SOLUTION BRIEF

Zero-Trust Access for Comprehensive Visibility and Control

Executive Summary

Zero-Trust Access (ZTA) solutions exist for nearly every part of the network. However, a piecemeal approach to ZTA control leaves security gaps and is costly and cumbersome to manage.

The Fortinet Zero-Trust Access (ZTA) framework leverages a tightly integrated collection of security solutions that enable organizations to identify and classify all users and devices seeking network access, assess their state of compliance with internal security policies, automatically assign them to zones of control, and continuously monitor them, both on and off the network.

Components of the Fortinet Zero-Trust Access Control Framework

- **FortiAuthenticator** user identity management server
- **FortiToken** two-factor authentication token
- **FortiNAC** network access control
- **FortiClient** advanced endpoint telemetry

Introduction

"Zero trust" has become a buzzword in recent years, adopted by many different technology vendors. ZTA is an important pillar of an overall platform strategy that combines ZTA with security-driven networking, dynamic cloud security, and artificial intelligence (AI)-driven security operations. When organizations permit access under ZTA constraints, they confine users to the resources that are necessary for their role only. ZTA also stipulates the identification, monitoring, and control of networked devices, which are often more numerous than users.

With decades of experience in helping enterprises maintain security coverage for their rapidly expanding networks, Fortinet offers a highly effective ZTA framework that delivers visibility and control in three key areas: users on the network, devices on the network, and those users' and devices' offline activities.

Effective and Practical Identity and Access Management

Both legitimate network users and bad actors command the CISO's attention, whether they are driving business success or jeopardizing it. For this reason, user identity management is a cornerstone of the Fortinet Security Fabric. Organizations can achieve complete user visibility and effective access policy enforcement with the Identity and Access Management (IAM) portion of the ZTA framework:

- **FortiAuthenticator** serves as the hub of authentication, authorization, and accounting (AAA); access management; single sign-on (SSO); and guest management services. It establishes user identity through logins, certificates, and/or multi-factor inputs. FortiAuthenticator shares these inputs with role-based access control (RBAC) services to match an authenticated user to specific access rights and services. FortiAuthenticator also supports Security Assertion Markup Language (SAML) implementations, enabling users to securely access Software-as-a-Service (SaaS) solutions such as Salesforce, ADP, or Microsoft 365.
- **FortiToken** provides two-factor authentication services to FortiAuthenticator, either through a hardware token or as a mobile solution. The mobile solution is an open authorization (OAuth)-compliant one-time password (OTP) generator application for Android and iOS devices that supports both time-based and event-based tokens. The zero-footprint solution makes it easy to scale multi-factor authentication implementations across the enterprise.

Whether the organization has a Fortinet Security Fabric in place or another security infrastructure, Fortinet ZTA solutions for user identity and access management provide robust security for the Fortinet Security Fabric.

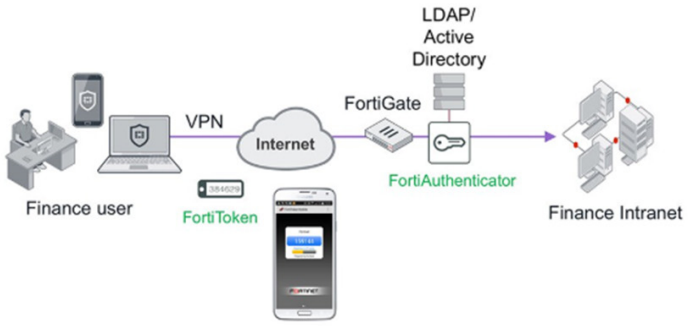

Figure 1: A typical Fortinet ZTA user identity and access management implementation.

Security for All the Things

The second objective of the Fortinet Zero-Trust Access solution is to maintain continuous visibility and access control of all devices on the network. This has been a considerable pain point for organizations. The growth in network device footprints is far outpacing the growth in network users—and certainly that of security teams. To help relieve those teams, Fortinet ZTA solutions provide integrated and automated discovery, classification, segmentation, and incident response.

Automated discovery and classification

The **FortiNAC** network access control solution accurately discovers and identifies every device on, or seeking access to, the network; scans it to ensure that it is not already compromised; and classifies it by role and function. FortiNAC can leverage existing agents to retrieve device information, but many organizations may not want to have to install agents at every location, in which case FortiNAC can communicate with the network initially, and then later identify devices.

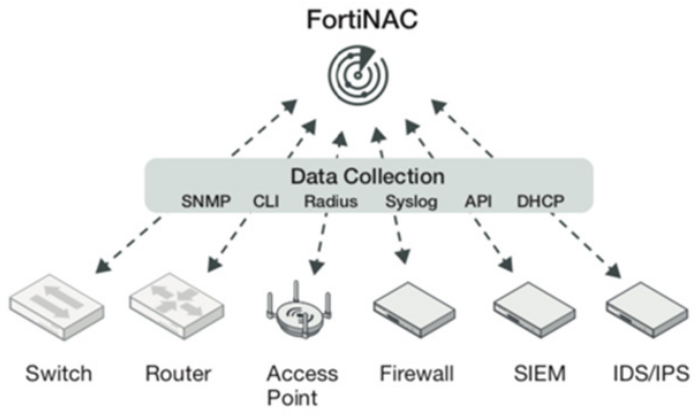

Figure 2: Supporting agentless data collection, FortiNAC provides extensive visibility into everything on the network.

