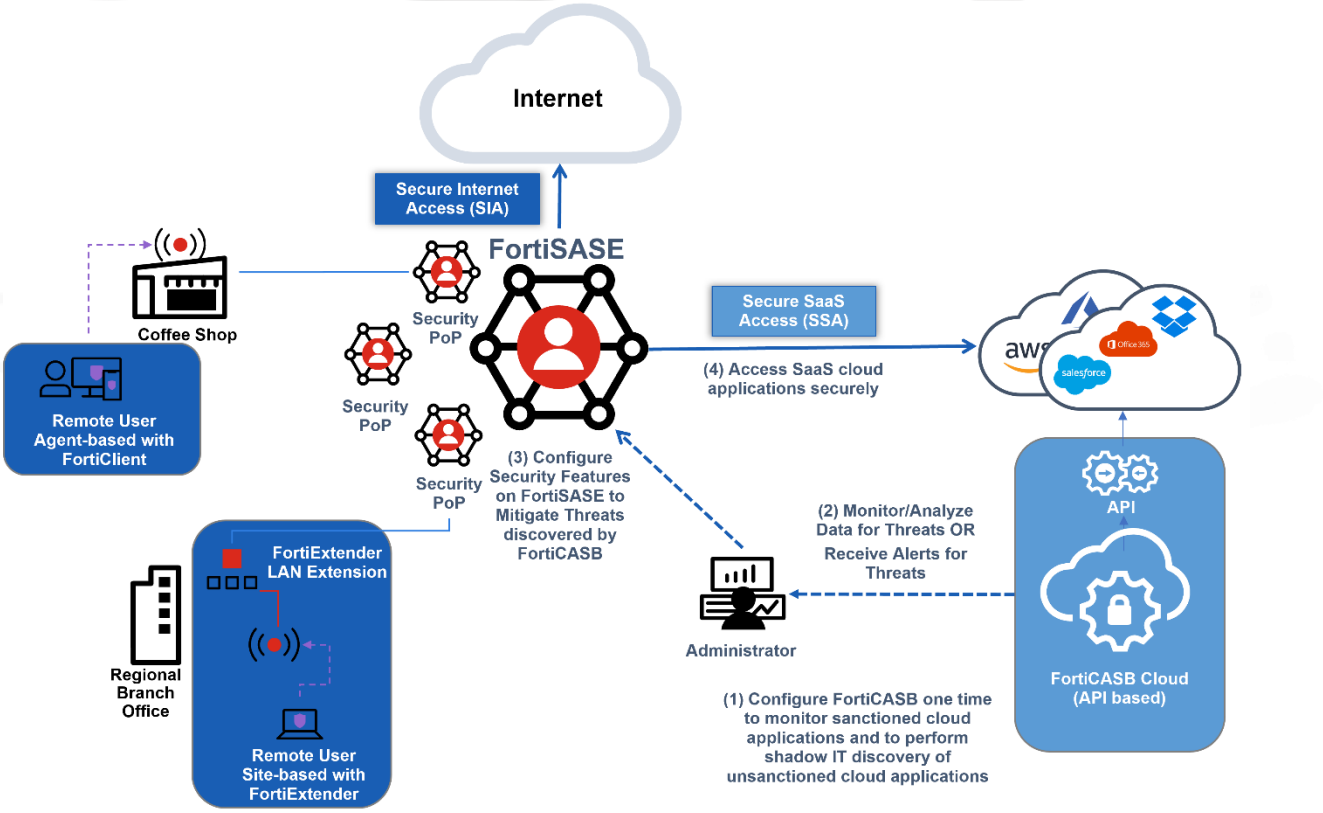
FortiCASB offers an API-based approach by obtaining data directly from SaaS cloud applications such as Office 365 or Dropbox using REST API queries with OAuth2.0 authentication. Therefore, FortiCASB can essentially perform deep inspection of cloud traffic, providing advanced monitoring, analysis, and reporting providing notifications when suspicious activity is triggered.

