LEARNING MADE EASY

Fortinet Special Edition

Zero Trust Access

for dummies®
A Wiley Brand

Reducing the attack surface

Securing the new hybrid workforce

Improving application access and security

Brought to you by:

FORTINET®

Lawrence Miller

About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. This is why the world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey. The Fortinet Security Fabric mesh platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 530,000 customers trust Fortinet to protect their businesses. And the Fortinet NSE Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

Zero Trust Access

Fortinet Special Edition

by Lawrence Miller

for dummies®
A Wiley Brand

Zero Trust Access For Dummies®, Fortinet Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119- 85984-0 (pbk); ISBN 978-1-119- 85985-7 (ebk)

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Jen Bingham

Editorial Manager: Rev Mengle

Acquisitions Editor: Ashley Coffey

Content Refinement Specialist: Mohammed Zafar

Introduction

As businesses continue to embrace digital innovation, cloud applications, and the new work-from-anywhere normal, enterprise networks have become far more complicated and dispersed with an ever growing number of edges. As a result, the network perimeter has all but disappeared. As more people and devices connect to the network from more places, the traditional perimeter-based approach to security — protecting the trusted corporate network from the untrusted internet — has become increasingly ineffective.

To protect this greatly expanded attack surface from modern threats, organizations must implement a "never trust, always verify" zero-trust model that incorporates rigorous access controls across the distributed network so that users, devices, endpoints, clouds, and infrastructure are all protected.

To successfully implement a zero trust access strategy, organizations must implement tightly integrated security solutions that deliver robust identity and access management, endpoint access control, network access control, and application access control to users and endpoints working from anywhere.

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but this book assumes a few things nonetheless! Mainly, that you're a chief information officer (CIO), chief information security officer (CISO), vice president, architect, engineer, or administrator working on an enterprise security, networking, or infrastructure team. As such, this book is written primarily for technical readers with at least a basic understanding of security and networking technologies and challenges.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book and when you finish reading it, you'll have complete trust in your knowledge of zero trust!

Icons Used in This Book

Throughout this book, you will see special icons that call attention to important information. Here's what to expect.


CASE STUDY

The case studies provide best practices from organizations that have successfully used modern data sharing methods.


REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with birthdays and anniversaries!


TECHNICAL STUFF

This icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.


TIP

Tips are appreciated, but never expected — you'll appreciate these useful nuggets of information and helpful advice.


WARNING

These alerts point out the stuff your mother warned you about (well, probably not, but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.)

Beyond the Book

There's only so much space in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?" go to `https://fortinet.com`.

IN THIS CHAPTER

- Recognizing modern threats
- Going beyond traditional access control
- Defining zero-trust concepts
- Reaping the benefits of zero trust

Chapter 1
Understanding the Need for Zero Trust

In this chapter, you learn how threat actors take advantage of the disappearing network perimeter and expanding attack surface to bypass traditional access controls, and how zero trust overcomes these challenges.

Surveying the Modern Threat Landscape

In today's digital enterprise, business applications and data are dispersed far and wide, away from corporate data centers, so that users now have greater access to corporate resources using more endpoints from many locations. The rapid growth of Internet of Things (IoT) devices and corporate bring-your-own-device (BYOD) initiatives have led to a proliferation of access points and endpoint devices on the network. As a result, the traditional network perimeter is disappearing — and the attack surface is expanding. At the same time, cyberthreats are growing more prolific, and attackers' tactics and techniques are evolving and becoming more sophisticated.

REMEMBER

IDC predicts that by 2025 there will be 55.7 billion IoT-connected modified devices worldwide.

Traditional security models work under the assumption that anything inside an organization's network should be trusted. But automatically extending trust to any device or user puts the organization at risk if either is compromised, whether intentionally or unintentionally. Attackers, malware, and compromised devices that bypass edge security checkpoints often have unrestricted access to the network because of this inherent trust model. Exploits such as credential theft and malware enable attackers to gain access to legitimate accounts. Once inside the network, they can move laterally and take advantage of the trusted internal network to target an organization's resources.

WARNING

According to the Verizon 2021 *Data Breach Investigations Report* (DBIR), 70 percent of breaches in the previous year were caused by outsiders, 45 percent involved hacking, 86 percent were financially motivated, 17 percent involved some form of malware (including ransomware), and 22 percent featured phishing or social engineering.

As companies modernize their networks to accommodate remote workers, multicloud architectures, and digital innovation, their approaches to security need to change as well.

Recognizing the Limitations of Traditional Access Control

Traditional access control strategies inherently trust a user or device on the network. This notion of trust is often based on the user or device's location: If they're on the network, they're trusted. But as the network perimeter continues to disappear, it becomes increasingly impossible to secure network resources. Users are now accessing the corporate network from home offices and mobile devices. Corporate resources are also increasingly located in multiple locations, beyond the traditional network, such as private and public clouds.

To overcome the limitations of traditional access control, organizations need a solution that provides:

- Ongoing verification of users and devices.
- Granular segmentation of the network to create zones of control, which helps limit the impact of a breach and establishes more control points.
- Least-privilege access for users and devices, so users are only granted the access they need to perform their roles, which helps to limit the impact of a compromised identity or device.

WARNING

Today's networks have vast, dynamic, and in some cases, even temporary edges. The fact that many devices are often offline makes continuously assessing risk and trust even more difficult. Because there's no way to verify that users or devices on or off the network can be trusted, you should assume that every device on the network is potentially infected.

Looking at Zero-Trust Basics

The zero-trust model is a concept that was introduced by John Kindervag while working at Forrester Research in 2009. The fundamental principle underpinning zero trust is "never trust, always verify." Zero trust challenges the traditional perimeter-based security model in which a firewall protects the trusted corporate network from the untrusted internet.

To be fair, the perimeter-based model isn't as black and white as labeling things either trusted or untrusted. Over the years, the perimeter-based approach has been tweaked here and there. For example, demilitarized zones (DMZs) are typically created for public-facing websites and applications that are "somewhat trusted" — shades of gray, if you will. Virtual private networks (VPNs) are used to extend (or punch holes in, depending on your perspective) the corporate network to remote and mobile users. And virtual local area networks (VLANs) and access controls are used to segment sensitive departments, such as human resources and finance, from the rest of the network.

But the perimeter-based approach to security has an inherent drawback: It grants excessive implicit trust. Once you're connected, whether directly or using a VPN, you are then trusted alongside the rest of the internal network.