Zone-of-control assignment

FortiNAC can deliver dynamic network microsegmentation in a mixed vendor environment, supporting more than 170 different vendors and 2,400 different devices and interacting with the network to keep devices in the proper network segment.

FortiNAC also integrates with FortiGate NGFWs to enable intent-based segmentation. This is an approach to segmentation based on business objectives, such as compliance with data privacy laws such as the General Data Protection Regulation (GDPR) or Payment Card Industry Data Security Standard (PCI DSS) transaction protection. With intent-based segmentation in place, security teams can tag assets with compliance restrictions, which FortiGate enforces, regardless of where the assets move in the network, helping to reduce the time and cost of compliance implementation. Organizations may also use intent-based segmentation to maintain internal access policies when they restructure the business, without having to reconfigure the network itself.

Continuous monitoring

ZTA assumes that trust is transient; a device may be certified as trusted and then subsequently infected. Also, the applications it runs may become compromised. To maintain up-to-date trust statuses for all devices on the network, FortiNAC provides ongoing monitoring, with real-time incident response. Once it detects abnormal device behavior, FortiNAC can take a variety of countermeasures, such as reassigning the device to a quarantine zone so that compromised devices cannot serve as a staging ground for threat infiltration or data exfiltration, or put devices in a remediation network segment for the user to address whatever issue has been detected.

Protecting Assets on and off the Network

For end-user devices, such as laptops and mobile phones, Fortinet extends ZTA control to both on- and off-network operation through **FortiClient**.

Secure remote access

To enable secure remote access, FortiClient provides flexible options for VPN connectivity. It supports both secure sockets layer (SSL) and Internet Protocol security (IPsec) VPNs. A split tunneling feature enables remote users on SSL VPNs to access the internet without their traffic having to pass through the corporate VPN headend, as in a typical SSL tunnel. This reduces latency, which improves user experience. At the same time, FortiClient includes protections to ensure that internet-based transactions cannot backflow into the VPN connection and jeopardize the corporate network.

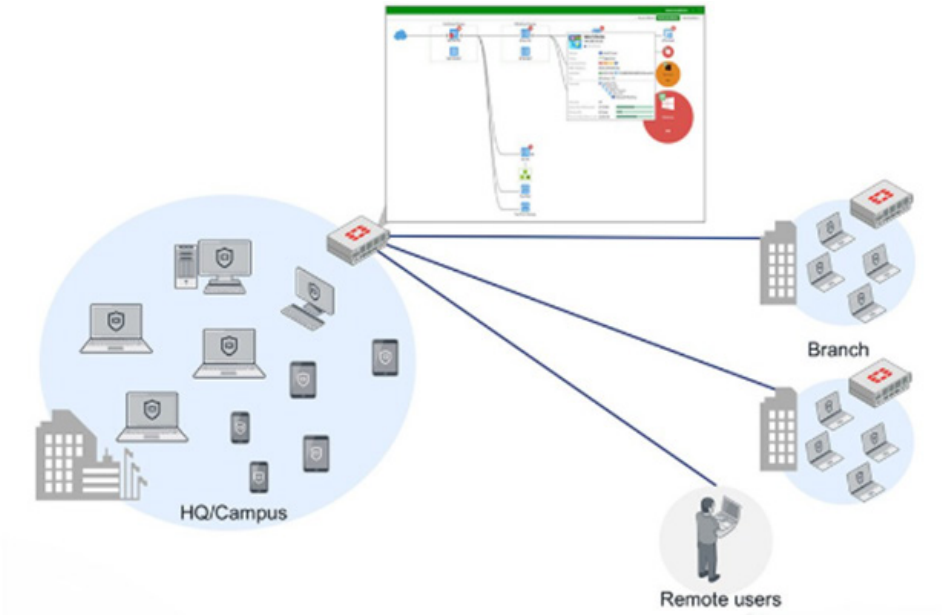

Figure 3: FortiClient ensures endpoint visibility and compliance throughout the Security Fabric. It also shares endpoint telemetry with the Security Fabric, enabling unified endpoint awareness.

Endpoint visibility

When end-user devices reconnect with the enterprise network, the **FortiClient Fabric Agent** shares endpoint security telemetry data—device operating system (OS) and applications, known vulnerabilities, patches, and security status—with FortiGate NGFWs and the rest of the Fortinet Security Fabric. This data helps the Fortinet ZTA tools refine the access rules for the devices.

Conclusion

The key to successfully implementing ZTA is to balance security and accessibility, since locking down the network is rarely an option. Fortinet ZTA solutions make it easier to accurately discover all the devices and users accessing the network and manage the associated security risks of each. This puts CISOs in a better position to support digital innovation (DI) initiatives that expand network access and leverage new network-connected technologies. Zero trust needs to be more than a buzzword or a talking point. With the right solution, it delivers true business value.

Key Benefits of the Fortinet ZTA Framework

- Complete and continuous control over who is on the network
- Complete and continuous control over what is on the network
- Integrated ZTA solution for the Fortinet Security Fabric that works equally on wired and wireless networks
- A complete, integrated solution coming from one vendor

FORTINET

www.fortinet.com

September 24, 2020 8:09 PM

693461-A-0-EN

D:\Fortinet\Work\2020\September\092420\sb-FA-zero-trust-network-access-for-comprehensive-visibility-and-control-6192020\sb-FA-zero-trust-access-for-comprehensive-visibility-and-control_092420