Since this FortiCASB performs out-of-band communication with SaaS applications, there is no performance impact on user SaaS application traffic.

FortiCASB provides insights on suspicious activity on past and current cloud user activity and relies on the network administrator to review and act upon these insights after they have already occurred. Mitigation actions include making configuration changes on FortiSASE or the FortiGate NGFW to block future suspicious activity or include denying or restricting a user's access on the SaaS application itself for the specific user generating the suspicious activity.

Access to FortiCASB is included with per-user and per-endpoint FortiSASE licensing.

A typical topology for deploying this example design is as follows:



SSA using FortiSASE Inline-CASB

For the secure SaaS access (SSA) use case, FortiSASE offers Inline-cloud access security broker (Inline-CASB) functionality for its application control and web filter security components and offers data loss protection (DLP) functionality to ensure FortiSASE agent-based and agentless remote users have secure access to SaaS applications.

FortiSASE uses Application Control to act as an Inline-CASB by providing access control to software-as-a-service (SaaS) cloud application traffic. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources.

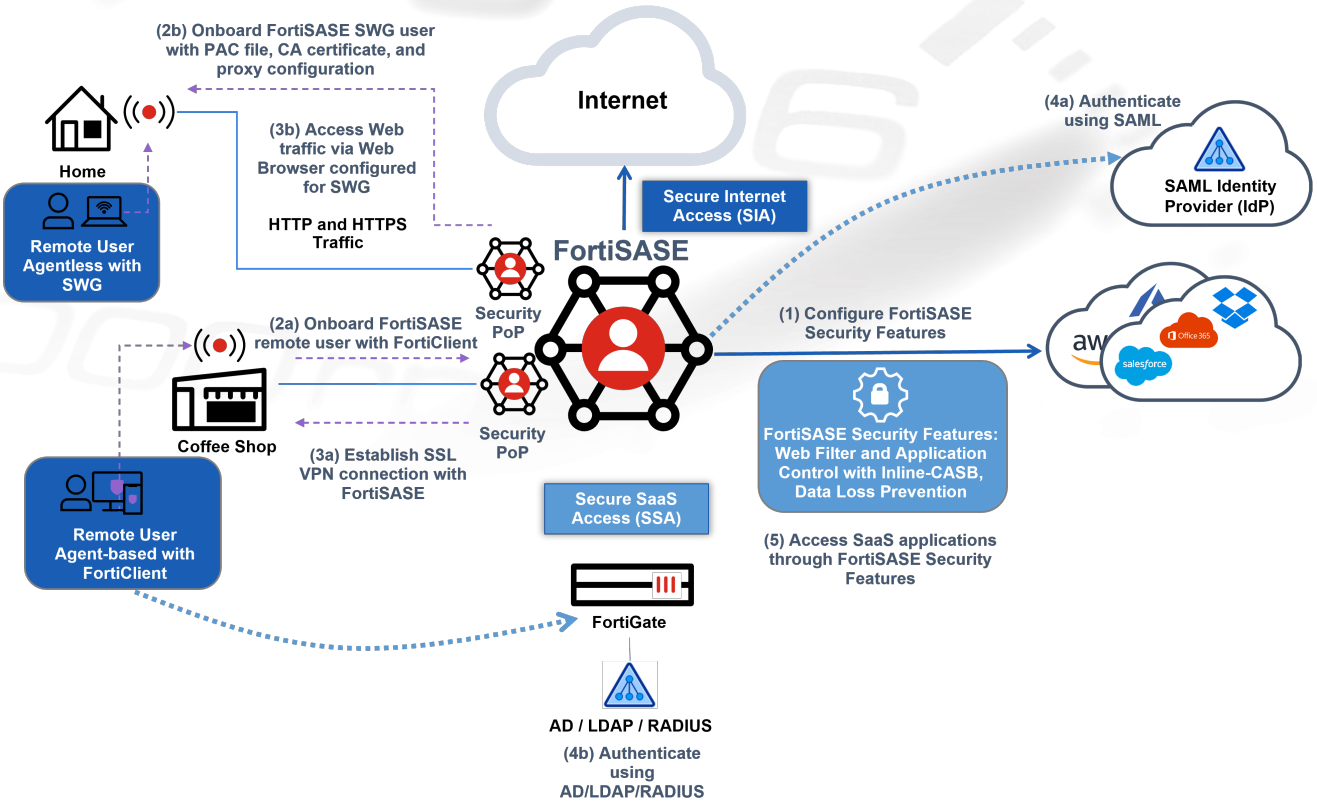
Also, FortiSASE uses Web Filter with an Inline-CASB security component to customize headers when agentless (SWG) or agent-based (FortiClient) remote users are accessing SaaS applications. When configured, FortiSASE intercepts HTTP headers and can modify them for outgoing traffic and this process is also commonly known as HTTP header insertion. By customizing HTTP headers for FortiSASE outgoing traffic destined for SaaS applications, the Web Filter with Inline-CASB can control SaaS application behavior by restricting tenants' access.