The zero-trust model moves security away from implied trust that is based on the network location of a user or device. Instead, trust is evaluated on a per-transaction basis. With zero trust, your network location or IP address no longer conveys an implication of trust. Instead, the zero-trust model requires trust to be explicitly derived from a combination of identity and context-based controls at a very granular level that grants access based on the security principles of least privilege and need to know.

Zero trust starts with a default deny posture for everyone and everything — that is, zero trust. In a zero-trust model, whenever a user or device requests access to a resource, their identity must be verified before access is granted. Verification is based not only on the identity of the user and/or device, but other attributes as well, including context (such as date and time), geolocation, and device security posture.

REMEMBER

However, access is not a "one and done" deal. Just because a user or device has been granted access to a resource doesn't mean they can roam about freely on the network. Access is granted at a very granular level. It's only given to the resource that is needed to perform a specific function for a limited time — not the entire network. A key element of the zero-trust model is that trust must be continually re-evaluated. If important attributes of the user or device change, the trust may be revoked and access to the resource removed.

Zero-trust access (ZTA) builds on the zero-trust model and focuses on knowing and controlling who and what is accessing the network. Role-based access control (RBAC) is a critical component of ZTA. Only by knowing definitively who a user is can the appropriate level of access be granted based on their role. ZTA covers user endpoints where management control and visibility are required. Aligning to the zero-trust model means implementing a least-access policy that grants the user the minimum level of network access required for their role and removes any ability to access or see other parts of the network.

TIP

In addition to knowing who and what is on the network, ZTA incorporates security for what is on the network. The ever-growing number of network-connected devices now includes IoT devices. These "headless" devices don't have usernames and passwords to identify themselves and their role on the network. Instead, network access control (NAC) solutions can be used to discover and control access for these devices. Using NAC policies, the zero-trust principle of least access can be applied to these IoT devices, granting sufficient network access to perform their role and nothing more.

Zero-trust network access (ZTNA) is an element of ZTA that controls access to applications regardless of where the user or application is located. The user may be on a corporate network, working from home, or someplace else. The application may be hosted in a corporate data center, or in a private or public cloud.

REMEMBER

ZTNA is the natural evolution of the VPN. Given the complexity of today's networks, ZTNA offers better security, more granular control, and a better user experience than a traditional VPN. You can learn more about ZTNA in Chapter 5.

Realizing the Benefits of Zero Trust

For effective security in the modern threat landscape, organizations must shift from trying to protect dynamic network perimeters to instead protecting applications and data spread across potentially billions of edges, users, systems, devices, and other critical resources. A zero-trust strategy provides comprehensive visibility and protection across devices, users, endpoint, cloud, and infrastructure with a "never trust, always verify" approach to security.

Zero trust delivers the following benefits for organizations:

- **Reduces risk:** When you automatically extend trust to any device or user in your network, you put your organization at risk when either becomes compromised, whether intentionally or unintentionally. Zero trust eliminates points of vulnerability by limiting network access for users, as well as by adopting extensive identity verification so that they only have access to the data and systems relevant to their role or position in the organization.

- **Increases visibility:** You know who and what is connected to the network at all times.
- **Extends security:** Security can be extended beyond the network with ZTNA. Unlike a VPN, which focuses exclusively on the network layer, ZTNA goes up a layer, effectively providing application security independent of the network.

IN THIS CHAPTER

- Trusting your users with strong authentication
- Using role-based access control (RBAC) to enforce least privilege
- Keeping privileged access secure

Chapter 2
Establishing IAM as a Foundation for Zero Trust

The first step in securing your network resources with zero trust access (ZTA) is to trust your users with verification before granting access. In this chapter, you learn why identity and access management (IAM) is the cornerstone of ZTA, how to manage privileged access on the network, and the role of role-based access control (RBAC) in enforcing the principal of least privilege.

Knowing Who Connects to Your Network

Security teams need to know who is on the network at all times. It's critical for organizations to know every user and what role that user plays in the company so IT can securely grant access to only those resources necessary for each role or job when needed.

However, organizations are at an increased risk from users that connect to their networks with weak passwords. Because so many online accounts today require user credentials, passwords are often too simple or are reused across multiple accounts, making them easy for attackers to compromise using exploits like phishing and social engineering. Even when organizations require complex passwords for their users, passwords alone aren't enough.

Strong authentication, or multi-factor authentication (MFA), refers to using multiple factors to verify that a user is who they say they are through a combination of factors, such as:

- Something you know (for example, a user ID and password)
- Something you have (for example, a hardware or software token, or a digital certificate installed on a device)
- Something you are (for example, a biometric indicator such as a fingerprint or iris pattern)

Adaptive or contextual authentication evaluates additional user attributes during a login attempt, such as time of day, geographic location, and/or network (trusted or untrusted) to assess the risk before allowing access. This technique can be used to either:

- Allow user access when the risk is deemed to be low
- Require two-factor authentication (2FA) when the risk is deemed to be high

For example, using the network attribute of the adaptive authentication, the system won't prompt an onsite user for 2FA because they're on the corporate network. However, the same user logging in from a public or home network and attempting to access corporate resources would be prompted for 2FA to further verify the user's identity.


TECHNICAL STUFF

Fast Identity Online (FIDO) provides the most secure and fastest login experiences for online applications and services. FIDO supports both Universal Authentication Frameworks (UAF, that is *passwordless authentication*) and Universal 2nd Factor (U2F, that is *universal two-factor authentication*).

Another challenge facing organizations today is the geographically dispersed workforce. Employees work from various locations such as the main office, branch offices, and home offices.

To support the evolving nature of work — including work-from-home and work-from-anywhere in the wake of the global pandemic — and the ongoing move to the cloud, organizations need a better way to securely connect their employees to critical business applications.

WARNING

Attacks against endpoint devices are increasing. According to a recent Ponemon Sullivan Privacy Report, 68 percent of respondents say the frequency of attacks against endpoints has increased over the past 12 months and the Verizon *Data Breach Investigations Report* found that 30 percent of breaches involved malware installed on endpoints.

Today, there is practically no standardization of device configurations for personal mobile devices permitted in bring your own device (BYOD) environments. Network risks associated with BYOD mobile devices include:

- Data leakage
- Unsecured Wi-Fi
- Network spoofing
- Unpatched vulnerabilities on rooted or jailbroken devices
- Malware and spyware
- Broken cryptography
- Improper session handling

Finally, organizations are at risk when access permissions are based on assumed trust of previously vetted devices. Many organizations have been breached by former employees and contractors. A lost or stolen device can reveal passwords that enable a breach on the network. This is why a zero-trust approach to security is so critical. As cybercriminals focus on compromising the broad array of network devices, security teams need better visibility and detection of every device connecting to the network.

