Hillstone NETWORKS

WHITE PAPER

Hillstone ZTNA Solution for

Zero-Trust Network Access

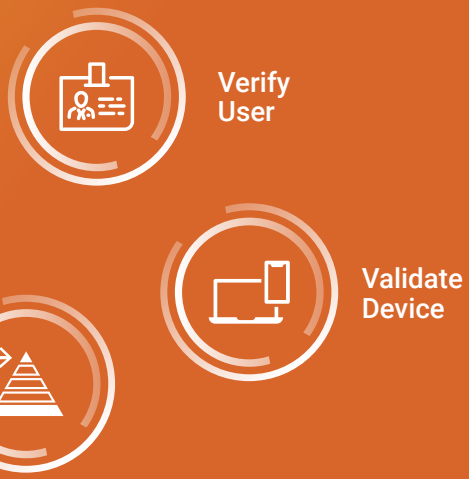
Introduction

Work-from-home (WFH) and work-from-anywhere (WFA) initiatives were trending pre-pandemic. CISOs globally were looking to enable greater workforce agility and improve workplace flexibility. When the pandemic hit, WFH and WFA became the number one priority for enterprises worldwide. Security and networking teams are faced with requirements to quickly onboard remote workers but still protect against malware and ransomware. Employee home networks, being less protected, make great launching points for ransomware infections, leading to existential threats to companies.

Even as the world unlocks, CISOs are tasked with enabling secure multi-location access: on-campus networks, from branch offices, at employee homes, and across public mobile networks.

Hillstone Networks has served CISOs well with comprehensive protection — from the edge of the enterprise to core data centers. To meet these new access challenges, we're expanding our edge solutions suite to include zero-trust network access (ZTNA).

Contents



What is ZTNA?

Zero-trust is a model of security that works on the concept of least privilege. Many security solutions today tend to be binary in their access models. If you're inside the perimeter, you're trusted to access (or at least attempt to access) all resources. If you're outside the border, you have zero access.

In a zero-trust model, systems provide the minimal access needed for resources or users to perform their tasks. This is independent of whether the user is inside or outside the perimeter. Zero-trust models are sometimes viewed as perimeter-less security, though in reality, it's more about a software-defined perimeter than no perimeter.

Regardless, under zero-trust, access is blocked by default. Resources that are not explicitly provisioned for access are invisible to the users and rendered unreachable. When extended to network access, zero-trust network access (ZTNA) is an approach that utilizes the identity of users and devices, coupled with other attributes and context to control access to crucial enterprise resources.

Why ZTNA?

By focusing on identity and context, ZTNA allows fine-grained access control to enterprise resources and adapts well to a WFH and WFA world. ZTNA also works in an environment where businesses need to connect with and collaborate with non-employee users like partners.

ZTNA utilizes the identity of a user, their role in the enterprise, their location of access, and device state to grant access to enterprise resources. ZTNA implementations can protect resources anywhere — in branches, in enterprise data centers, in the cloud. It has the flexibility of providing different levels of access privileges based on a combination of attributes. For example, companies can limit employees to read-only versus write access if the employee is connecting from an untrusted public WiFi at an airport. This approach ensures that enterprises are keeping their attack surface as small as possible without impeding employee productivity.

Different flavors of ZTNA

ZTNA can be implemented in different ways. ZTNA is often incorporated into an existing access solution, like a VPN, or as part of an advanced next-generation firewall (NGFW) implementation. This provides immediate benefits for customers who likely have NGFW installed across multiple perimeters.

To enable ZTNA, these solutions add a component in the form of a client agent. These client agents reside on user devices and gather additional information, including whether the device is a registered and valid corporate device (via MAC address, installed software certificate, or hardware trusted platform modules), whether it has antivirus or anti-malware software installed, and whether the device has been recently patched with the latest software updates.

Upon authentication, both the user identity and device information, along with other attributes (time-of-day, location of access, source IP reputation, recent behavior, and activity, resource being accessed) are processed by the policy decision engine, which renders not an outcome of access granted or access denied but may include limitations on that access. Detailed role and group information from corporate directories (Microsoft Active Directory, LDAP) associated with the identity can be used as part of decision-making.

As ZTNA solutions evolve, the advanced logic may be moved into a separate ZTNA broker instance. In this extended architecture, the ZTNA broker is responsible for handling the identity and advanced policies associated with access control and can work in concert with distributed enforcement points like NGFW or other gateway security devices.

ZTNA brokers can be used to control access (via a proxy) into Software-as-a-Service (SaaS) applications in the cloud, protecting not only on-premises assets but applications hosted in the public cloud and private cloud.

