# The CISO’s Guide to Effective Zero-Trust Network Access

## Providing Continuous Visibility and Control of All Devices and Users

# Table of Contents

Executive Overview ........ 3

Introduction ........ 4

Seeing and Controlling Who Is on the Network ........ 6

Seeing and Controlling What Is on the Network ........ 8

Controlling Managed Devices off the Network ........ 11

Summary ........ 12

## Executive Overview

Best practices in network access stipulate a zero-trust network access (ZTNA) approach. CISOs looking to implement ZTNA will find numerous technologies designed to meet the requirements of the National Institute of Standards and Technology (NIST) Zero Trust Architecture.[1] It can be a challenge, however, to get all these technologies to work together to prevent security lapses.

Closely following the latest standards and leveraging decades of cybersecurity experience, Fortinet has found that the most effective ZTNA strategy is a holistic approach that delivers visibility and control in three key areas: who is on the network, what is on the network, and what happens to managed devices when they leave the network.

# Introduction

As digital innovation (DI) tugs relentlessly on the reins of network security, CISOs are seeing their networks fragment and their attack surfaces expand. Because networks now have numerous "edges," it is difficult to create a single defensible boundary, rendering perimeter-based access control strategies ineffective. Furthermore, it is getting harder to distinguish between internal, trusted users and external unknown or untrusted ones; employees and contractors are too often implicated in major network breaches. Even compliant users can become vectors for attacks, as they roam on and off the network, often with their personal devices.

Consequently, CISOs have had to rethink the basis for trusting users and devices that request access to network resources. Best practices have evolved from trusting everything inside the network, to verifying once and then trusting, to trusting no device or user and providing only least-privilege access. The common shorthand for this latest access model is zero-trust network access, or "ZTNA."

The requirements of ZTNA have been refined for more than a decade following the original coining of the term. NIST's latest Zero Trust Architecture document acknowledges that ZTNA is a work in progress. So, rather than defining the specifics of the architecture, it offers a set of guiding principles and advises security professionals to think of the transition to ZTNA as a journey.

As the CISO's companion on that journey, Fortinet has developed a holistic approach for effective ZTNA. There are three pillars to this approach:.

- ZTNA solutions must provide continual visibility of devices and users connected to the network, as well as the network resources they are attempting to access.
- The solutions must be able to enforce security policies regardless of the device type, location, or method of access.
- They must be able to maintain enforcement and visibility when the devices go offline.

Networks have numerous “edges,” rendering perimeter-based access control ineffective. ZTNA is the prevailing network access paradigm, and a holistic approach is the key to success.

## Seeing and Controlling Who Is on the Network

The borderless digital enterprise supports a growing variety of users. In addition to the traditional employee-user, there are contractors, supply chain partners, and customers who require access to data and applications, which may reside on-premises or in the cloud. Regulating network resource access involves both identifying the user requesting access and verifying that the user has the authority to access the requested resources.

### Breach-resistant identification and authentication

User identities are readily compromised. Bad actors can obtain usernames and passwords either by brute force—which is often easy because passwords are commonly weak—or by social engineering tactics such as email phishing. For this reason, enterprises are adding multi-factor authentication (MFA) to their login processes. MFA includes something the user knows, such as a username and/or password, and something the user has, such as a token device that generates a single-use code or a software-based token generator. By 2024, 70% of applications are anticipated to use MFA.[2] Emerging biometric solutions—fingerprints, facial scans, and iris scans—also promise to minimize the risk of stolen credentials.

### Least-privilege authorization

The second challenge is preventing authenticated users from abusing their access privileges. To this end, CISOs should mandate least-privilege access policies, which restrict access to the minimum that a user needs, based on their role in—or relationship with—the organization. Authentication and authorization solutions should be integrated with the enterprise's network security infrastructure (and to a policy-based Active Directory database) to enable automated enforcement and easy management of least-privilege access policies.

It is also important to ensure that these security interventions do not hamper productivity or the quality of the user experience. CISOs should opt for ZTNA solutions that support single sign-on (SSO) functionality and perform with minimal latency. Both features help facilitate compliance and minimize user fatigue.

Zero-trust network access solutions should firmly enforce access control policies, while enhancing the productivity and experience of the authorized user.

## Seeing and Controlling What Is on the Network

While CISOs are rightly concerned about the noncompliant and unpredictable behavior of users, they should pay no less attention to the devices accessing their networks. These include end-user devices (desktop and mobile), networked office equipment, retail front-end systems (e.g., point-of-sale), operational technologies, and numerous distributed sensors and other devices collectively known as the Internet of Things (IoT). Growth projections for installed IoT devices vary, but most expect them to number in the billions worldwide in the coming years.