Today's enterprise identity environments are made up of various systems that may include networking devices, servers, directory services, and cloud applications. Managing an identity that resides in these various systems can quickly grow into such a large administrative challenge that it negatively affects users, administrators, and application developers. Federated identity is a solution that enables users from a group of linked organizations to share the same user verification method to various applications

and resources. It does this by connecting users' online identities across multiple domains and networks. Federated identity solves several common access and security issues for organizations. Organizations can manage user access and provide easy access to applications by using security tools like MFA and single sign-on (SSO). An example of federated access is an organization enabling users to access partner websites, Active Directory, and web applications without having to log in every time.

TIP

A robust IAM solution should have the following capabilities:

- Establish identity through login, MFA, and digital certificates, which may evolve to add contextual authentication.
- Support both hardware and software token options for MFA, as well as FIDO, UAF, and U2F.
- Provide role-based information from an authentication source for use in privileged access.
- Establish and enforce role-based least privilege access policies.
- Provide added security with support for SSO to help improve user compliance and adoption.
- Leverage Security Assertion Markup Language (SAML) to authenticate users for access to cloud-based software-as-a-service (SaaS) applications.
- Verify zero trust network access (ZTNA) connections for devices and users on a per-session basis to individual applications.

Enforcing Role-Based Least Privilege Access

Managing individual user account permissions for just a few hundred users can be a daunting challenge. In an enterprise with thousands of users it can be impossible to manage. Role-based access control (RBAC) enables IT administrators to manage the permissions assigned to users more efficiently by assigning sets of permissions to groups or roles. In this way, users in an entire department, for example, can quickly be assigned access to a sensitive financial application or network file share. Additionally,

as users rotate through different job roles (for example, due to promotions or transfers), administrators can easily revoke the permissions associated with the old role and assign permissions associated with the new role. Active Directory frequently plays a key role in RBAC administration.

REMEMBER

However, RBAC can be a double-edged sword. Roles must be clearly defined and assigned only the minimum permissions necessary to perform the required functions for that role. This is the principle of *least privilege*. If roles are too broadly defined, large groups of users may be assigned excessive permissions in an effort to address everyone's needs with a broad brushstroke. Roles that are poorly defined may be easily misunderstood, resulting in users being improperly assigned to roles. Finally, roles must be actively managed to ensure they're revoked and assigned appropriately, and to ensure the permissions associated with roles reflect changes in the organization and/or IT infrastructure. Failure to revoke roles or permissions can cause "permission creep" within the organization, resulting in excessive permissions for large groups of users.

Managing Privileged Access

Accounts that have privileged access permissions associated with them are particularly valuable targets for attackers. These accounts typically have access to critical systems and resources on the network, as well as confidential or sensitive data. Privileged access allows the user to make administrative changes to systems, applications, and network and security infrastructure such as installing software (or malware), altering (or deleting) critical system files or data, creating new accounts, and resetting user passwords.

TECHNICAL STUFF

Privileged access permissions may be assigned to accounts or roles used by humans such as domain administrators, local administrators, emergency "break glass" accounts, superuser, and privileged business users. Privileged access permissions may also be assigned to accounts that are not used by humans such as application and service accounts.

Privileged access management (PAM) is a subset of IAM. Whereas IAM is used to authenticate and authorize all of an organization's users, PAM is specifically focused on managing and securing administrator and user accounts with elevated privileges (that is, privileged access).

UTILITY CO. ENHANCES SECURITY ACROSS IT AND OT INFRASTRUCTURE

CASE STUDY

Falu Energi & Vatten (Energy & Water) is a municipally owned utility company with products and services spanning electricity, heating and cooling, water, sewage, and recycling across the Swedish municipality of Falun.

Challenges

Back in 2009, earlier than many other utility companies, Falu Energi & Vatten realized both the potential and the necessity of digital transformation, embarking on a long-term project of modernization and digitization of the myriad processes and tools underpinning its operations.

For Falu Energi & Vatten, the first step in preparing for these changes was the realization that its IT network and security infrastructure would need a level of end-to-end visibility, control, and integration that its previous firewall architecture was unable to provide.

Solutions

After a careful evaluation of potential solutions, Falu Energi & Vatten chose Fortinet.

The resulting network included FortiGate next-generation firewalls (NGFWs), FortiSwitch, and FortiAP wireless access points. FortiClient, FortiAuthenticator, and FortiToken were added to ensure that every connected user and device would be strongly authenticated and would meet its zero trust access requirements.

With its integrated software inventory module, FortiClient provided Falu Energi & Vatten with increased visibility into software installed on the endpoint. In addition to managing licenses, software inventory can improve security hygiene. When installed software isn't required for business purposes, it unnecessarily introduces potential vulnerabilities, and thereby increases the likelihood of compromise.

Business Impact

- Improved the safety, reliability, and efficiency of essential services through centralized security policy monitoring and control
- Laid the foundations for ongoing IT and operational technology (OT) integration
- Provided the central visibility, control, and automation needed for the company's digital transformation

Through the resulting network infrastructure, Falu Energi & Vatten now has a solid foundation on which to build a safer, more reliable, and more efficient future for its business and the community of Falun.

IN THIS CHAPTER

- Exploring the evolving capabilities of EDR
- Making EDR part of a zero-trust strategy

Chapter 3
Leveraging EDR for Zero Trust

Endpoints — including desktop and laptop computers, servers, Internet of Things (IoT) devices, and more — comprise the single largest attack vector in an enterprise IT environment. Attackers target endpoints because endpoint security is generally less robust than security in the datacenter and day-to-day security decisions on the endpoint — such as whether or not to download and install an unknown file, open a potentially malicious email attachment, or click on a suspicious link — are left to the end user.

In this chapter, you learn how endpoint detection and response (EDR) has evolved from a rudimentary tool for manually investigating incidents to a highly automated detection and remediation endpoint solution, and why EDR is critical to an effective zero trust strategy.

Looking at the Evolution of Endpoint Detection and Response

Endpoint protection has traditionally been focused on preventing malware and other known threats from infecting a desktop or laptop PC. For practically as long as these devices have been around, users have been admonished to run antivirus software and keep it up to date. Over the years, antivirus software evolved into anti-malware software or Endpoint Protection Platforms (EPP) to broadly encompass other forms of malware including worms, trojans, spyware, rootkits, exploits, malicious scripts, and more. While anti-malware tools have improved greatly since their introduction, increasingly leveraging machine learning and behavioral analytics to prevent both known and unknown threats from infecting a PC, the unfortunate reality is that prevention isn't always possible.