In addition, FortiSASE uses data loss prevention (DLP) to prevent sensitive data from leaving or entering your network by defining various sensitive data patterns, scanning for the patterns while inspecting traffic, and allowing, blocking, or logging only when traffic matches the patterns.

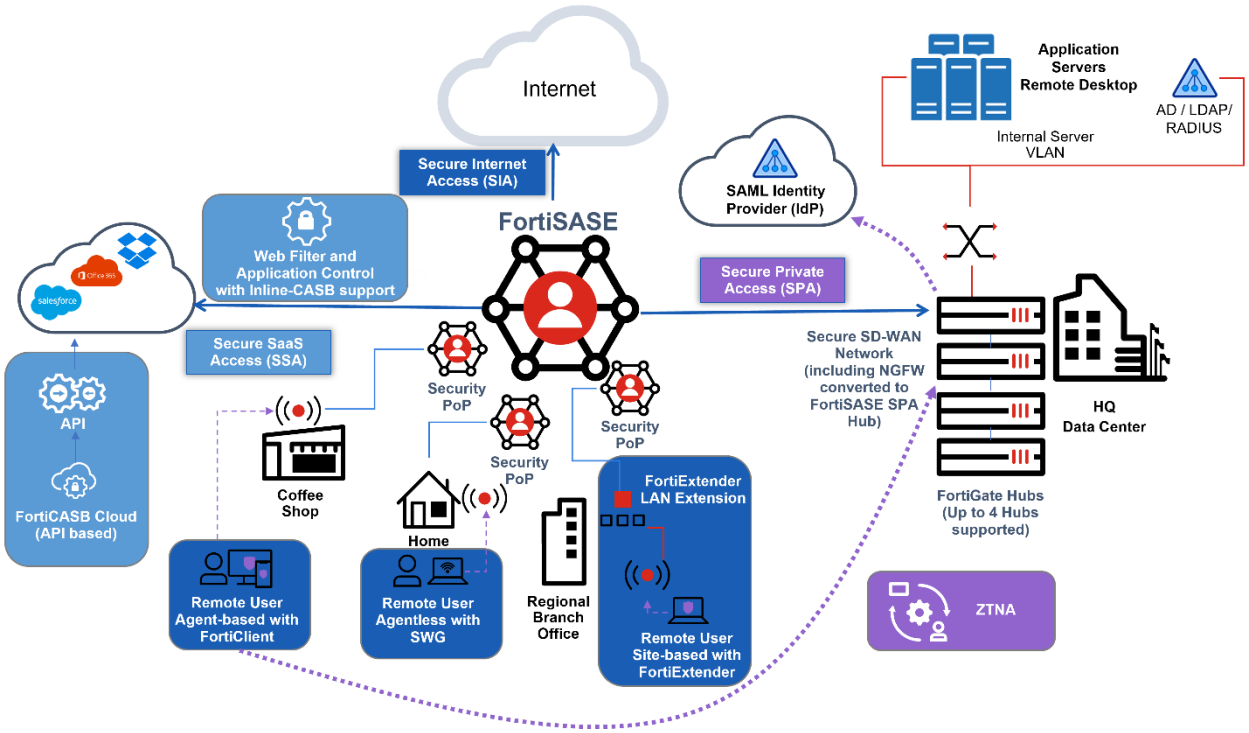
SSL deep inspection is required by Application Control, Web Filter, and DLP components to perform inline scanning and detection of content within encrypted payloads. FortiSASE must be configured to block QUIC traffic to ensure traffic falls back to TLS encryption which can be inspected.

