



FortiSASE

Secure Access Service Edge

Maksym Porytskyy, Senior Systems Engineer

mporytskyy@fortinet.com

Проблематика

- **Гібридна робота**, що все більше стає нормою, **призводить до невідповідності безпеки та досвіду** (experience) для **віддалених співробітників** порівняно з тими, хто працює в офісі (з відповідними системами безпеки)
- У той же час **традиційні VPN** не мають **гнучкості** надання **доступу до окремих застосунків для певної категорії співробітників** та не забезпечують **видимість / контроль доступу** до застосунків та сервісів **SAAS**



Рішення

What is FortiSASE ?

- **FortiSASE** is a **cloud-delivered security-as-a-service solution** provided by Fortinet for **remote users** while they are **outside** of the protection of the **corporate network**
- **FortiSASE** is a SaaS-based service that allows remote users to **securely access the Internet, SAAS and corporate recourses**
- **FortiSASE** is utilizing components of the **Fortinet Security Fabric and FortiOS** to provide security functionality for remote users
- With **FortiSASE**, you can **ensure** that remote (off-net) endpoints and users are protected with the **same security policies** as when they are in corporate network (on-net), no matter their location

FortiSASE



FortiGate Delivered as a
Cloud Service

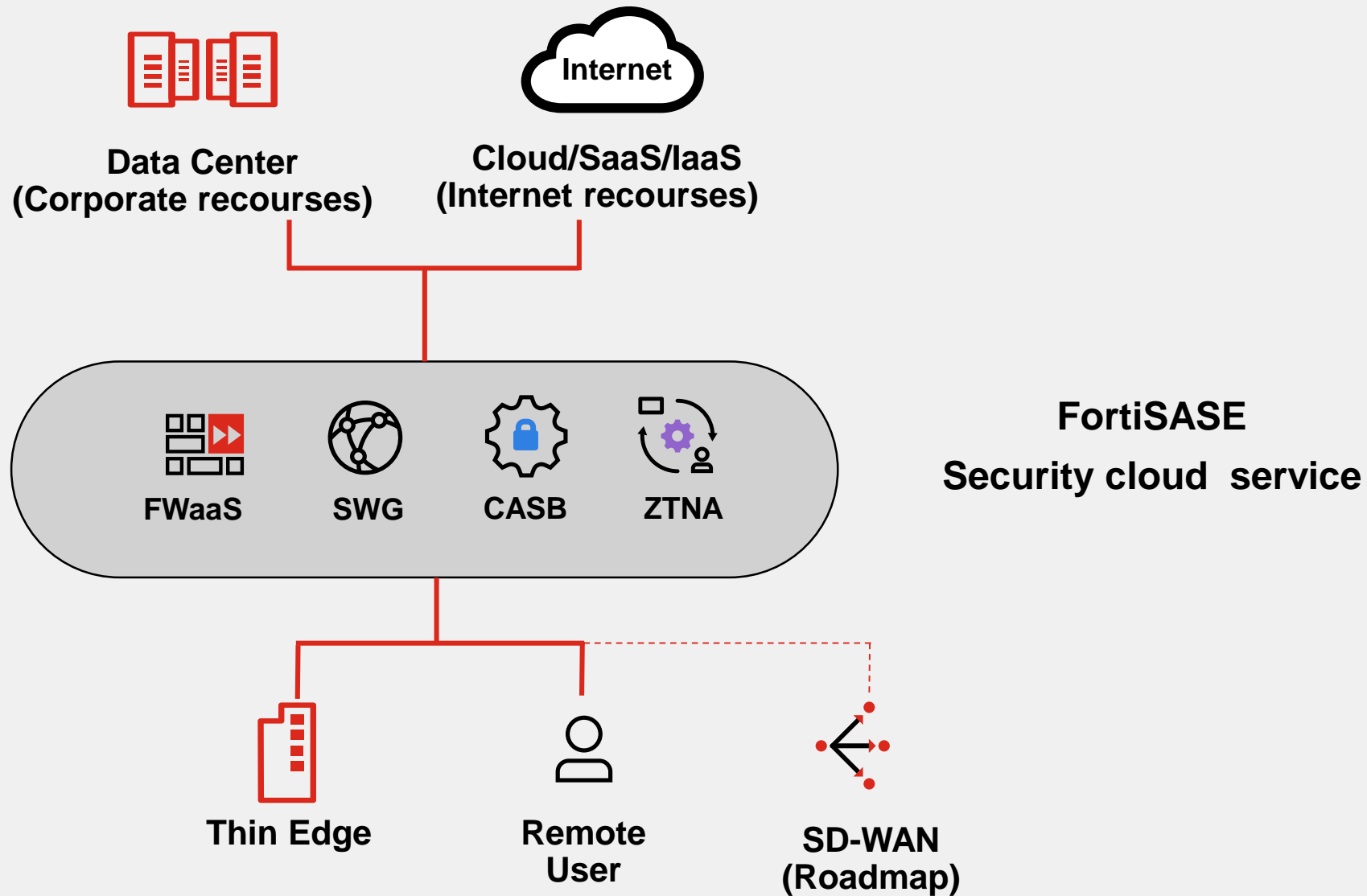


Remote
Users

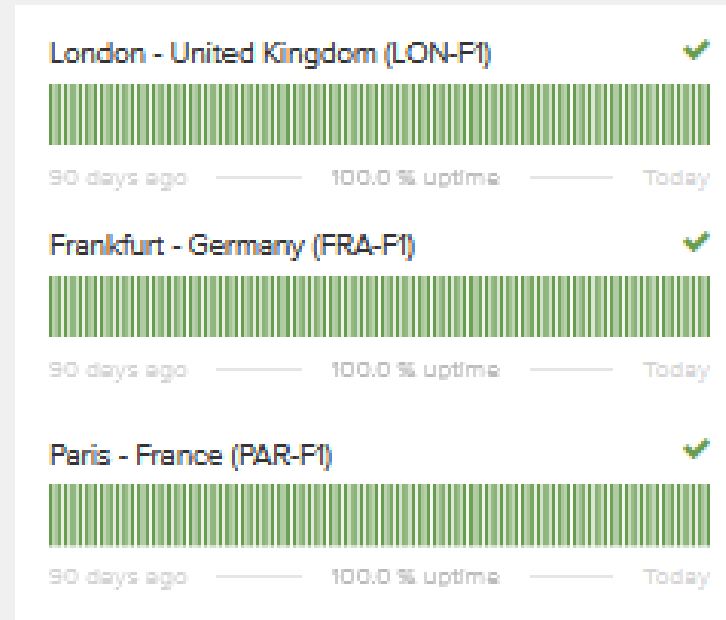
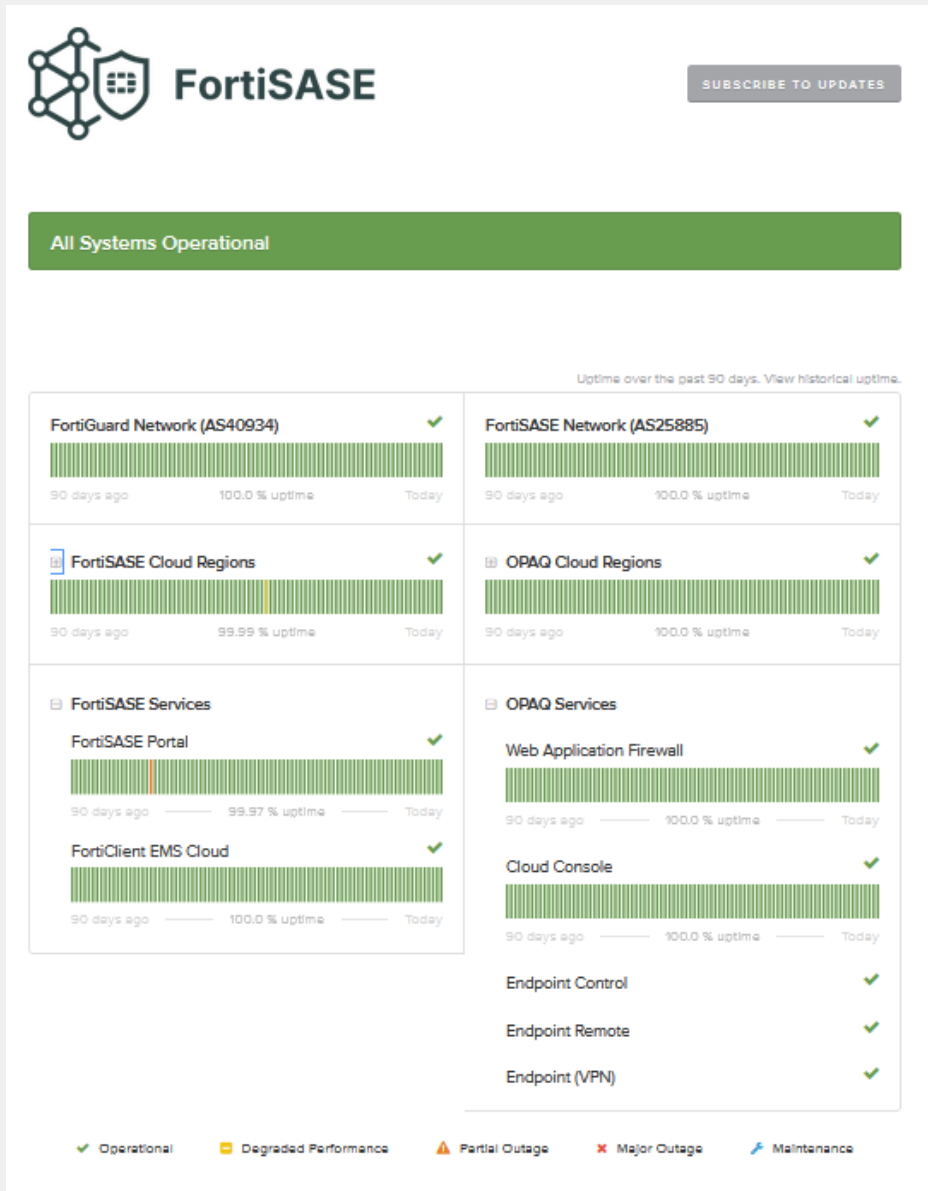


