Forcepoint ONE

Zero Trust Network Access

Forcepoint ONE Zero Trust Network Access (ZTNA) is one of the three foundational gateways of the Forcepoint ONE all-in-one cloud platform. It controls access to individual applications hosted behind a firewall, without the need for virtual private networks (VPNs), while providing data loss prevention (DLP) and malware protection for private web-based applications.

Key Benefits

- Eliminates the need for VPNs while proving access to individual applications – not the entire private data center
- 99.99% verified uptime since 2015
- Auto-scaling and over 300 points of presence on AWS minimizes latency and maximizes throughput
- Unified administration console reduces repetitive and redundant configuration management
- Unified managed device agent for CASB, SWG, and ZTNA simplifies deployment
- Active Directory sync agent accelerates user on-boarding
- Data-in-motion scanning blocks malware and data exfiltration between users on any device and any private web-based application.
- Field Programmable SASE Logic can block specific HTTP/S request methods resulting in granular control of any element in a private web app web page
- File level encryption of structured data ensures data privacy and data sovereignty without completely blocking access to data

Forcepoint ONE ZTNA Architecture

The Forcepoint ONE ZTNA requires the installation of a Forcepoint ONE ZTNA connector for each private data center hosting one or more private applications. Once installed, users can access web applications hosted in that data center from any device supporting a modern browser. Access to non-web applications hosted in the private data center is supported from any Windows or Mac with the Forcepoint ONE unified agent installed.

ZTNA Connector

The Forcepoint ONE ZTNA connector software is deployed as a cluster of load balanced VMs behind the firewall of your private data center with each VM running the connector software in a Docker container.

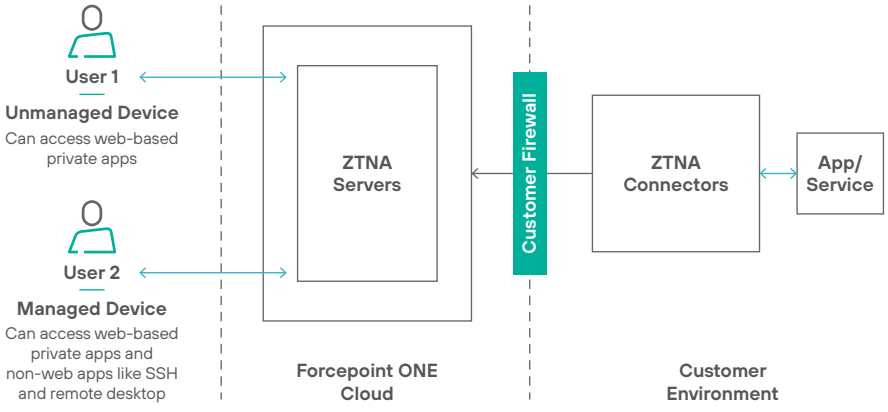

Figure 1: Forcepoint ONE ZTNA Connector Architecture.

The ZTNA connector initiates an encrypted connection to a corresponding ZTNA server in a nearby Forcepoint ONE local edge data center on AWS. Because the connection is initiated by the ZTNA connector, no inbound ports need to be opened in the private data center firewall.

Simplified ZTNA Connector Setup

ZTNA connector setup is as easy as 1, 2, 3.

1. Create a location object for the private data center through the admin portal.
2. Download and install the ZTNA connector OVA or create your own CentOS AMI by downloading the ZTNA creation script from the admin portal or through a wget command executed from the command line of the Linux system used to create the AMI.
3. After deploying the ZTNA connector VM in your private data center, run the setup script on the VM and provide the necessary parameters so the ZTNA connector can connect to the nearest Forcepoint ONE ZTNA server.

Once this is done, you can add private web applications through the admin portal by referencing the name of the location object associated with that private data center.

Forcepoint ONE ZTNA Features

Forcepoint ONE ZTNA supports both web-based and non-web applications.

Private Web-Based Application Access

Private web-based applications are handled by the ZTNA gateway in a fashion similar to how the agentless reverse proxy CASB handles managed SaaS applications. Once a web-based private application is added through the admin portal, the administrator can build the same type of proxy policies used for managed SaaS applications with the same types of upload and download DLP policies used to control movement of sensitive data and malware. And for web-based private applications using structured data, field level encryption is also supported.