FortiSASE web filter with Inline-CASB, application control with Inline-CASB, and DLP do not require any special licenses beyond per-user FortiSASE licensing.

A typical topology for deploying this example design is as follows:



Design topology



DESIGN TOPOLOGY

In this example topology, minor changes to the existing physical infrastructure were necessary. FortiGates replaced existing firewalls at the headquarters (HQ) data center. The internal application servers stayed in place with the same IP scheme in the server VLAN.

Secure Internet access using FortiSASE was achieved as follows:

- As the coffee shop remote user demonstrates, FortiClient was installed on supported endpoints to provide remote users with agent-based access to FortiSASE using SSL VPN dial-up tunnels.
- As the home remote user demonstrates, for endpoints that do not support FortiClient, the web browser settings were configured to support explicit web proxy functionality using agentless access to FortiSASE.
- As the regional branch office remote user demonstrates, for endpoints where FortiClient was not supported or were not chosen to be used, FortiExtender as a LAN extension was configured, and endpoints configured to point to the FortiExtender as the default gateway.

Authentication for agent-based and agentless FortiSASE remote users was achieved using the internal LDAP server.

For FortiSASE remote users, no access is provided directly to the internal network.

- ZTNA access proxy is used and the required ZTNA components were deployed to achieve secure private access for TCP-based applications. See Design topology.
- The existing SD-WAN network and FortiSASE private access capability were deployed to achieve secure private access for UDP-based applications.

For secure SaaS access, FortiCASB was used by network administrators to gain visibility and achieve reporting on all user activity using out-of-band API communication for configured SaaS applications. Based on periodic audits of FortiCASB reports and configuration of triggers and notifications, network administrators were able to fine-tune their FortiSASE and FortiGate configurations to mitigate suspicious cloud activity.

As an alternate secure SaaS access use case, FortiSASE Inline-CASB functionality for its application control and web filter security components can be used with SSL deep inspection to provide secure SaaS access to FortiSASE agent-based and agentless remote users including the ability to block access to SaaS applications since detection occurs inline with the SaaS user traffic itself.

Planning and provisioning

This section outlines the general deployment workflow for planning and provisioning the designs that previous sections describe.

SIA for agent-based remote users

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Configure remote authentication and onboard users.
3. Configure policies to apply desired scanning and filtering for your users.
4. Download and install FortiClient on Windows, macOS, and Linux endpoints.
5. Using the invitation code, connect FortiClient to FortiSASE to activate the SASE license and provision the FortiSASE VPN tunnel.
6. In FortiClient, connect to the FortiSASE tunnel using the username and password assigned to each user.
7. Test access to the Internet using a remote device.

SIA for agentless remote users

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Configure remote authentication and onboard users.
3. Configure secure web gateway policies to apply desired scanning and filtering for your users.
4. Download the proxy autoconfiguration (PAC) file from the FortiSASE portal. Customize the file to exclude internal corporate networks.
5. Host the PAC file on an externally accessible server.
6. Configure proxy settings on endpoints to point to the PAC file.
7. Test access to the Internet using a remote device.