The challenge in managing all of these devices lies in their wide dispersion, the varying levels of device supervision, and the lack of support for standard communication protocols in legacy devices. CISOs can help security administrators address endpoint management challenges by giving them the tools they need to efficiently discover, categorize, and control access for everything that is on the network.

### NAC should deliver visibility in seconds

To know what is on the network at any point in time, CISOs need network access control (NAC) tools that can automatically identify and profile every device as it requests network access, as well as scanning it for vulnerabilities. During the discovery process, the NAC solution should detect MAC Authentication Bypass (MAB) attack attempts and log these incidents. It should also share the information it collects in real time with other network devices and security infrastructure components.

The NAC processes should be completed in seconds to minimize the risk of device compromise. For this reason, CISOs should be wary of solutions that rely on traffic scanning. Such solutions allow devices to connect to the network during identification. However, the scanning process takes up to half an hour, during which time the network may be compromised.

Another caveat pertains to solutions that rely on 802.1X Wi-Fi protocol. These work well for wireless networks, where every client has a supplicant as part of communication control, thus making 802.1X easy to run. However, 802.1X-based solutions are onerous to deploy on switched networks. Ideally, a NAC solution should be easy to deploy from a central location and offer consistent operation across wired and wireless networks. This will support the pace of growth that enterprises are experiencing. With the central location, the NAC solution won't require the sensors at every device location, which can drive up deployment and management costs.

## Microsegmentation enables ZTNA control

Enforcement of access control policies is essential for all devices, but it is particularly challenging with IoT devices. These are typically low-power, small-form-factor devices with no extra CPU or memory to support security processes. They also tend to feature nonstandard operating systems that aren't necessarily compatible with endpoint security tools used to secure them. Therefore, the device security is unreliable, and the network itself needs to provide the needed security.

Due to the large scale of IoT deployment, CISOs must prioritize IoT control as they consider ZTNA solutions. Access control cannot be implemented in the devices themselves, so it must come from the network. The way to do this is to microsegment the network with next-generation firewalls (NGFWs), grouping similar IoT devices together. This hardens the network in two ways. First, it breaks up the lateral (east-west) path through the network, making it harder for hackers and worms to gain access to the devices. Second, it reduces the risk that an infected device will serve as a vector through which a hacker can attack the rest of the network.

As with the other ZTNA solution components, the NGFWs should be architected so that they can process all intersegment traffic with minimal latency. This will ensure that the ZTNA device-control mechanism is not a hindrance to productivity throughout the organization.

CISOs should ensure that security administrators have the tools they need to efficiently discover, categorize, and control everything that is on the network from a central location.

## Controlling Managed Devices off the Network

One characteristic of digital enterprises is the transient nature of network connectivity and use. Cloud services have enabled ubiquitous access, which means users can roam, disconnecting their device from the network at one location and reconnecting it at another. They might also start working on one device and continue on another. Controlling managed devices when they go off-network is a challenge, because even if devices are secure the first time they connect to the network, they may be compromised while offline and infect the network when they return.

To overcome this challenge, CISOs should look at endpoint security as part of a ZTNA solution. An endpoint security solution should provide off-network hygiene control, including vulnerability scanning, web filtering, and patching policies. It should also provide secure and flexible options for virtual private network (VPN) connectivity. As with the identity management tools, the endpoint security solution should support SSO functionality for ease of use. Once an endpoint is connected to the network, the endpoint security solution should relay device status information to other network and security components for risk assessment and determining appropriate access level.

## Summary

Zero-trust access control is not a new concept. So, CISOs are likely to be inundated with advice on ZTNA technologies and solutions. Industry guidelines such as NIST SP 800-207[3] provide a realistic path to transitioning to ZTNA. Working with leading network security providers and selecting integrated and automated tools can help overcome the key challenges of ZTNA network access: knowing who and what is on the network, controlling their resource access, and mitigating the risks that such access entails.

[1] Scott Rose, et al., "Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture," NIST, February, 2020.

[2] Michael Kelley, et al., "Gartner Magic Quadrant for Access Management," Gartner, August 12, 2019.

[3] Scott Rose, et al., "Draft (2nd) NIST Special Publication 800-207, Zero Trust Architecture," NIST, February, 2020.

www.fortinet.com

693421-0-0-EN

June 24, 2020 9:02 AM

ebook-zerotrust-network-access