From the end user perspective, web-based private applications are accessed by clicking on the corresponding tile in the user portal the same way one can access a managed SaaS application. In the user portal, private web-based applications are indicated by the destination field displayed in the upper left of the tile and the private data center location name in the lower left as shown below.

Private Non-Web Application Access

The ZTNA gateway also supports controlled access to non-web private applications such as SSH and RDP. This access requires the Forcepoint ONE unified agent for Windows or macOS on the user device. Once installed and configured, users simply access the app from the command prompt as they normally would using the IP address or server name. The ZTNA gateway will automatically route the connection through the appropriate ZTNA connector to the destination server.

Forcepoint ONE Platform Features

The Forcepoint ONE ZTNA gateway additionally supports these features built into to the Forcepoint ONE platform:

- → **Platform-level contextual access control.** Users cannot be granted access to any of the three foundational gateways unless they are authenticated according to Forcepoint ONE login policies factor in user location, device type, device posture, user behavior, and user group. When user login through a new device is detected, or "impossible travel" based on client IP address is detected, the user can be presented a muti-actor authentication (MFA) challenge to prevent use of stolen credentials.
- → **Unified management console** for configuration, monitoring, and reporting for SWG, CASB, and ZTNA. Lets administrators reuse DLP match patterns across SWG, CASB, and ZTNA for private web applications, and see a consolidated view of all traffic and anomalies.
- → **Unified on-device agent** for Windows or MacOS with unique auto-generated and auto-rotated certificates.
- → **Active Directory Sync Agent** to synchronize your current AD users and groups with Forcepoint ONE users and groups.
- → **Auto-scaling, distributed architecture on AWS** with over 300 points of presence resulting in 99.99% verified service uptime since 2014.

Figure 2: Forcepoint ONE user portal showing both managed SaaS (top) and private web apps (bottom).

Forcepoint ONE ZTNA Features and Benefits

FEATURE	BENEFIT
Auto-scaling, distributed architecture on AWS with over 300 POPs worldwide.	→ 99.99% uptime. → Minimal latency: often even faster than direct application access. → Allows in-line proxying of Slack traffic without timeouts.
Integration with any SAML-compatible IdP in SAML relay or ACS proxy mode. Optional built-in IdP using Microsoft ADFS.	→ Flexible deployment. → Denial of service protection when using SAML r elay mode.
Active Directory Sync Agent. Synchronizes your current AD users and groups with Forcepoint ONE users and groups.	→ Leverages your existing Microsoft AD instance to quickly onboard users and maintain the groups they are assigned to.
Contextual access control based on user group, device type, location, or time of day, with escalation to multi-factor authentication based on "impossible travel," unauthorized location, or unknown device. Additional layer of access control for individual websites or applications based on user group, device type, or location.	→ Detects and blocks suspicious login attempts. → Reduces risks associated with stolen passwords. → Segments users based on risk and need to access.
Single unified agent for on-device SWG, CASB forward proxy, and ZTNA for non-web applications. Includes support for deployment through MDM systems and uses self-generated auto-rotated certificates.	→ Simplifies agent deployment. → Enhances security. → Reduces IT overhead.
Single administrator console for managing all system capabilities across all applications, users, and devices.	→ Reduces complexity and time to value. → Increases visibility and control.
DLP and malware scanning for data in motion. Scans file attachments downloaded from or uploaded to any web-based app or website for malware or sensitive data and logs and blocks the transfer as appropriate.	→ Stops data loss and spread of malware in transit between users and any corporate SaaS application.
Field Programmable SASE Logic. Monitors, logs, and optionally blocks any HTTP/S request method based on any portion of the request method.	→ Fine-grained control of any element in any web page of a private web-based application.
File level encryption of structured data in web-based private applications	→ Ensure data privacy and data sovereignty without completely blocking access to data.
Detailed reporting of private web-based application traffic.	→ Complete visibility of access to private a web-based applications including those accessed from unmanaged devices.