SOLUTION BRIEF

Zero-trust Solutions for Comprehensive Visibility and Control

Executive Summary

Zero-trust solutions exist for nearly every part of the network. However, a piecemeal approach can leave security gaps and is costly and cumbersome to manage.

Fortinet zero-trust solutions include Zero Trust Access (ZTA) and Zero Trust Network Access (ZTNA), which leverage a tightly integrated collection of security solutions that enable organizations to identify and classify all users and devices seeking network and application 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.

Fortinet Security Fabric Components Used in Zero-trust Security

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

Introduction

"Zero trust" has become a buzzword in recent years, adopted by many different technology vendors. The concept of zero trust came about because the old network security model of "inside means trusted" and "outside means untrusted" no longer works. ZTA is about knowing and controlling who and what is on your network. Role-based access control is a critical component of access management. ZTA is an important pillar of an overall platform strategy that combines zero-trust approaches with security-driven networking (SDN), dynamic cloud security, and artificial intelligence (AI)-driven security operations. The zero-trust model stipulates that organizations restrict user access to only the resources that are necessary for a given role and that they support the identification, monitoring, and control of networked devices.

With decades of experience in helping enterprises maintain security coverage for their rapidly expanding networks, Fortinet offers highly effective zero-trust solutions that deliver on the zero-trust principles of:

- Ongoing verification of users and devices
- Creating small zones of control
- Granting minimal access to users and devices

Fortinet has been assembling these necessary pieces under the umbrella of the Fortinet Security Fabric, enabling companies to move forward with zero-trust strategies that can support their journey to the cloud and work-from-anywhere trends.

Effective and Practical Identity and Access Management

Because the zero-trust model limits access granularly, it also limits the ways threat actors can gain access to and move within an organization's networks. Whenever a user or device requests access to a resource, they must be verified before access is given. That verification is based on the identity of the users and devices, plus other attributes and context, such as time and date, geolocation, and aspects of the device security posture. Another primary tenet of zero trust is to secure remote access. ZTNA connections grant access on a per-session basis to individual applications only after devices and users are verified.

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 Fortinet identity and access management (IAM) solutions that include:

- 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 solutions for user identity and access management provide robust security for the Fortinet Security Fabric.

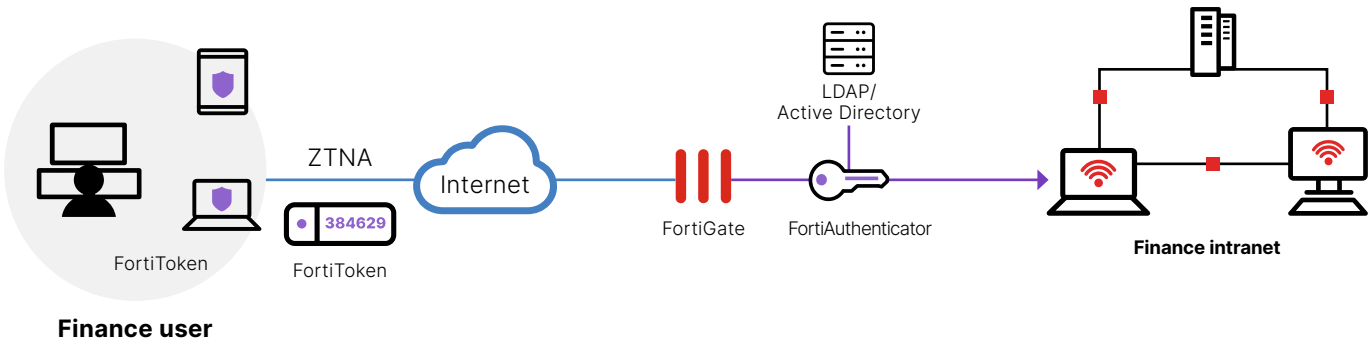

Figure 1: A typical Fortinet ZTNA user identity and access management implementation.

Security for All the Things

The second objective of Fortinet zero-trust solutions is to maintain continuous visibility and access control of all devices on the network, which has historically been a pain point for organizations. The growth in network device footprints is far outpacing the growth in network users—and certainly that of security teams. Fortinet 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.