REMEMBER

When prevention fails, endpoint detection and response (EDR) provides the tools for security teams to detect and respond to threats on endpoints and the network. Unfortunately, early EDR solutions are too slow and complex to operate in a fast-paced and dynamic threat environment. These first-generation EDR solutions require highly skilled security teams to run manual queries to search for specific indicators of compromise (IoCs) in endpoint telemetry, then manually triage and respond to any threats that are detected. Most organizations today simply don't have the skilled resources necessary to effectively operate these EDR tools.

Over the years, first-generation EDR solutions have evolved with the addition of some key bolt-on functionality including:

- **Threat intelligence:** Automated correlation of endpoint telemetry to IoCs from threat intelligence feeds reduces the need for manual queries to detect threats.
- **Attack visualization:** Threats can be mapped to help security analysts get a more complete picture of an attack in progress or an attack that has already happened.
- **Automated remediation:** Basic response capabilities typically include the capability to block specific IP addresses and processes, isolate endpoints from the network, and query the endpoint for additional data.

- **Threat hunting:** Advanced search capabilities and access to forensic data enables proactive threat hunting in the network environment.


TIP

Second-generation EDR solutions offer organizations greater visibility of their endpoints and network environment, tight integration with prevention tools (such as anti-malware), and policy-based automated risk mitigation using customizable playbooks. An example of a playbook action could be to block specific outbound attack communications, automatically rollback any system damage from ransomware, or prevent malicious file system access. These capabilities enable rapid detection and automated remediation of threats and attacks in real-time, and complete forensic investigative analysis.

EDR and Zero Trust

EDR is an essential component in a zero-trust strategy, enabling organizations to extend the "never trust, always verify" security posture of zero trust to their endpoints.

EDR provides an organization with a central tool for collecting, organizing, and analyzing data from the endpoints connected to its network. EDR can coordinate alerts and automate responses to imminent threats. This involves the incorporation of three elements:

- **Endpoint data collection agents** monitor endpoints and collect data. This includes data about processes, activity that occurs on the endpoint, connections to the endpoint, and data transferred to and from the endpoint.
- **Automated incident response** uses custom policy-based rules to identify threats and then trigger an automatic response. The automated response can both recognize the threat and determine what kind of threat it is. It can then perform a response, such as sending an alert that the endpoint's user will be logged out, doing so, and isolating the endpoint.

- **Analysis** of endpoint data in real time enables EDR to diagnose threats quickly — even if they do not necessarily match preconfigured threat parameters. Analysis also uses forensic tools to examine the nature of the threat and determine how the attack was executed after it has been contained and eradicated.

These three elements of EDR work together as part of an effective zero trust strategy to enable detection, containment, investigation, and eradication of threats in your endpoint and network environment.

Detection

When a threat evades the preventive controls on your endpoints and breaches your network environment, rapid detection is critical to minimize damage. However, detection can be extremely challenging, particularly when you are dealing with an advanced threat that has already evaded your endpoint protection tools. EDR uses continuous file analysis and cyberthreat intelligence to rapidly detect threats. EDR examines each file that interacts with the endpoint and can flag any files that may present a threat. Cyberthreat intelligence leverages a combination of artificial intelligence (AI) and large repositories of past and currently evolving threat data to detect threats that are targeting your endpoints.

Containment

Once a threat has been detected, EDR contains it using segmentation to prevent the threat from spreading across the network. This involves isolating specific areas of the network so that a threat can't infiltrate adjacent network elements. However, this may not be enough. Therefore, in addition to segmentation, an effective EDR solution also contains the threat itself. Containment is particularly important when it comes to ransomware. Because ransomware can effectively hold an endpoint hostage, it needs to be contained to prevent other endpoints from getting infected.

File testing

Sandboxing allows EDR to contain a threat within an environment that is designed to simulate the conditions within a section of

your network for the purpose of understanding the nature of the threat. Once the threat is confined to this safe and isolated area, EDR closely monitors and analyzes the threat's behavior. This information can produce helpful, actionable insights that can be used to improve the organization's overall security posture and can be conveyed to the cyberthreat intelligence system to help it evolve to address future threats.

Elimination

While the other facets of EDR provide critical knowledge about the threat, that information is useless if it isn't employed to eliminate it and similar threats in the future. The elimination process depends on gathering critical information about the threat and then using it to execute an action plan. For example, the system has to figure out where the threat came from and where it went. Information about the threat's origin can be used to enhance future security measures. The system also needs to pinpoint the applications and data the malicious file affected or tried to attack, as well as whether the file has replicated itself to continue its attack.

IN THIS CHAPTER

- Knowing what is connected to the network
- Gaining visibility and control of devices
- Implementing automated response and network orchestration

Chapter 4
Bringing Zero Trust to Device Security

If cybercriminals were to write a book titled *The Seven Habits of Highly Effective Hackers*, there would definitely be a chapter called "Begin with the Endpoint in Mind." Endpoints are a preferred initial attack vector for cybercriminals to gain access to more valuable network resources. In this chapter, you learn how to apply a zero-trust strategy to your device security.

Discovering and Identifying Devices

In addition to knowing who is on the network (discussed in Chapter 2), organizations need to know what devices are on the network. These devices include:

- Networked office equipment (such as printers)
- Retail systems (for example, point-of-sale systems)
- Operational technology (OT)
- Internet of Things (IoT) sensors and devices

REMEMBER

The challenge in managing all these devices lies in their wide deployment, the varying levels of device management, inconsistent configuration controls, and the lack of support for standard communication protocols in many legacy devices.

The traditional network perimeter has all but disappeared as the proliferation of devices connecting to the network has created an exponentially larger attack surface for organizations to protect, with every endpoint device essentially constituting a microperimeter. The result of this explosion of devices and the expanding attack surface is that many organizations are losing visibility and control because they're no longer certain what devices are connecting to their networks. And because each microperimeter is associated with an individual device, these endpoints have become a prime target for malware infections and sophisticated exploits.

WARNING

Attacks against IoT devices are increasing, and the scale and impact of a successful IoT attack can be devastating. For example, the Cybersecurity Infrastructure and Security Agency (CISA), working with several industry security firms, recently discovered a vulnerability in millions of IoT smart camera devices that allows an attacker to gain access to the cameras, watch live video feeds, and create botnets.

The greatest area of growth in the endpoint attack surface is from the IoT device explosion. Cyberattacks on IoT devices are booming as organizations connect more and more smart devices to their networks. Attackers exploit these devices to conduct distributed denial-of-service (DDoS) attacks and other malicious activities.