Branch
Office

FortiSASE architecture and components

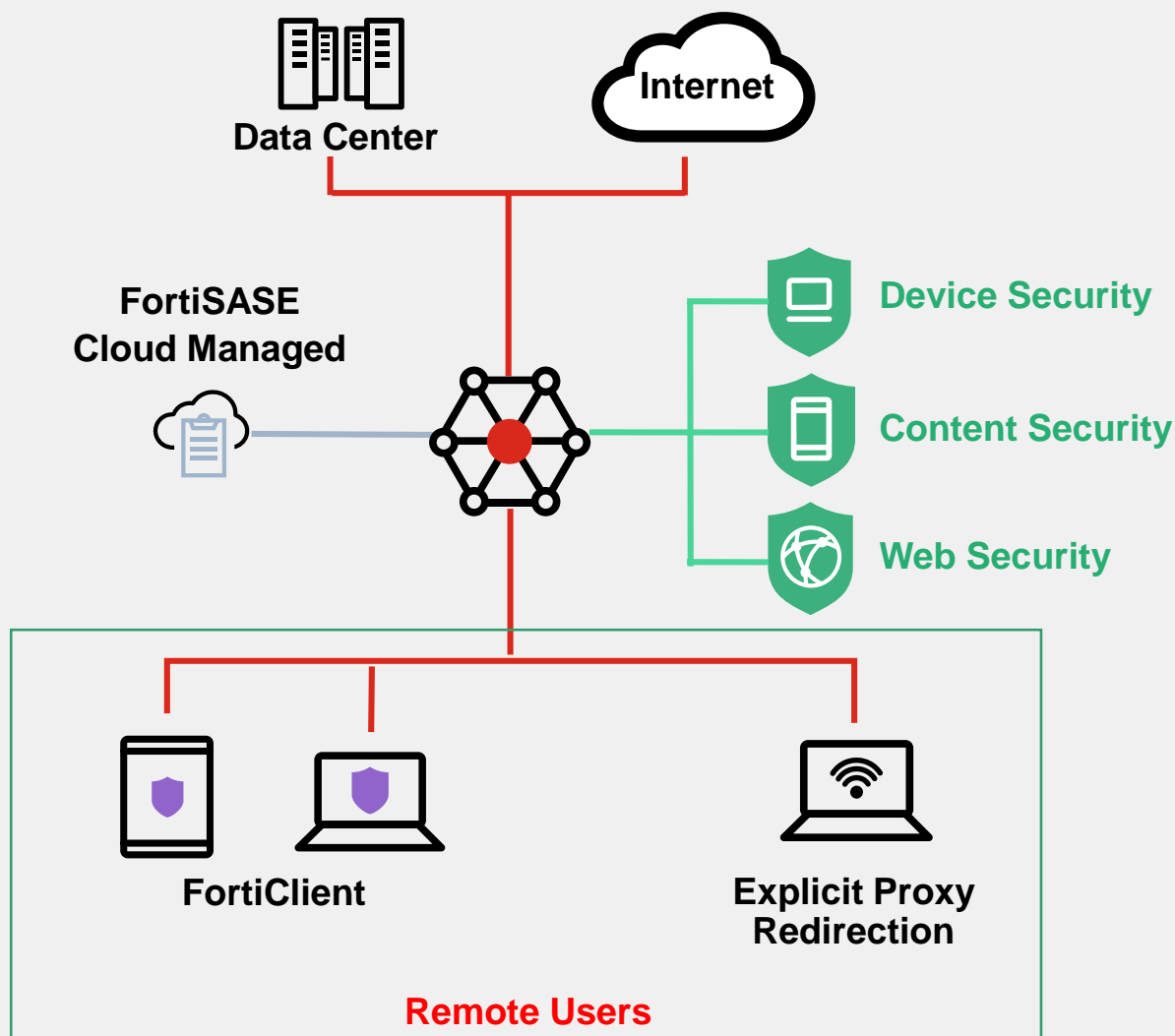


FortiSASE Security Point of Presence (PoP) = Fortinet DC



<https://status.fortisase.com/>

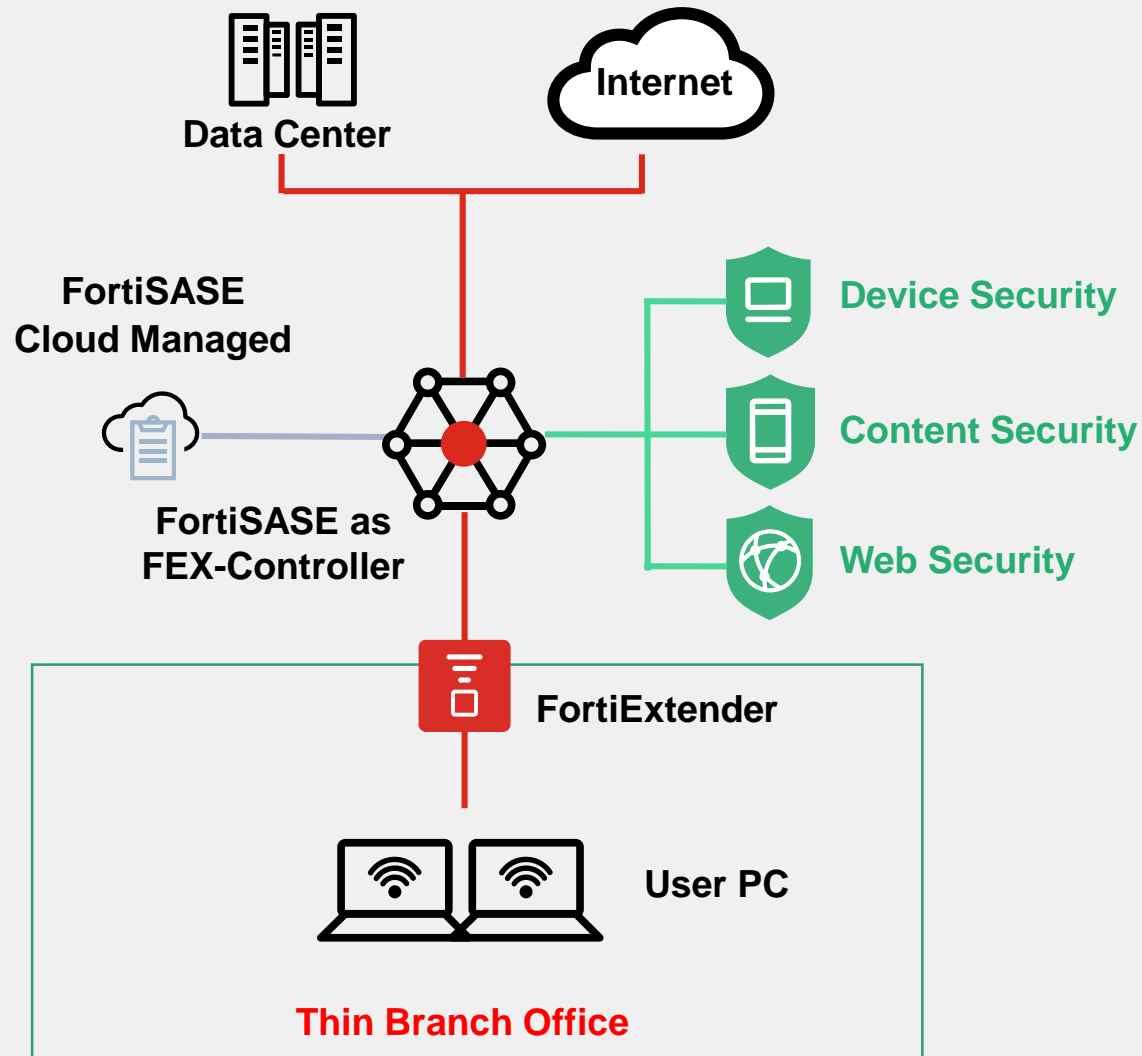
FortiSASE connection modes – Remote Users



Endpoint mode (agent mode), where endpoints connect to FortiSASE through an always-up VPN connection using **FortiClient**. In endpoint mode, you can also configure **Zero Trust Network Access**, an access control method that uses client device identification, authentication, and **Zero Trust tags** to provide **role-based application access**

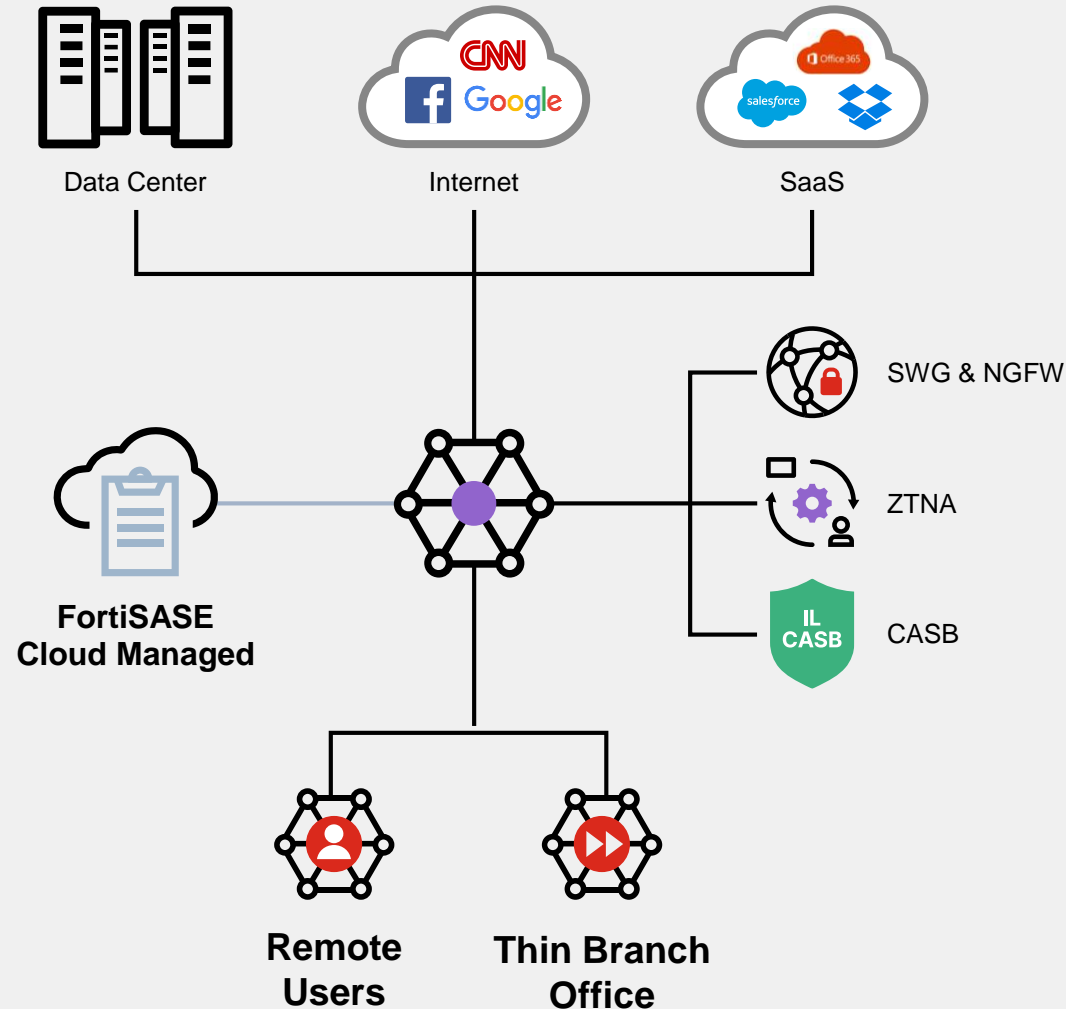
Secure Web Gateway (SWG) mode (agentless mode), where users configure **FortiSASE** as an **SWG server** on their device at the **OS level** or in a **browser (proxy settings)**. Once configured, sessions initiated in the browsers are protected by the SWG policies configured in FortiSASE

FortiSASE connection modes – Remote thin branch



Thin Edge mode - branch offices can use thin-edge devices such as FortiExtender to establish secure connections to the FortiSASE platform. All devices directly connected to the thin-edge device redirect their Internet traffic to FortiSASE

FortiSASE Key Use Cases for Remote Users



Secure Internet Access for Faster Internet
(FortiClient, Agentless, Thin Branch)