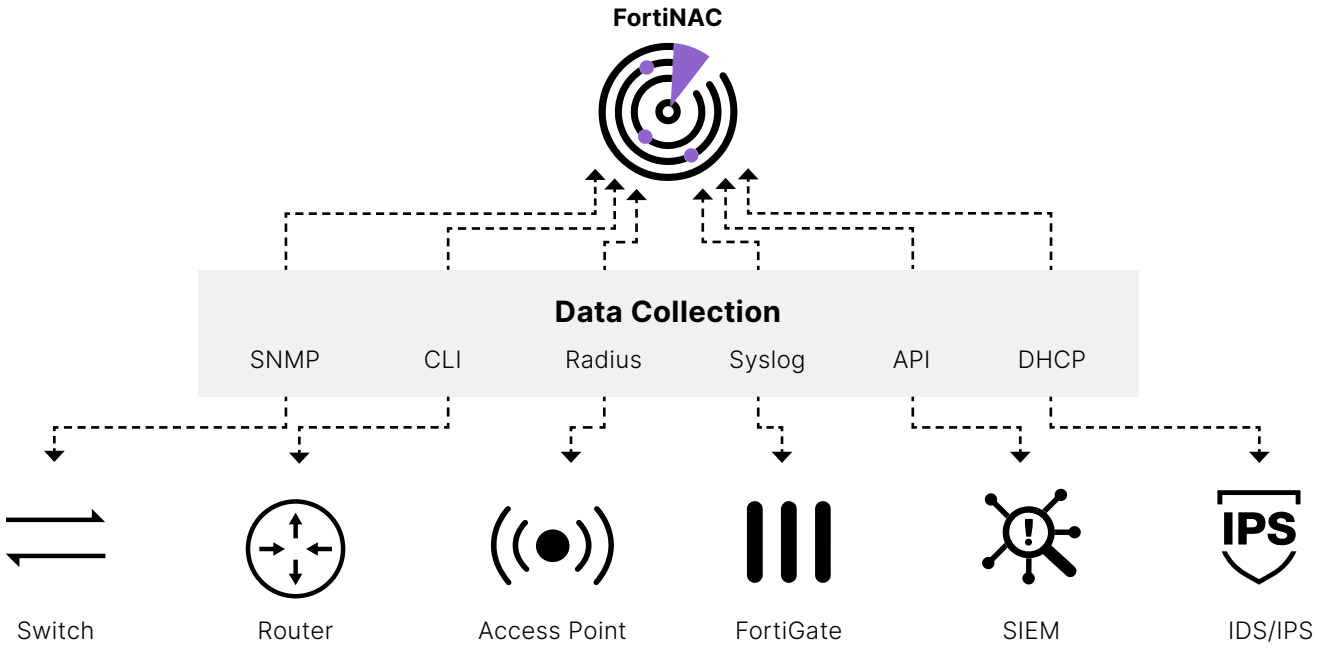

Figure 2: Supporting agentless data collection, FortiNAC provides extensive visibility into everything on the network.

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 next-generation firewalls (NGFWs) to enable intent-based segmentation. This segmentation approach is 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

The zero-trust model assumes that trust is transient. A device may be certified as trusted and then subsequently infected along with the applications it runs. 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 zero-trust access control and user and device access to applications both on and off the network through FortiClient.

Secure remote access

To enable secure remote access, FortiClient provides flexible options for virtual private network (VPN) connectivity and ZTNA. 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.

ZTNA is the evolution of the traditional VPN with better security, more granular control, and a better user experience. For many organizations, ZTNA can be a smarter choice for securely connecting a remote workforce. Unlike a traditional VPN tunnel that provides unrestricted access to the network and applications, ZTNA connections are granted to individual applications per session. Access is granted only after both the device and user have been verified. Because location is no longer a reliable indicator for access as it is with a VPN, ZTNA policy is applied whether users are on or off the network.

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. For ZTNA, the FortiClient ZTNA agent provides the device posture check and the user identification as part of the verification process as well as creating the encrypted tunnel from the device to the FortiOS proxy point.

Conclusion

The key to successfully implementing zero-trust strategies is to balance security and accessibility because locking down the network is rarely an option. Fortinet zero-trust solutions make it easier to accurately discover all the devices and users accessing the network and manage the associated security risks of each. Zero trust is more than a buzzword or a talking point. With the right solutions in place, zero trust delivers true business value.

Key Benefits of Fortinet Zero-trust Solutions

- 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
- Secure remote connections that limit application access and repeatedly verify users and devices every time an application session starts
- A complete, integrated solution from one vendor

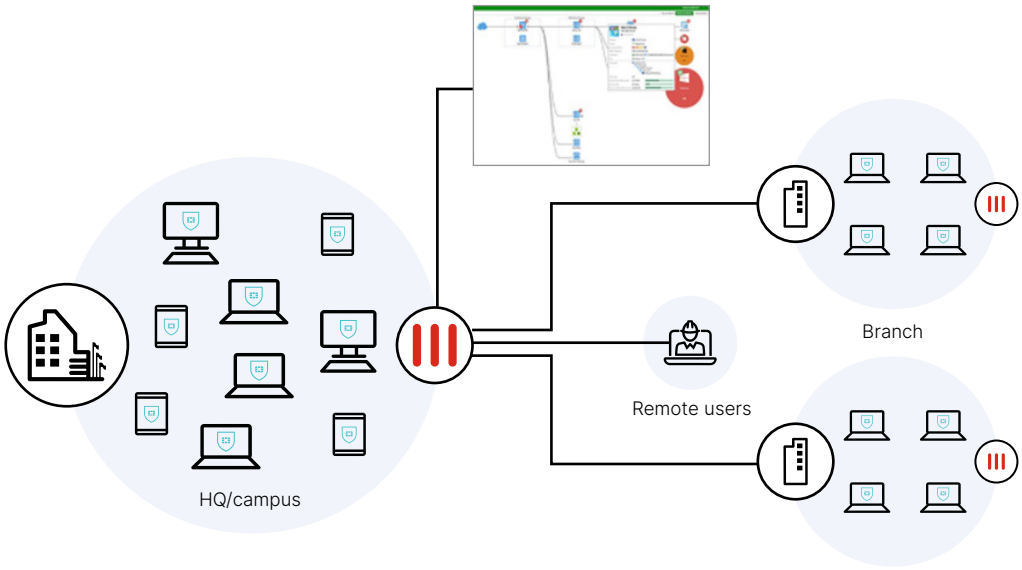

Figure 3: FortiClient ensures endpoint visibility and compliance throughout the Security Fabric. It also shares endpoint telemetry with the Security Fabric, enabling unified endpoint awareness.

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.

July 21, 2021 5:59 AM
693461-C-0-EN