REMEMBER

To secure endpoints, enterprises must have full visibility into where each device is, what it does, and how it connects to other devices across the network topology. Lack of visibility leaves an organization vulnerable to unseen risks, and many organizations don't have a strategy in place to deal with attacks on IoT devices. Security teams must be able to discover and identify all devices at the edges of the network.

Traditional network segmentation is used by some organizations, but it is difficult to define secure network-based segments that can be simultaneously accessible to all authorized users and applications and completely inaccessible to all others. Policy-based segmentation enables a more dynamic — and granular — network segmentation strategy that can automatically adapt to ensure least privilege in a zero-trust network.

Ensuring Endpoint Visibility and Control

Network access control (NAC) solutions help organizations keep up with the ever-expanding attack surface associated with the proliferation of endpoints and devices on the network. NAC solutions provide visibility into the network environment for enforcement and dynamic policy control. Whether devices are connecting from inside or outside the network, NAC solutions can automatically respond to compromised devices or anomalous activity. With NAC solutions, organizations can:

- Discover, identify, profile, and scan all devices for vulnerabilities
- Establish and ensure ongoing network control
- Establish and enforce policies that limit network access to only what is needed for that device
- Maintain automated response and network orchestration (discussed later in this chapter)

A NAC solution can automatically identify and profile every device as it requests network access and scan the device for vulnerabilities. The NAC processes should be completed within a few seconds to minimize the risk of device compromise. NAC solutions that rely on traffic scanning allow devices to connect to the network during identification. However, the traffic-scanning process can take up to half an hour, during which time the network may be breached by a compromised device or endpoint.

TIP

A NAC solution should be easy to deploy from a central location and offer consistent operation across wired and wireless networks.

Providing Automated Response and Network Orchestration

To accelerate and expand the reach and scale of their attacks, cybercriminals leverage extensive automation. Although visibility into the network can help detect potential threats, the response to these threats can be fragmented and ineffective because of slow manual workflows. Without the benefit of advanced security processes, security teams are often operating at a disadvantage, which increases an organization's risk.

Attacks are more sophisticated and security analysts face increasingly complex and fragmented security infrastructures with too many point products from different vendors.

Fundamental to the security of a constantly changing network is understanding its makeup — you can't protect what you can't see. An effective NAC platform provides policy-based security automation and orchestration that enables discovery of every endpoint and network infrastructure device, provides contextual awareness for implementing dynamic network access control, and delivers the capability to contain a cyberbreach through automated threat response.

GRUPO UNIVERSAL GAINS VISIBILITY AND CONTROL WITH FORTINAC

CASE STUDY

Grupo Universal is one of the main conglomerates in the Dominican Republic, made up of 10 subsidiaries offering solutions for insurance, financial, and other services organizations.

Challenges

IT security and IT infrastructure availability are essential to Grupo Universal. In 2017, the company launched one of its most important projects since its foundation in 1964: its technological and digital transformation.

Given the technological demands of today's digital economy, storing data in centralized architectures limits employee access and user response. Grupo Universal's IT teams recognized the risks of a centralized database and decided to evolve into a wireless connection model, which in spite of also presenting some challenges, allowed the company to meet customer and internal users' network security demands.

To help with the decentralized infrastructure project, Grupo Universal chose to partner with Fortinet.

Solutions

In order to reduce the administrative complexity for operational teams, Grupo Universal proposed having centralized management

that would reduce risks and maintain an updated communications infrastructure.

Through the integration of Fortinet Secure SD-WAN with other Security Fabric solutions, Grupo Universal was able to deploy a high-performance communications infrastructure and end-to-end security. Management and analytics solutions such as FortiManager and FortiAnalyzer delivered complete visibility with a single pane of glass and centralized policy management.

FortiNAC network access control provides full visibility of all devices on the network, allowing for complete control of the level of access given per device, and FortiClient delivers advanced, proactive end-point protection from zero-day threats. It seamlessly integrates with FortiSandbox for advanced threat detection.

Secure email gateway FortiMail protects cloud-based email services from advanced email threats to keep users and data secure. With the FortiWeb web application firewall, Grupo Universal was able to safely access cloud-based, business-critical applications. Adding FortiAP across the organization tied everything together, and ensured secure wireless access for devices for branch offices.

Business Impact

- Improved performance and communications speeds with redundant links across all locations
- Cost savings of $30,000 per year in communication links and $70,000 per year in WAN optimization
- Faster cloud access and cloud-hosted applications with local breakouts

Through this project, Grupo Universal not only appropriately scaled their communications and IT infrastructure, centralized administration, and improved control management and risk response, but they also managed to reduce costs and increase network availability to 99.9 percent. With Fortinet's support, Grupo Universal was able to effectively integrate its communications and security in its technological and digital transformation process.

IN THIS CHAPTER

- Recognizing the limitations of virtual private networks
- Introducing zero-trust network access
- Improving remote access security and user experience with zero-trust network access

Chapter 5
Reimagining the VPN with Zero Trust

Although virtual private networks (VPNs) have become commonplace, many organizations are now looking for better solutions to securely connect their increasingly remote and mobile workforces. In this chapter, you learn how zero-trust network access (ZTNA) improves security, enables more granular control, and delivers a better user experience than traditional VPNs.

Saying Goodbye to the VPN

VPNs have long been the de facto method for remotely accessing corporate networks, but they have some serious issues, particularly in terms of security. The recent proliferation of remote working — necessitated by the global pandemic — has put renewed focus on the limitations of traditional VPNs.

For organizations that rely on a traditional VPN to secure their remote workers and home offices, there are many drawbacks including:

- **VPNs use the outdated and ineffective perimeter-based approach to security.** Once users connect to the corporate network with a VPN client, they often have broad access to all the resources on the network. This largely unrestricted access exposes the rest of the corporate network to threats that use the endpoint as an attack vector. If split tunneling is enabled, a user can surf the internet — without going through a corporate firewall — while still connected to the corporate network. The risk of a data breach, ransomware attack, or malware infection on the corporate network increases exponentially if users are permitted to install a VPN client on personally owned devices that may already be compromised.
- **VPNs have no visibility into the traffic they deliver.** VPNs are used to connect to the corporate network over an encrypted tunnel when working from hotels, coffee shops, or home. This tunnel prevents cybercriminals from snooping in on the session, but also prevents security controls from inspecting the traffic. Because most home offices and public hotspots are connected to largely unsecured networks, they're a relatively easy target for cybercriminals to exploit using social engineering tactics and malware.
- **VPNs aren't designed for today's highly distributed network resources.** Applications and data are now spread across corporate data centers, multicloud environments, and distributed branch and home offices. Most VPN solutions weren't designed to manage this level of complexity. A VPN connection backhauls all traffic across the corporate network for inspection, which is bandwidth-intensive and causes latency. Split tunneling can address this inefficiency but creates its own set of challenges (discussed previously).