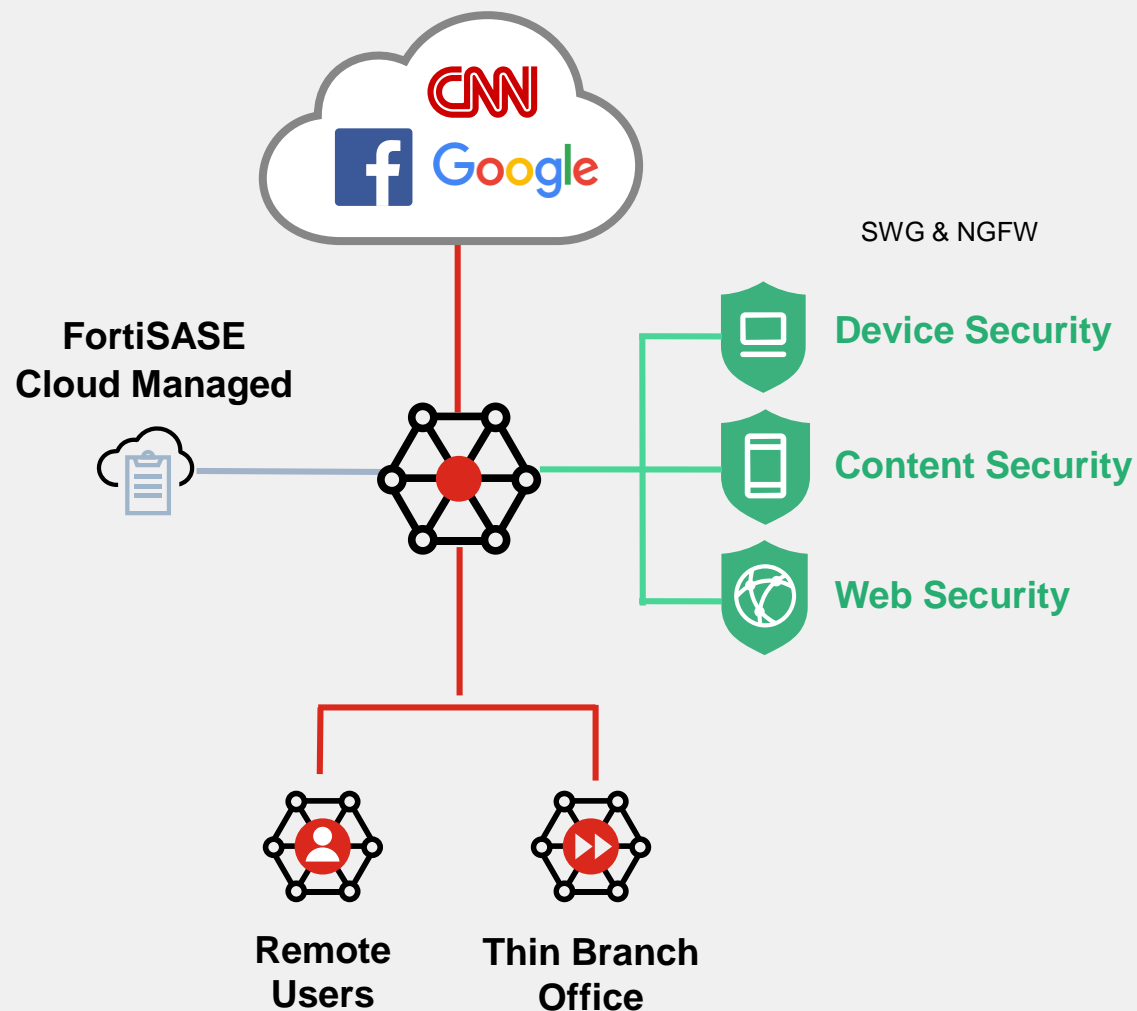


Secure SaaS Access for Visibility and Control
(FortiClient, Agentless, Thin Branch)



Secure Private Access to Corporate Apps
(FortiClient)

Use case: Secure Internet Access



Secure Internet Access



Market Leading Security as a Service

ML-enabled security, deployed close to the protected assets **powered by FortiGuard Labs**



Consistent Context Aware Policy

Centralized detection and prevention delivered from the cloud **build for hybrid environments**



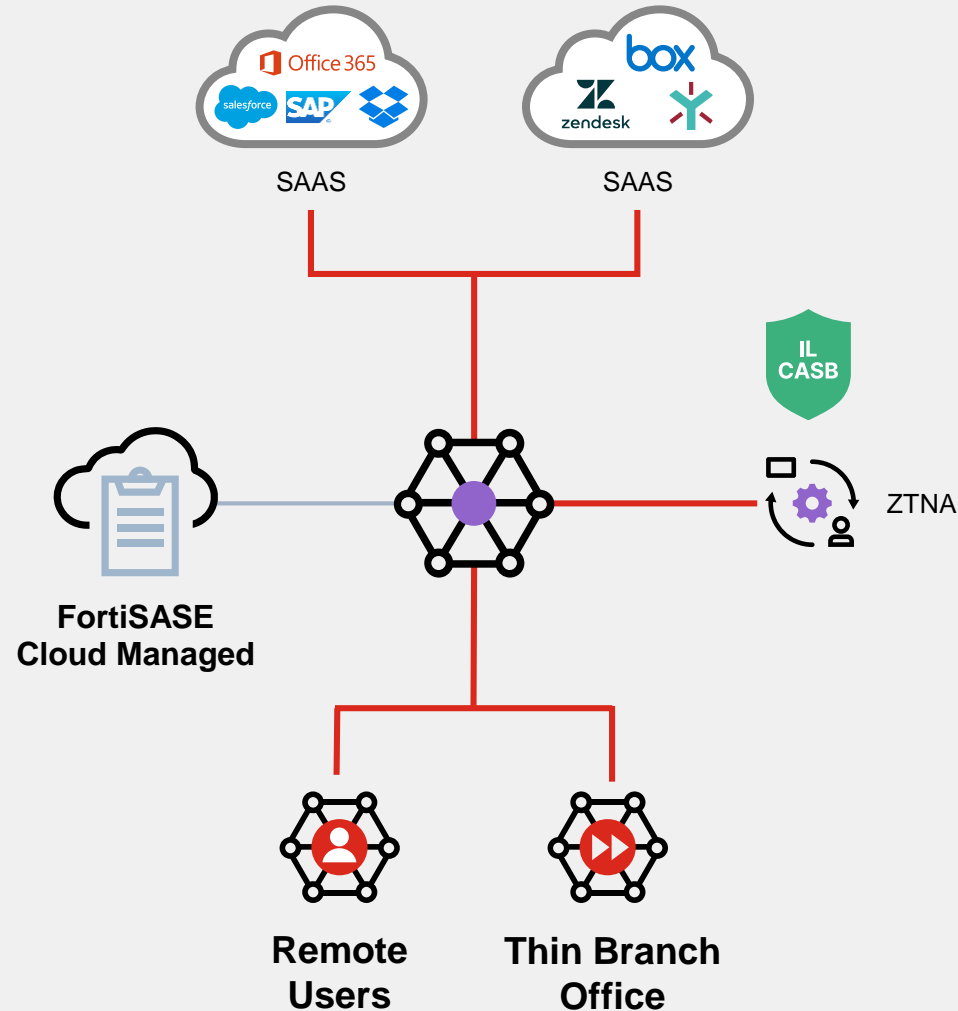
Coordinated Real-Time Prevention

Continuously assess the risks and automatically respond and **counter known and unknown threats**



Traffic redirection based on Agent (FortiClient) or Explicit Proxy (PAC file) or Lan Extension (FortiExtender)

Use Case: Secure SaaS Access for Visibility & Control



Secure SaaS Access



In-line CASB for Cloud App Control

Cloud Application control and granular activity visibility along with threat protection and reporting



API based CASB for Sanctioned Apps

Cloud Application Access control, Compliance reporting and Shadow IT control with API based CASB



Unified Agent Benefits

FortiClient Agent covers all the use-cases from SASE, ZTNA, In-line CASB, API based CASB and EPP

