SOLUTION BRIEF

Improve Application Access and Security With Fortinet Zero Trust Network Access

Executive Summary

The massive shift from working in an office to working at home has highlighted many security and connectivity challenges. In addition, today's networks are highly distributed with resources spread across data centers and multiple clouds. It's critical for organizations to enable secure access from anywhere to any application—while applying consistent security policies. That's why today's enterprises need to evolve remote access from traditional virtual private networks (VPNs) to a zero-trust network access (ZTNA) solution.

Fortinet ZTNA simplifies secure connectivity and reduces the attack surface. Users are authenticated and verified before they are allowed to access a particular application. The solution includes a set of products that integrate into the Fortinet Security Fabric, enabling easy management and end-to-end visibility.

Gartner predicts that by 2023, 60% of enterprises will phase out traditional VPNs and use a ZTNA model.[1]

Fortinet ZTNA Advantages

Building a zero-trust network access solution requires a variety of components—a client, a proxy, authentication, and security. But in most organizations, these solutions are provided by different vendors. The components often run on different operating systems and use different consoles for management and configuration, so establishing a zero-trust model across vendors is nearly impossible.

With Fortinet, not only can you easily establish zero-trust access through one vendor but also with one operating system. FortiOS 7.0 updates turn an organization's existing Fortinet infrastructure into the newest part of a zero-trust architecture. FortiGate next-generation firewalls (NGFWs) and FortiClient endpoint protection employ ZTNA capabilities with simplified management. The same adaptive, application access policy is used whether users are on or off the network. And, by building ZTNA into FortiOS, it's tightly integrated into the Fortinet Security Fabric, enabling easy management and superior visibility.

Fortinet can apply ZTNA to remote users, home offices, and other locations, such as retail stores, by offering controlled remote access to applications. It's easier and faster to initiate than a traditional VPN. This gives users a better experience while providing a more granular set of security protections. It doesn't matter if applications are in the data center, private cloud, or public cloud. Users and applications can be geographically independent and still create secure and reliable connections.

Fortinet ZTNA Components

The Fortinet ZTNA solution is made up of:

FortiGate NGFWs. These network firewalls act as the ZTNA proxy point and policy enforcement point. Deployed FortiGates, including virtual machines (VMs), can become FortiOS proxy points for the ZTNA solution. FortiGates provide the encrypted tunnel termination and the application access enforcement. FortiOS will also trigger the user verification and device risk assessment for each application session. That FortiGate will have the secure connections to the applications on-premises or in a cloud.

Existing FortiGate and FortiClient customers can use ZTNA as soon as they upgrade to FortiOS 7.0. There are no additional licensing fees.

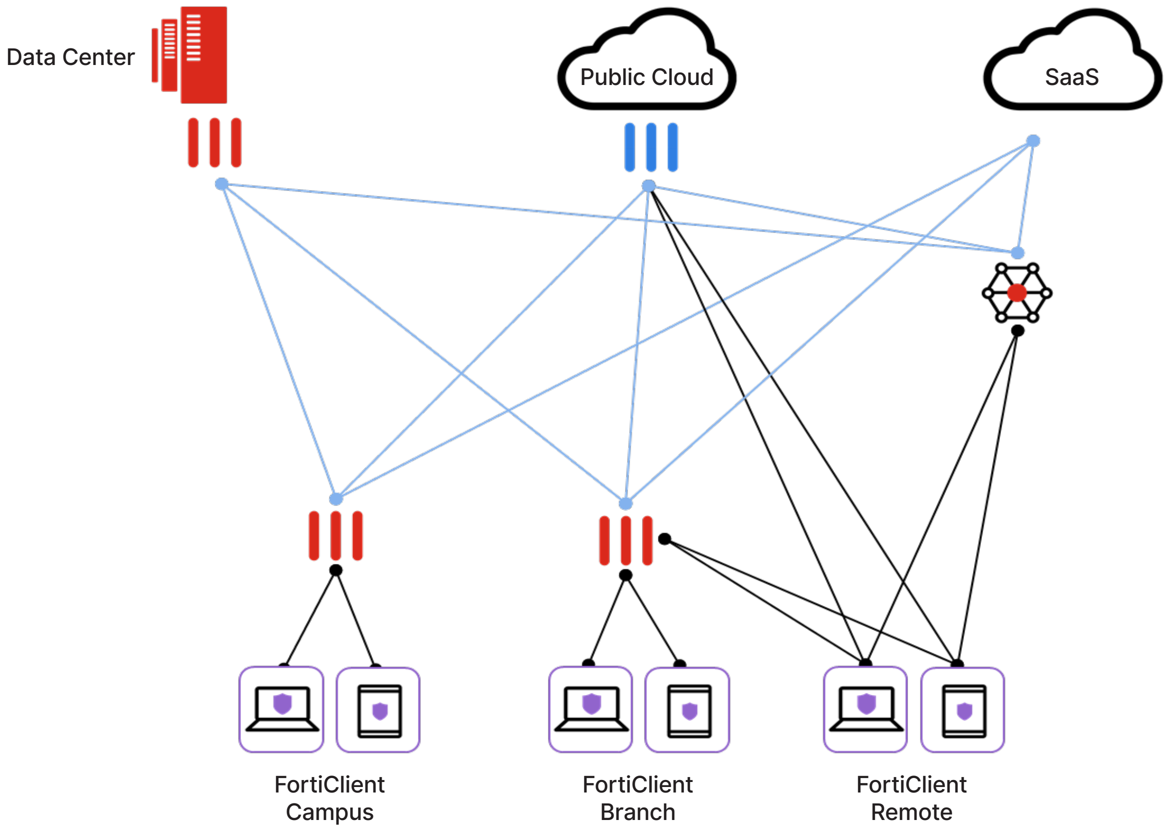
FortiManager centralized management. This Security Fabric management solution enables proxy-point configuration to be applied to all FortiGates at the same time.