Building a Secure Remote Connection for Today's Business

ZTNA offers a better remote access solution than traditional VPNs and also addresses application access issues. ZTNA starts with the premise that location doesn't confer trust: Where a user or device is physically located is irrelevant. Any user is capable of malicious behavior and any device can be compromised. ZTNA is based on this reality.

REMEMBER

ZTNA grants access to individual applications and workflows on a per-session basis only after a user and/or device has been authenticated. Users are verified and authenticated to ensure they're allowed to access an application before they're granted access. Every device is also checked each time an application is accessed to ensure the device meets the application access policy. Authorization uses a variety of contextual information, including user role, device type, device compliance, location, time, and how a device or user is connecting to the network or resource.

With ZTNA, once a user and device are properly authenticated — for example, using a combination of multifactor authentication (MFA) and endpoint validation — they can securely connect to the network and be granted least privilege access to requested resources. The principle of least privilege means the user and device can only access those applications or resources that are needed to perform an authorized task or function — and nothing else.

Access control doesn't end at the access point. ZTNA operates in terms of identity rather than securing a place in the network, which allows policies to follow applications and other transactions end to end. By establishing greater levels of access control, ZTNA is a more efficient solution for end-users and provides policy enforcement wherever it's needed.

TIP

Although the ZTNA authentication process provides points of authentication, unlike a traditional VPN, it doesn't specify how that authentication takes place. As new or different authentication solutions are implemented, they can be seamlessly added to the ZTNA strategy.

Today, there are two primary approaches to implementing ZTNA:

- **Client-initiated ZTNA:** Sometimes called endpoint-initiated ZTNA, the client-initiated ZTNA model was initially known as a software-defined perimeter and is based on the Cloud Security Alliance (CSA) architecture. This approach uses an agent that is installed on a device to create a secure tunnel. When a user wants to access an application, the agent gathers information like the user's identity, device location, network, and the application being used, and it builds a risk profile to assess the overall security posture. It then connects back to the application over a proxy connection, and if the risk profile meets the organization's policy requirements, the user and device are granted access to the application for the session. Applications can be on premises or cloud-based apps. Using the client-initiated model can be challenging because managing the agents on devices can become a headache for IT unless a central management solution can coordinate deployment and configuration. Additionally, unmanaged devices need to be handled by other means, such as a network access controller (NAC).
- **Service-initiated ZTNA:** The service-initiated ZTNA model uses a reverse-proxy architecture, which is also sometimes referred to as application-initiated ZTNA. Based on the BeyondCorp model, the biggest difference from client-initiated ZTNA is that it doesn't require an endpoint agent. It uses a browser plug-in to create a secure tunnel and perform the device assessment and posture check. A key disadvantage is that it's limited to cloud-based applications. Because the application's protocols must be based on Hypertext Transfer Protocol (HTTP)/Hypertext Transfer Protocol Secure (HTTPS), it limits the approach to web applications and protocols, such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) over HTTP. Although a few newer vendors are offering additional protocol support, the model isn't suited to companies that have a hybrid combination of cloud and on-premises applications.

WARNING

Organizations should be careful to select ZTNA solutions that integrate with their existing infrastructure. Building a complete ZTNA solution requires a variety of components: a client, a proxy, authentication, and security. Often these solutions are provided by different vendors and the components may run on different

operating systems and use different consoles for management and configuration, so establishing a zero-trust model across vendors can be difficult or impossible.

Seeing the Advantages of Zero-Trust Network Access

Adopting a zero-trust approach to security is a process that touches many systems and may take years for some organizations to fully implement. But addressing remote access is a good first step toward implementing the zero-trust security model. ZTNA solutions offer many advantages over traditional VPNs, including:

- **Organizations can extend the zero-trust model beyond the network.** Unlike a VPN, which operates at the network layer, ZTNA focuses on the transport layer, effectively providing application security independent of the network.
- **ZTNA works transparently in the background, which improves the user experience.** For users, ZTNA is easier to manage than a VPN. Users no longer have to remember when to use the VPN or go through the process of connecting. There's also no risk of tunnels accidentally being left open because someone forgot to disconnect the VPN client. With ZTNA, a user simply launches the application and immediately gets a secure connection whether the application is on premises or in a cloud. This encrypted tunnel is created on demand and in the background — completely transparent to the user. Because the corporate network is no longer an implicit zone of trust, the same tunnel is created whether the user is on the network or off the network.
- **Users and devices are verified and validated before access to an application or resource is granted.** This process includes a security posture check that verifies that the endpoint is running the right firmware and endpoint protection software to verify it is safe to connect to the application. The verification is granular, per session, using the same access policy whether a user is accessing resources that are on premises or in the cloud. The same policy also controls who can access that app based on the profile of the authenticating user and device.

- **Because ZTNA focuses on application access, it doesn't matter what network the user is on.** ZTNA automatically creates secure connections to applications, no matter where the user is located. For every application session, ZTNA verifies the security posture of both the user and device — even when users are in the office.
- **ZTNA reduces the attack surface by hiding business-critical applications from the internet.** On the application side, because the user is connecting back to the enforcement point and then proxying that connection to the application, the application can exist on premises or in a cloud, all while hidden from the internet. The application only needs to establish a connection with the enforcement points, keeping them safe from cybercriminals.

REMEMBER

More organizations are recognizing the need to transition away from traditional VPNs. ZTNA is proving to be a better solution that is easier to use and provides better application security.

IN THIS CHAPTER

- Adjusting to the new work reality
- Implementing zero trust for application access
- Keeping endpoints, networks, and clouds secure

Chapter 6
Extending Zero-Trust Control Off-Net

In today's networks, a user, device, or application could be connecting from anywhere, which changes the security paradigm. The old, perimeter-based security model focused on location: Where is the user connecting from? Where is the application hosted? Where is the server installed? In this chapter, you learn why security must evolve to protect users, devices, and applications wherever they're located.

Securing the New Hybrid Workforce

Although businesses have been increasingly enabling mobile and remote work scenarios for years, the global pandemic forced many companies to transition to remote work for much of their workforce practically overnight. Even as organizations begin to bring their employees back to the office, they're having to rethink the office environment and plan for a new reality — one that includes permanently supporting remote or hybrid work from home (WFH) or work from anywhere (WFA) models.

TIP

According to the Pew Research Center, 54 percent of employed adults in a recent survey say that they want to work from home all or most of the time when the COVID19 outbreak is over.