Comprehensive Cloud-Delivered Security



APP

Application Control



DNS

DNS Filtering



SSL

SSL Inspection



URL

Web Filtering



IPS

**Intrusion Prevention
System**



FF

File Filter



AV

Anti-Virus



DLP

**Data Loss
Prevention**



SBX

Sandboxing



FORTIGUARD

Security Profile Group – add security functionality

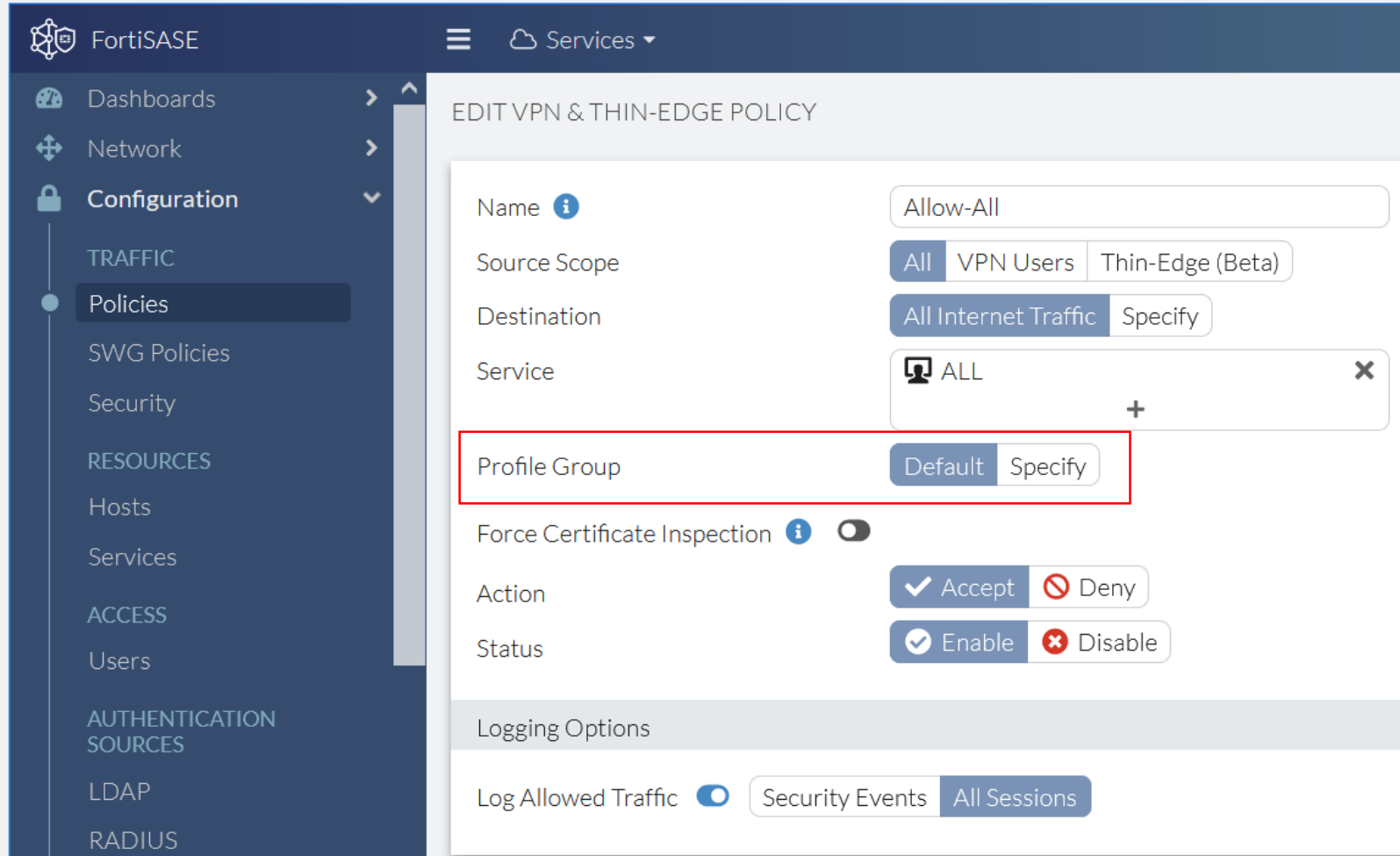
The screenshot displays the FortiSASE Security Profile Group configuration interface. The left sidebar shows the navigation menu with sections like Dashboards, Network, Configuration, TRAFFIC, Policies, SWG Policies, Security, RESOURCES, Hosts, Services, ACCESS, Users, AUTHENTICATION SOURCES, LDAP, RADIUS, VPN User SSO, SWG User SSO, ENDPOINTS, Profile, Tagging, ZTNA Access Proxies, System, and Analytics. The main content area shows the configuration for a Security Profile Group named 'SWG' (Outbound). The interface is divided into eight panels, each representing a different security module:

- AntiVirus:** Shows a table with 'Threats' (No Data) and 'Inspected Protocols' (HTTP, SMTP, POP3, IMAP, FTP, CIFS) with status indicators (green checkmarks).
- Web Filter:** Shows a table with 'Threats' (No Data) and 'Filters' (Allow, Block, Exempt, Monitor, Warning, Disable) with counts (57, 10, 0, 8, 16, 2).
- Intrusion Prevention:** Shows a table with 'Threats' (No Data) and 'Intrusion Prevention' (Recommended: Scanning traffic for all known threats and applying the recommended action).
- File Filter:** Shows a table with 'Threats' (No Data) and 'File Types' (Block, Monitor) with counts (0, 0).
- Data Leak Prevention:** Shows a table with 'Threats' (No Data) and 'Content Filters' (Allow, Block, Monitor) with counts (0, 0, 0).
- DNS Filter:** Shows a table with 'Threats' (No Data) and 'DNS Filters' (Allow, Block, Monitor) with counts (65, 9, 17).
- Application Control:** Shows a table with 'Threats' (No Data) and 'Application Filters' (Allow, Block, Monitor) with counts (19, 0, 0). A warning message states: '111 cloud applications require SSL Deep Inspection.'
- SSL Inspection:** Shows a table with 'Threats' (No Data) and 'SSL Inspection' (Certificate Inspection: SSL certificates are inspected to categorize traffic. No decryption of traffic is performed).

Each panel includes 'View All', 'View Logs', and 'Customize' buttons. The top right corner shows the 'Profile Group: SWG' and 'Outbound' settings.



Security Policies



FortiSASE Services

EDIT VPN & THIN-EDGE POLICY

Name ⓘ Allow-All

Source Scope All VPN Users Thin-Edge (Beta)