FortiClient Agent. FortiClient acts as the ZTNA agent and is installed on the endpoint device. It creates automatic, encrypted ZTNA tunnels to the ZTNA enforcement point/proxy point (FortiGate).

FortiClient Enterprise Management Server (EMS). EMS plays the critical role of configuring the ZTNA agents to manage the ZTNA solution. It lets them know which FortiOS proxy point they should connect to.

Fortinet identity and access management (IAM). This solution provides the services necessary to securely confirm the identities of users and devices as they enter the network. It includes:

- **FortiAuthenticator** to provide centralized authentication services, including single sign-on (SSO)
- **FortiToken** to confirm the identity of users by adding a second factor (two-factor authentication)



How It Works

The Fortinet solution enables ZTNA capabilities by leveraging new features in FortiOS 7.0 and by using FortiClient as the ZTNA agent. To protect traffic over the internet, the FortiClient ZTNA agent on the device creates an encrypted, secure tunnel from the device to the ZTNA enforcement point (FortiGate).

This tunnel is created on-demand, transparent to the user, which solves a major pain point of VPN remote access. Because everyone on the network is no longer considered automatically trusted, the same tunnel is created whether the user is on or off the network.

This architecture has benefits on the application side, as well. Because the user is connecting to the FortiGate and then proxying that connection to the application, the application can exist on-premises, in a private cloud, or in a public cloud—all while hidden from the internet. The application only needs to establish a connection with the FortiGate, keeping it hidden from prying hackers or bots.

Secure Remote Access for Today’s Distributed Networks and Users

Fortinet makes it easy to transition from traditional VPN to ZTNA. With the technology built into the FortiOS operating system, delivering consistent and secure access, regardless of user or application location, is simplified. It’s a better experience for the end-user and easier to manage for the network admin. Moreover, the attack surface is reduced via the ongoing verifications and proxy-ed applications. The Fortinet ZTNA solution delivers more secure remote access than a traditional VPN, while enabling a better user experience.

Fortinet ZTNA does not require secure access service edge (SASE) services. However, Fortinet SASE can become FortiOS proxy points when they shift to FortiOS 7.0. SASE and ZTNA services will be able to be delivered alongside each other.

- ZTNA will provide secure access and application access control.
- SASE will provide the Firewall-as-a-Service (FWaaS), sandboxing, data loss prevention (DLP), secure web gateway (SWG), and malware protection, as well as the network peering.

[1] Mike Wronski, “Since Remote Work Isn’t Going Away, Security Should Be the Focus,” Dark Reading, September 24, 2020.

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

March 2, 2021 10:27 AM

D:\Fortinet\Work\2021\0302\sb-zero-trust-network-access

911211-0-0-EN