This accelerated adoption of remote and hybrid work models has caused a proliferation in the number of devices and locations that must be protected as the digital attack surface has expanded and more applications, devices, data, and users are now exposed. Understanding and controlling the flow of traffic across these widely dispersed environments is critical.

WFH/WFA requires both connectivity and security. The applications that your employees need to perform their work functions may be hosted in an on-premises data center, in a private cloud, or in a public cloud, so user identification, authentication, authorization, and access permissions are critical.

REMEMBER

In the public cloud, applications can be hosted as a software as a service (SaaS) offering, or they may be running as a platform as a service (PaaS), and/or an infrastructure as a service (IaaS) workload.

To securely implement WFH/WFA, more organizations are looking at zero-trust access (ZTA). ZTA limits user and device access to networks, which provides identity assurance. Zero-trust network access (ZTNA) then limits user and device access to only the applications that users need to do their jobs. Combining ZTA and ZTNA strengthens the company's security posture.

Looking at WFH/WFA from an outbound perspective, secure access service edge (SASE) solutions provide secure access for employees, customers, and partners across operating environments by securing any user, on any device, anywhere on the network. A cloud access security broker (CASB) — which is a key component of SASE — sits between your users (remote workers) and cloud applications and can be used to monitor activity and enforce security policies.

TECHNICAL STUFF

SASE (pronounced "sassy") is a cloud-delivered service that combines network and security functions with software-defined wide-area network (SD-WAN) capabilities to support the dynamic, secure access needs of today's hybrid organizations. Conceptually, SASE extends networking and security capabilities beyond

where they're typically available, which allows users, regardless of location, to take advantage of ZTNA, CASB, firewall as a service (FWaaS), secure web gateway (SWG), and a variety of threat detection functions.

BANK MIGRATES ITS WORKFORCE TO A SECURE REMOTE ENVIRONMENT

CASE STUDY

Founded in 1988, Banco Fibra is a wholesale bank that guarantees precision, transparency, and speed to businesses in Brazil. Its business strategy is focused on serving medium and large companies in the most diverse segments and agribusiness. Fibra is built by people, but strongly reliant on technology. This combination guarantees agile, flexible, and customized business solutions to customers.

Information security is a top priority at Banco Fibra. As a financial institution and potential target for cyberattacks, the company has always diligently preserved its customers' trust by protecting their data's integrity and confidentiality. This concern prompted the bank's transformation journey several years ago — one that would be key in strategically positioning the company within the business world's new digital environment.

Challenges

Banco Fibra was already a Fortinet customer, using FortiGate and FortiClient solutions before the COVID quarantine. The bank initially intended to use these solutions to provide network and endpoint security and improve operational efficiency. Now, faced with an unprecedented scenario, there was an opportunity to take advantage of these solutions' functionalities and quickly migrate the workforce to a remote model.

After the initial setup of the new remote-work model, many adaptations were necessary to meet the employees' technology demands, particularly to define the user profiles and to ensure the secure access and the proper application performance. Another challenge was operating their softphone solution over the VPNs. Ensuring the performance of the softphone solution was important because it integrated with the customer relationship management (CRM) application the bank uses to provide customer service and monitor customer experience.

(continued)

(continued)

Solutions

In a matter of days, Banco Fibra deployed the required virtual private networks (VPNs) using the existing security solutions. In less than 10 days, Banco Fibra was able to set up its remote-work environment with appropriate policies, access rules, and user authentications, among other features.

Business Impact

- Quickly transitioned teams to a remote-work model, keeping the bank's operations running throughout the COVID-19 pandemic
- Maintained the high quality of its customer service in a remote-work environment
- Extended the bank office's high level of security to its 350 employees´ homes
- Created the foundations to escalate bank's digital transformation

The bank is currently considering expanding its VPN solution to achieve even more redundancy and availability. Another project involves expanding the security perimeter to the data center, providing even more scalability and better use of cloud resources in a natively secure format.

Improving Application Access and Security

In the zero-trust model, application access is controlled on a per-session basis and each user and device must be verified, whether they're connecting remotely or from the corporate network.

Application access should be mapped to the individual's role so that only those applications that are necessary for the user to perform their assigned job functions are available. Regardless of whether an application runs in an on-premises data center or a cloud environment, zero trust is enforced.

REMEMBER

Zero trust access (ZTA), discussed in Chapter 2, focuses on role-based access control (RBAC) to the network. Zero-trust network access (ZTNA), discussed in Chapter 5, brokers user access to applications.

Zero-trust application access and security solutions:

- Verify users and devices for each application session
- Control user access to applications based on policy
- Enforce application access policy no matter where the user is located
- Create a secure, automatic connection between the user and ZTNA proxy point
- Work with physical firewalls, virtual appliances, and Secure Access Service Edge (SASE) platforms

Delivering Security Services to Endpoints, Networks, and the Cloud

Digital transformation initiatives and workforce mobility trends (including WFH/WFA) have changed and expanded the enterprise attack surface, opening up new attack vectors that can be exploited by threat actors both inside and outside the network. A comprehensive zero-trust security strategy must extend robust enterprise security services to endpoints, corporate networks, and private and public clouds.

REMEMBER

One of the main reasons for the growing attack surface is the proliferation of IoT and smart devices that are accessing the network. Security teams often lack visibility into the deluge of devices accessing their networks. A zero-trust approach empowers organizations to identify and secure unknown IoT endpoints and devices that access the network. Integrated endpoint visibility, granular control, advanced protection, and policy- and context-based endpoint assessment capabilities work together in a ZTA solution to ensure organizations are protected against compromised devices.

By implementing a ZTNA framework that identifies, segments, and continuously monitors all devices connecting to their networks, organizations can replace their high-risk, flat networks to ensure that internal resources remain secured, and that data, applications, and intellectual property are protected. This strategy not only reduces the risks associated with traditional perimeter-based security, but also increases the visibility and control of off-network devices while simplifying overall network and security management.

WARNING

As attacks become more sophisticated and advanced, the traditional perimeter-based approach to security is no longer sufficient. Depending on the nature and sophistication of the threat, no single point in an organization's security infrastructure has visibility into all aspects of the threat. ZTA confirms the identity of the users and devices that are connecting to your network and ensures they have only the minimum level of access permissions needed to perform a function or job.