SIA for site-based remote users

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Register the FortiExtender 200F device used with the LAN extension feature to the same FortiCloud account used to log into FortiSASE.
3. Factory reset the FortiExtender and configure it via the FortiExtender GUI or CLI to connect to FortiSASE.
4. Authorize the FortiExtender.
5. Configure a policy to allow traffic from the thin-edge LAN to FortiSASE for secure Internet access (SIA) and apply desired scanning and filtering for your site-based users.
6. Configure the remote user endpoints to direct Internet traffic to the FortiExtender as the default gateway
7. Test access to the Internet using a remote device.

SPA using ZTNA

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Configure remote authentication and onboard users.
3. Configure VPN policies to apply desired scanning and filtering for your users.
4. Configure zero trust network access (ZTNA) tags and tagging rules.
5. Connect the FortiGate to FortiSASE over the FortiClient Cloud Fabric connector. Authorize the FortiGate on FortiSASE. FortiSASE automatically synchronizes the tags to the FortiGate.
6. On the FortiGate, configure remote authentication servers, authentication schemes, and rules.
7. Configure ZTNA servers.
8. Configure ZTNA policies and use user groups and ZTNA tags for access control.
9. In FortiSASE, configure ZTNA connection rules to push to clients.
10. Test and monitor the configuration using a remote device.

For details on ZTNA configuration on the FortiGate, see the ZTNA Deployment Guide. For details on integrating ZTNA with FortiSASE, see the FortiSASE SPA Using ZTNA Deployment Guide.

SPA Using SD-WAN

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Ensure the FortiGate SD-WAN deployment has the proper configuration:
   a. Configure a new FortiGate SD-WAN deployment using FortiManager.
   b. Review and modify the configuration settings of an existing FortiGate SD-WAN deployment using FortiManager.
3. Using the FortiSASE *Secure Private Access* page, configure the FortiSASE security PoPs as spokes of the FortiGate SD-WAN hub using its specific network attributes as parameters.
4. Verify IPsec tunnels on the FortiGate SD-WAN hub(s).

5. Verify BGP routing on the FortiGate SD-WAN hub(s).
6. Test private access connectivity to the FortiGate SD-WAN network from remote users.

SPA Using NGFW

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Convert the FortiGate next generation firewall (NGFW) to a FortiSASE SPA hub:
   a. Convert FortiGate NGFW configured using FortiOS CLI or GUI.
   b. Convert FortiGate NGFW managed by FortiManager.
3. Using the FortiSASE *Secure Private Access* page, configure the FortiSASE security PoPs as spokes of the FortiSASE SPA hub using its specific network attributes as parameters.
4. Verify IPsec tunnels on the FortiSASE SPA hub.
5. Verify BGP routing on the FortiSASE SPA hub.
6. Test private access connectivity to the FortiSASE SPA hub network from remote users.

SSA Using FortiSASE Inline-CASB

1. Provision your FortiSASE instance and select the regions where your users will be located. Input licenses as needed.
2. Configure remote authentication and onboard users based on SIA use cases.
3. Configure SSL deep inspection.
4. Customize inline-CASB headers for restricted SaaS access using web filter.
5. Configure application control with Inline-CASB to control access to SaaS cloud applications, as desired.
6. Configure policies to apply desired application control scanning and web filtering for your users.
7. Establish connectivity to FortiSASE and redirect traffic for SIA.
8. Test Web Filter with Inline-CASB using a FortiClient endpoint.
9. Test Application Control with Inline-CASB using a FortiClient endpoint.

More information

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

- 4-D FortiSASE Concept Guide
- 4-D ZTNA Architecture Guide
- 4-D SD-WAN/SD-Branch Concept Guide
- 4-D SD-WAN Architecture Guide for Enterprise

Feature documentation

Product document	Specific chapter if available
FortiOS 7.2 Admin Guide	• Zero Trust Network Access • SD-WAN
FortiClient 7.0 Admin Guide	
FortiCASB 21.4 Online Help	

Solution hub

https://docs.fortinet.com/product/fortisase

4-D Resources: SASE

- 4-D Resources: Secure Access Service Edge

www.fortinet.com

72-241-997798-20240408