Destination All Internet Traffic Specify

Service ALL +

Profile Group Default Specify

Force Certificate Inspection ⓘ

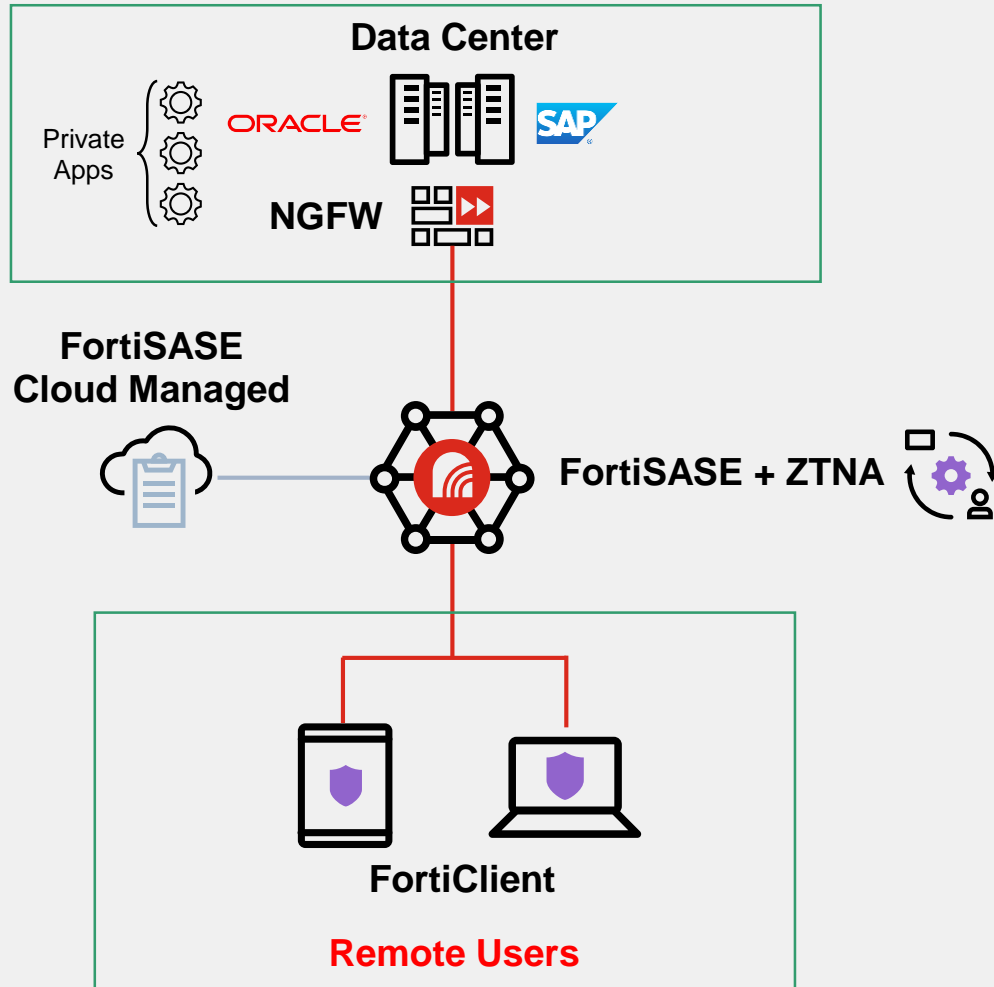
Action Accept Deny

Status Enable Disable

Logging Options

Log Allowed Traffic Security Events All Sessions

Use case: Secure Private Access to Corporate Apps (ZTNA) endpoint mode only



WHY IT MATTERS

Traditional VPN complex to enable access to private applications

HOW WE SOLVE IT

- Provision and manage ZTNA through FortiSASE management
- Allow explicit per-application access
- End point posture checks before traffic redirection

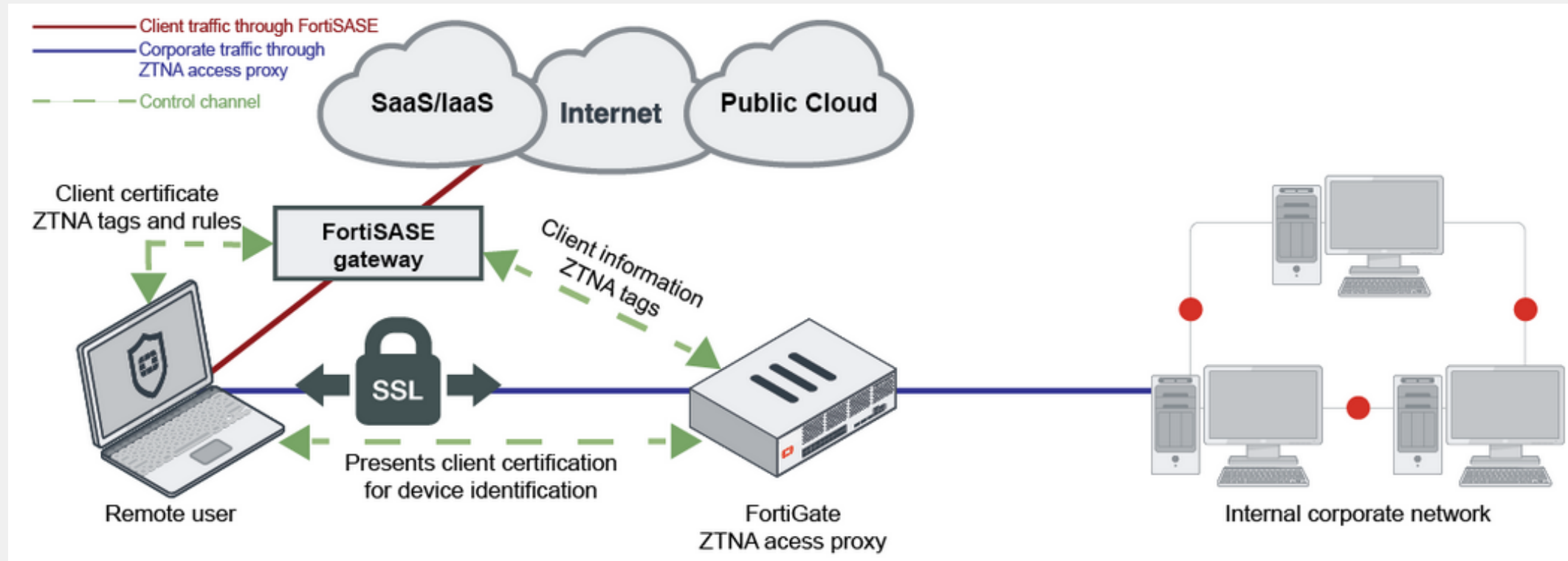
BENEFITS

- Allow Secure access to corporate applications
- Automate & Speed ZTNA adoption

LICENSE OFFERING

- No additional license required to enable ZTNA in FortiSASE

Secure Private Access to Corporate Apps (ZTNA) endpoint mode only



Tagging rule types

Operating System Windows macOS Linux iOS Android

Rule Type EMS Management

EMS Management

- AntiVirus
- Certificate
- Domain
- EMS Management
- File
- IP Range
- OS Version
- Registry Key
- Running Process
- Sandbox
- Severity Level
- User Identity
- Windows Security
- On-Fabric Status

Operating System Windows macOS Linux iOS Android

Rule Type EMS Management

EMS Management

- AntiVirus
- Certificate
- Domain
- EMS Management
- File
- IP Range
- OS Version
- Running Process
- Sandbox
- Severity Level
- User Identity
- Security
- On-Fabric Status

Operating System Windows macOS Linux iOS Android

Rule Type EMS Management

EMS Management

- AntiVirus
- Certificate
- EMS Management
- File
- IP Range
- OS Version
- Running Process
- Sandbox
- Severity Level
- User Identity
- On-Fabric Status