Organizations increasingly rely on hybrid and multicloud environments to support their evolving digital transformation requirements. According to a recent report from Fortinet, 76 percent of organizations surveyed reported using at least two cloud providers. Similarly, the Flexera *2021 State of the Cloud Report* found that 92 percent of enterprises have a multicloud strategy, 80 percent have a hybrid cloud strategy, and respondents are using an average of 2.6 public and 2.7 private clouds in their environments. The result is that applications can reside anywhere — from on premises to branch office to data center to cloud. And now that the era of WFH/WFA is upon us, organizations are rethinking how they secure their network edges both on premises and in the cloud.

IN THIS CHAPTER

- Assess the business process criticality of your assets
- Understand what applications are used
- Apply role-based access controls
- Verify on an ongoing basis

Chapter 7
Ten Steps on the Journey to Zero Trust

Implementing a zero-trust strategy for your organization is a journey, not a destination. This chapter offers ten key steps to help you succeed on your journey to zero-trust access (ZTA).

Assess Your Assets and Their Business Process Criticality

You can't protect every asset and resource on your network at the same level. It's important to prioritize your efforts by first determining which assets and resources are most critical to your business processes. Once you've determined where to start, you can begin implementing your ZTA strategy to protect your most critical resources and valuable assets first.


TIP

The criticality of your business processes (and the systems and applications they depend upon) will drive other important decisions such as additional security policy controls, service-level agreements (SLAs) and operational-level agreements (OLAs), and recovery time objectives (RTOs) and recovery point objectives (RPOs) for business continuity and disaster recovery.

Identify the Users/Entities and Roles on Your Network

Identifying every user and entity on your network is critical to establishing an effective ZTA strategy. Once identity is established, access policies are determined by a user's role in the organization. A least privilege access policy is used to grant access to only those resources necessary to perform a specific role or job. Access to additional resources is provided only on an as-needed basis.

Role-based access control (RBAC) is a critical component of access management. The capability to authenticate and authorize users with RBAC provides a robust network security posture that benefits the entire organization, including its partners, suppliers, and contractors.

Identify the Devices on Your Network

The next step in adopting a zero-trust strategy is to discover and identify all the devices on your network — whether that's an end-user's phone or laptop, a virtual server, a network printer, a headless Internet of Things (IoT) device, or a security badge reader.

REMEMBER

The proliferation of applications and devices is expanding the traditional network perimeter, creating billions of edges that must be managed and protected. Network access control (NAC) tools deliver visibility into the devices on your network.

Identify the Applications Used by Your Organization

Applications are at the heart of business operations and processes. Today, these applications include not only those that are installed on endpoints or servers in your data center. The application landscape now consists of software-as-a-service (SaaS) offerings and application workloads hosted in private and public clouds.

Create Zones of Control within Your Network and Assets

Network segmentation has long been used to limit traffic in certain areas of the network and to provide additional security controls within the network. Perhaps the earliest example is the demilitarized zone (DMZ) that many organizations create for public-facing web applications between the internet and the corporate network.

Internal segmentation firewalls establish visibility and control within the network and provide the ability to scan, protect, and block traffic.

Apply Role-Based Access Controls to Your Assets

Role-based access controls (RBAC) are used to efficiently manage the permissions that groups of users are granted to a specific asset, based on their job or role within the organization.

WARNING

Organizations often focus on ensuring group memberships are properly maintained and accurate. Although this is an important aspect of RBAC, it's just one side of the coin. Equally important is ensuring that the permissions assigned to a role aren't excessive. The scope should be limited to the specific resource that is required by the role and only the permissions necessary to perform a function within that role should be granted (that is, least privilege access).

Control Where Devices on Your Network Can Communicate

A zero-trust security approach uses microsegmentation to create granular trust zones around individual resources, which helps to enforce the principle of least privilege access. Users and entities are only granted access to the resources that are needed to perform a specific role or job. Microsegmentation prevents users (and attackers) from roaming freely on the network.

TECHNICAL STUFF

Microsegmentation adds a dynamic, policy-based element to traffic segmentation, enabling much more granular control than regular network segmentation.

Extend Control of Devices When Employees Are off the Network

Enhanced workplace mobility and an increased emphasis on remote work — including work from home (WFH) and work from anywhere (WFA) — has led to increased interest in endpoint security including endpoint visibility, control, scanning, patching, and web filtering off the network.

REMEMBER

With a zero-trust strategy in place, organizations can address the challenge of protecting off-network devices by improving endpoint visibility. Vulnerability scanning, robust patching policies, and web filtering are all critical elements of a zero-trust strategy. In addition, a zero-trust approach can enable secure remote access to networked resources. This allows security teams to see, control, and protect every asset whether on or off the network. Going beyond the VPN, ZTNA extends traditional ZTA network access to per-application usage, so administrators not only know who is on the network but even which applications they're currently using, with transactions and usage constantly being monitored and inspected.

Apply Application Access Control

An effective ZTA strategy addresses both network connection and application access based on the underlying assumption that no user or device is inherently trustworthy. No trust is granted for any transaction without first verifying that the user and the device are authorized to have access.

Continuously Verify and Authenticate Users and Devices

ZTA requires continuous authentication, verification, and monitoring of users and devices that are connected to the network. Successfully logging into the network doesn't grant a user or device unrestricted access to the resources on your network. Further authentication may be required to access certain sensitive resources in restricted zones and the duration of user sessions should also be limited. This ensures that sessions can't be hijacked and that appropriate controls can be enforced if, for example, the device state changes during the session and its risk posture becomes unacceptable.

FORTINET

Reliable, secure connectivity, everywhere you need it.

Today's remote workers require enterprise-level connectivity at home. Unreliable and under-secured home networks not only impact productivity, but also expose organizations to security risks and cyber attacks.

Linksys HomeWRK for Business | Secured by Fortinet combines enterprise-grade security from Fortinet with consumer-friendly connectivity from Linksys. Our joint solution:

Separates the corporate network from the home network
Extends unified security policies from the corporate network to home
Centralizes management of work-from-home networks
Prioritizes mission-critical applications

Learn more at https://www.fortinet.com/products/secure-home-network

LINKSYS HomeWRK BUSINESS
SECURED BY FORTINET

Get started with a zero-trust access strategy today

Every time a device or user connects to your network and is automatically trusted, your organization's applications and data are at risk. The traditional perimeter-based approach to security in which everything inside the network is trusted and everything else is not trusted is no longer effective. Organizations need to shift to a zero-trust access strategy, based on the principle of "never trust, always verify," to ensure they know every device and user that accesses the network and how to protect their assets on and off the network.

Inside...

- Understand the basics of zero trust
- Know and control *who* connects to your network
- Know and control *what* connects to your network
- Enforce role-based least-privilege access
- Secure endpoints, networks, and cloud

Lawrence Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 200 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-85984-0
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.