Build a Secure Remote Connection Solution for Today's Business

Table of Contents

Executive Overview

Many organizations use virtual private networks (VPNs) that function like a tunnel back to the company network, but relying exclusively on a VPN has security risks. Even after the pandemic ends, CISOs are going to need a better strategy for supporting telework because it's likely that many employees will continue to work remotely at least part of the time. Given the limitations of VPNs and the dynamic and distributed nature of today's networks, it's clear that a better solution is needed. Zero-trust network access (ZTNA) is the evolution of VPN remote access. It simplifies secure connectivity, providing seamless access to applications no matter where the user or the application may be located.

54% of employed adults say that they want to work from home all or most of the time when the coronavirus outbreak is over.[1]

Introduction

The recent rise in remote working has put a spotlight on the limitations of virtual private networks (VPNs). For years, VPNs have been the de facto method of accessing corporate networks, but they have some serious drawbacks, particularly in terms of security.

The biggest issue is that a VPN takes a perimeter-based approach to security. Users connect through the VPN client, but once they're inside the perimeter they often have broad access to the network, which exposes the network to threats. Every time a device or user is automatically trusted in this way, it places an organization's data, applications, and intellectual property at risk.

In addition to the issues using a VPN for remote access, network operators are looking for a better way to secure applications. Having some applications on the cloud and some on-premises makes it difficult to deliver a common method of control and enforcement, particularly when some users are on-site and others are remote. Deploying applications to the cloud can expose them to probes from unwanted actors and increases risk.

Going Beyond the VPN

Zero-trust network access (ZTNA) offers a better remote access solution that also addresses concerns related to application access. The term *zero trust* means exactly what it sounds like. With this security model, the assumption is that no user or device is trustworthy, and no trust is granted for any transaction without first verifying that the user and the device are authorized to have access.

Because ZTNA starts with the idea that location does not grant a level of trust, where a user is working becomes irrelevant. The same zero-trust approach applies no matter where a user or device is physically located. Because any device is considered to be potentially infected and any user is capable of malicious behavior, the ZTNA access policy reflects that reality.

Unlike a traditional VPN tunnel with unrestricted access, ZTNA grants access per-session to individual applications and workflows only after a user and/or device has been authenticated. Users are verified and authenticated to ensure they are allowed to access an application before they are 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 in place, once a user has provided appropriate access credentials such as multi-factor authentication and endpoint validation and is connected, they can then be given what is known as least privileged access. The user can access only those applications that they need to efficiently perform their jobs 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 needed.

Although the ZTNA authentication process provides points of authentication, unlike a traditional VPN, it does not specify how that authentication takes place. As new or different authentication solutions are implemented, they can be seamlessly added to the ZTNA strategy. New authentication solutions may do things like help eliminate issues related to weak or stolen passwords and credentials, address challenges due to the inadequate security of some Internet-of-Things (IoT) devices, or add extra levels of verification to access sensitive or confidential information or critical resources.

ZTNA vs. VPN

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. With ZTNA, a user simply clicks the application and immediately gets a secure connection whether the application is on-premises, in a public cloud, or on a private cloud. This tunnel is created on-demand, transparent to the user. Because the network is no longer a zone of trust, the same tunnel is created if the user is on the network or off the network. The encrypted tunnel happens in a transparent manner, providing security in the background.

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, in a private cloud, or in a public cloud, all while hidden from the internet. The application only needs to establish a connection with the enforcement points, keeping them safe from prying hackers or bots.

ZTNA Models

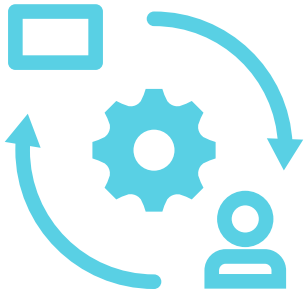
Vendors have adopted two primary approaches to implementing ZTNA in their products and services: client-initiated and service-initiated.

1. 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 architecture. This approach uses an agent on a device to create a secure tunnel. When a user wants to access an application, the agent performs an assessment to determine the security posture. After gathering information like the user's identity, device location, network, and the application being used, it builds a risk profile. It then connects back to the application over a proxy connection, and if the information meets the organization's policy, access to the application is granted. Applications can be on-premises or Software-as-a-Service (SaaS) 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).

2. 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 is not suited to companies that have a combination of hybrid cloud and on-premises applications.



“Gartner predicts that by 2023, 60% of enterprises will phase out traditional VPNs and use a ZTNA model.”[2]

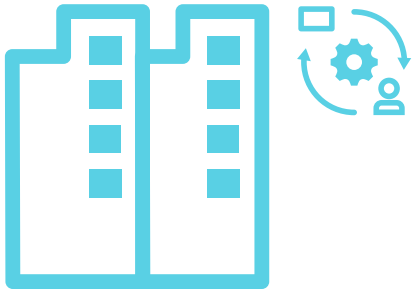
ZTNA and the Future

Adopting a zero-trust approach to cybersecurity is a process that touches many systems and may take years for many organizations to fully implement. But addressing remote access is a good first step toward implementing a complete zero-trust solution.

As companies transition their approach to remote access, they often have a mix of VPN and ZTNA. Many vendors providing ZTNA services are doing so in conjunction with SASE services. This service-initiated approach makes it easy to control cloud applications access from cloud security, but it can incur expensive SASE charges and may be limited in the types of applications it can support.

Building a complete zero-trust network access solution requires a variety of components: a client, a proxy, authentication, and security. Often these solutions are provided by different vendors and the components often 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.

By selecting integrated and automated tools, CISOs can overcome the key challenges of implementing ZTNA. Using an integrated firewall-based and SASE approach, they can employ ZTNA capabilities with simplified management using the same adaptive, application access policy whether users are on or off the network. ZTNA can be applied to remote users, home offices, and other locations such as retail stores by offering controlled remote access to applications that is easier and faster to initiate while providing a more granular set of security protections than traditional legacy VPNs.



Only 15% of organizations have completed a transition to a zero-trust security model, which does not automatically assume that anyone inside the network perimeter is trusted.[3]

Secure Remote Access With ZTNA

With the increase in remote work, the limitations of traditional VPNs have become clear. The more people move and work from anywhere, the less secure a traditional perimeter-based approach becomes. Every time a device or user is automatically trusted, it places the organization's data, applications, and intellectual property at risk. ZTNA solutions are a better way to secure remote access than traditional VPNs and also improve controls around application access.

[1] Kim Parker, et al., "How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work," Pew Research Center, December 9, 2020.

[2] Mike Wronski, "Since Remote Work Isn't Going Away, Security Should Be the Focus," Dark Reading, September 24, 2020.

[3] "2019 Zero Trust Adoption Report," Cybersecurity Insiders, November 2019.

March 6, 2021 12:36 AM

ebook-ztna-remote-connection

911928-0-0-EN