Operating System Windows macOS Linux iOS Android

Rule Type EMS Management

EMS Management

- EMS Management
- IP Range
- OS Version
- User Identity
- On-Fabric Status

Operating System Windows macOS Linux iOS Android

Rule Type EMS Management

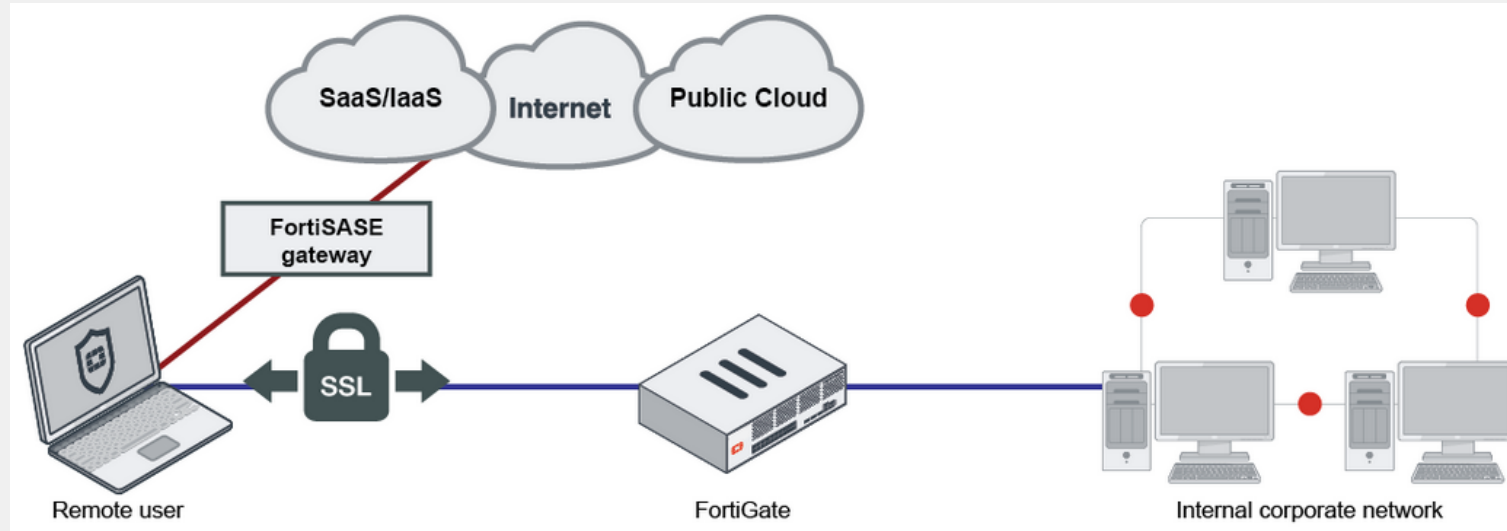
EMS Management

- EMS Management
- IP Range
- OS Version
- User Identity
- On-Fabric Status



Secure Private Access to Corporate Apps

SWG mode



For organizations that already use VPN for remote access and want to secure their remote clients from malware and malicious attacks, endpoints can use SWG mode to secure Internet access through the FortiSASE SWG while using VPN connections to an NGFW to remotely access protected networks

FortiClient only tunnels traffic for the corporate network by using SSL VPN split tunneling

Logging

The image displays three overlapping screenshots of the FortiSASE user interface, illustrating the logging and monitoring capabilities. Red boxes highlight specific navigation paths and dashboard sections.

Top Screenshot: Shows the 'Outbound Traffic' dashboard, which displays 'Traffic from internal network to external network'. The navigation menu on the left has 'Analytics' expanded, with 'LOGS' and 'Traffic' highlighted.

Middle Screenshot: Shows a dashboard with six security services: AntiVirus, Web Filter, Intrusion Prevention, File Filter, Data Leak Prevention, and DNS Filter. The navigation menu on the left has 'Analytics' expanded, with 'LOGS' and 'Security' highlighted.

Bottom Screenshot: Shows a dashboard with three event categories: VPN Events, User Events, and Endpoint Events. The navigation menu on the left has 'Analytics' expanded, with 'LOGS' and 'Events' highlighted.

Logging and monitoring are useful components to help you understand what is happening on your network, and to inform you about network activities, such as a virus detection, visit to an invalid website, intrusion, failed login attempt, and others.



Monitoring

FortiSASE

Services

Dashboards

Status

Security

+

MONITOR

FortiView Sources

FortiView Thin-Edge

FortiView Destinations

FortiView Applications

FortiView Cloud Applications

FortiView Websites

FortiView Policies

FortiView Sessions

FortiView VPN

FortiView Threats

FortiView Sources

0

05:2005:2505:3005:3505:4005:45

Drilldown

+ 🔍 Search filterable columns

User

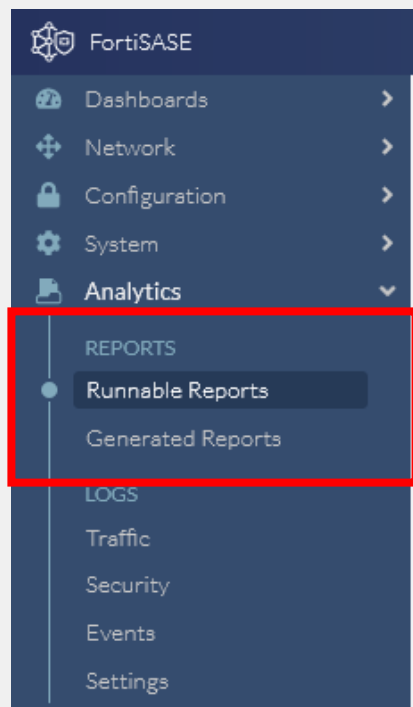
Threat Score ▼

Dashboard	Usage
Sources	Displays sources by traffic volume and drilldown by source.
Destinations	Displays destinations by traffic volume and drilldown by destination.
Applications	Displays applications by traffic volume and drilldown by application.
Cloud Applications	Displays cloud applications and drilldown by application.
Web Sites	Displays websites by session count and drilldown by domain.
Policies	Displays policies by traffic volume and drilldown by policy number.
Sessions	Displays sessions by traffic source.
VPN	Displays VPN connections by user.
Threats	Displays threats and drilldown by threat.

+ Adding a custom monitor



Reporting



Title	Description
Application	
Application Risk and Control	Risks introduced by applications on endpoints, and efforts to control those risks. Applications are organized into categories, and the report includes information, such as bandwidth by app, web categories, vulnerability exploits, virus, botnet, adware malicious attacks, and file transfers.
Bandwidth and Applications Report	Traffic, bandwidth, and sessions used on endpoints by users and applications. Also includes a summary of destinations accessed by the user and applications.
Cyber-Bullying Indicators Report	Users exhibiting behavior that aligns with common cyberbullying indicators, such as use of offensive phrases on social media.
High Bandwidth Application Usage Report	Applications with high bandwidth usage that might affect network performance. This report focuses on the following types of applications: <ul style="list-style-type: none">• Peer-to-peer, such as BitTorrent, Xunlei, Gnutella, and Filetopia• File sharing and storage applications, such as Onebox, Google Drive, Dropbox, and Apple Cloud• Voice or video applications, such as YouTube, Skype, Spotify, Vimeo, and Netflix
Self-Harm and Risk Indicators Report	Users exhibiting behavior that aligns with common self-harm and risk indicators, such as use of risky terms on social media.

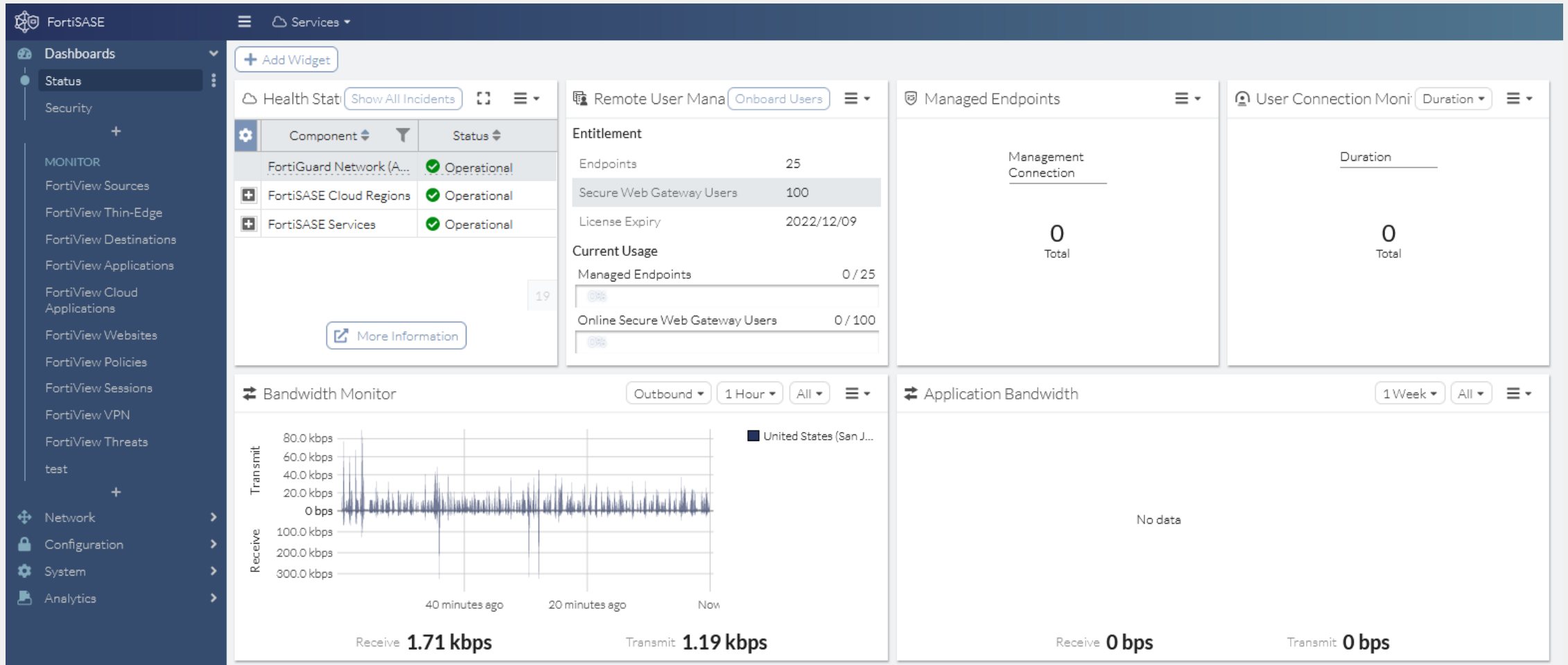
Security	
Cyber Threat Assessment	Risk of applications on endpoints to cyber threat. Includes a review of application visibility and control, threat detection, threat prevention, and recommended actions.
Security Events and Incidents Summary	Security-related events or incidents collected by FortiSASE.
Threat Report	Malware and botnet attempts on endpoints. Includes detected malware and botnets. Also includes blocked intrusions, sources, and a timeline of the attempted intrusions as well as a severity rating of the blocked intrusion.
VPN Report	VPN traffic on endpoints, including authenticated and failed user logins as well as top VPN users. Identifies SSL VPN tunnels and users as well as web mode by bandwidth and duration.
Web Usage Report	Web usage on endpoints and a bandwidth summary. Includes top active users and top bandwidth usage. Also identifies users who are blocked the most from web sites.

Regularly run reports
at scheduled intervals

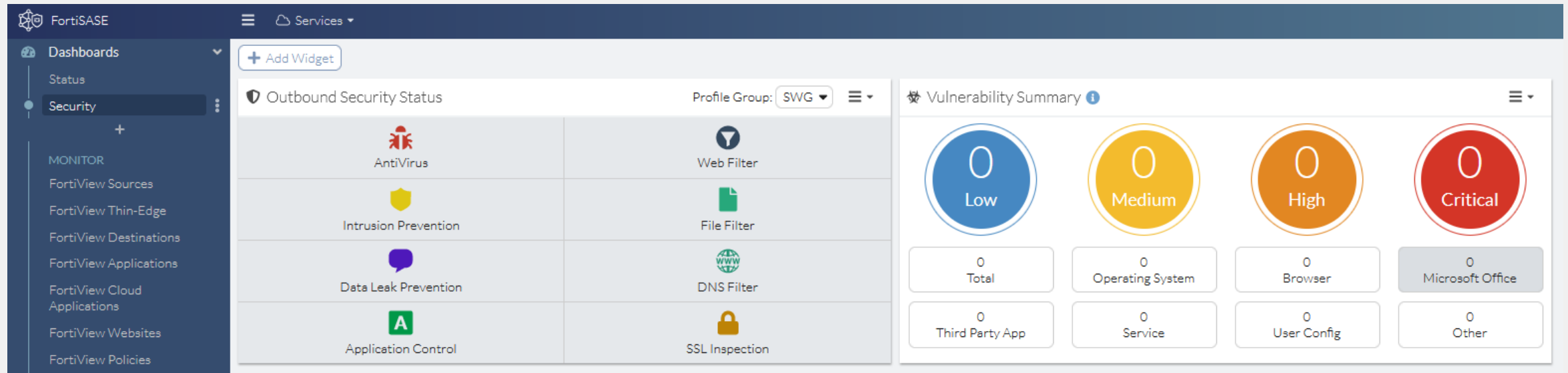
Manually run reports



Dashboard view: Status



Dashboard view: Security



FortiSASE Trusted Traffic = Split Tunneling

Type Infrastructure FQDN Local Application Subnet

Match

Search

- Infrastructure (293)
- 8x8 8X8-8X8.Cloud
- Acronis-Cyber.Cloud
- Act-on-Basic.Service
- Adobe-Adobe.Cloud
- Adobe-Adobe.Sign
- Adobe-Basic.Service
- ADP-Basic.Service
- AdRoll-Basic.Service
- Aerohive-Aerohive.Cloud
- Akamai-CDN
- Alcatel-Lucent-Rainbow

Type Infrastructure FQDN Local Application Subnet

Match

Search + Create

- IPv4 Host (7)
- Unspecified (7)
- FortiClient
- gmail.com
- login.microsoft.com
- login.microsoftonline.com
- login.windows.net
- wildcard.dropbox.com
- wildcard.google.com

Type Infrastructure FQDN Local Application Subnet

Match

Search + Create

- IPv4 Host (0)
- IPv4 Host Group (0)

Traffic configured as trusted traffic is excluded from the FortiSASE VPN tunnel and redirected to the endpoint physical interface

Type Infrastructure FQDN Local Application Subnet

Match

An application can be specified by its name, full path or the directory where it is installed. Environment variables (e.g. %programfiles%, %appdata%) can be used in file and directory path.

For example:
Application Name: chrome.exe
Full Path: C:\Program Files\Internet Explorer\iexplore.exe
Directory: C:\windows\ (must end with "\\")



FortiSASE License

- **User-based:** this allows users to connect with multiple devices (up to 3) concurrently (agentless or agent-based)
- **Endpoint-based:** simplest option allows customers to purchase FortiClient-based SASE subscription for corporate devices. This license enables SASE access, with Endpoint Protection Platform (EPP), VPN, and ZTNA components available on each device
- **Thin Edge:** enables customers to connect branch offices to FortiSASE with an optional bandwidth add-on subscription



Варто замислитись

1

How are you securing remote users access to Internet ?

2

How are you securing access to corporate applications ?

3

Do you have consistent Security Policy for users on and off network ?

4

Do you have dynamic policy based on posture endpoint ?



Переваги FortiSASE

- Не треба розгортати та підтримувати рішення у замовника (cloud)
- Ідентичність політик безпеки для on-net та off-net користувачів (FOS)
- Динамічне налаштування доступу до Corporate App на основі оцінки пристроїв (ZTNA)
- Єдине ПЗ (агент) на пристроях користувачів для Internet та Corporate App (FCL)
- Централізоване керування ПЗ безпеки на пристроях користувачів (EMS-FCL)
- Всеохоплюючий контроль безпечного доступу користувачів до Internet
- Динамічне налаштування BW у FortiSASE cloud
- Зменшення затримки у деяких випадках (trip)
- Дуже схожий GUI до FOS
- OPEX замість CAPEX



FORTINET®