The ZTNA broker has global visibility across all enforcement points and gains the ability to perform sophisticated analytics on access requests and on user and device posture and behavior. This can unlock future value for improved analytics around user behavior as part of analyst firm Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) framework to enable continuous and adaptive security.

How ZTNA Complements Existing Security

ZTNA is not a standalone solution but works in concert with existing security and enforcement solutions like NGFW. It helps increase the value of a CISO's investment in perimeter solutions, both in hardware appliance-form and virtualized software packages for private and public clouds. By enabling a more informed access decision and by unlocking finer-grain controls, the CISO is able to up-level the controls built into today's perimeter-based solutions. At the same time, these fine-grained controls help dramatically reduce the threat surface for enterprises, even with users accessing resources from outside corporate environments — from home and on the go. Achieving the desired outcome of more security with more productivity is a massive win for CISOs, especially in today's post-breach world with threats running rampant.

Hillstone's Vision for ZTNA

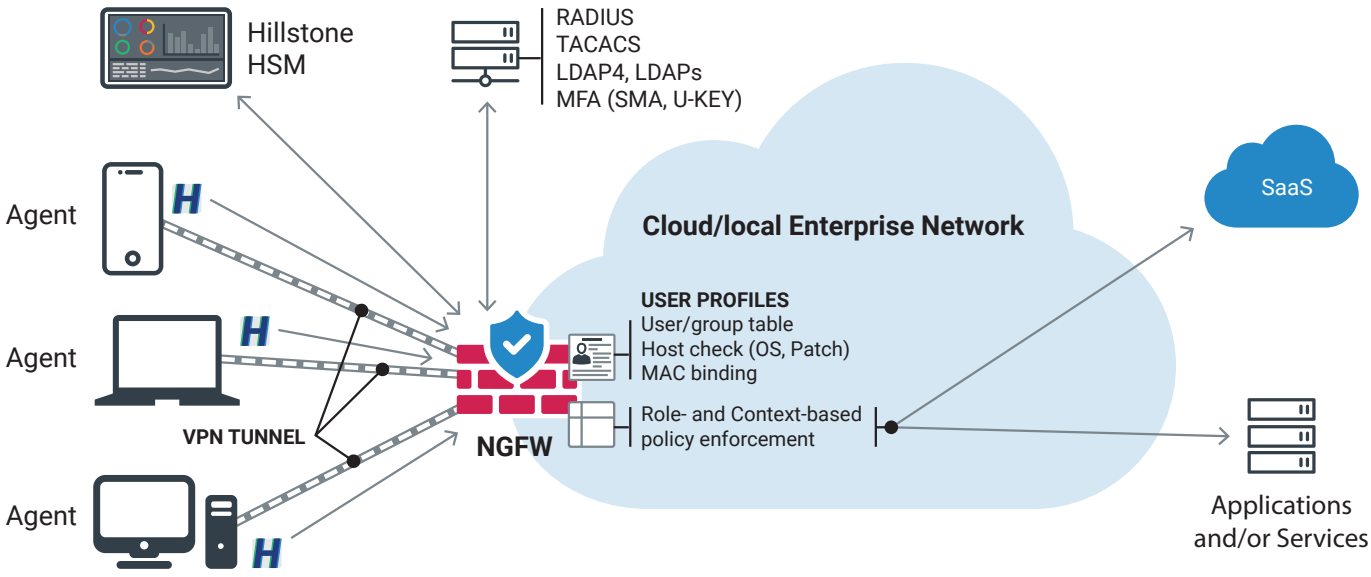
Hillstone's edge solutions provide the most comprehensive security for enterprises worldwide. By adding ZTNA capabilities to our NGFW products, we empower networking and security teams with:

- **Improved visibility** — To **see** what's going on beyond the network traffic level, enabling greater visibility into user, device, and resource access behavior.
- **Advanced intelligence** — To **understand** who is accessing what, zfrom where, and which devices. The added context around user identity, role, group, and device posture allows many finer-grain decisions than before, ensuring more secure decisioning.
- **Distributed enforcement at scale** — ZTNA, whether installed on individual NGFWs (but centrally managed via Hillstone Security Manager) or as part of our future ZTNA broker offering, leverages the power and performance of our NGFWs to **act** rapidly, enforcing fine-grained access policies across the entire enterprise.

See. Understand. Act.

Hillstone combines the capabilities of the Hillstone Security Management (HSM) Platform with our NGFW product line to offer our clients ZTNA features. Hillstone ZTNA supports a wide range of authentication schemes and popular enterprise devices and operating systems. And HSM enables scaled deployment and management.

With ongoing investment into the research and development of our solutions, you can expect rapid evolution of our ZTNA implementation, achieving a broader scale, better intelligence, and more deployment options in the near future.



Diverse User Authentication Schemes

Hillstone's ZTNA supports multiple authentication schemes and identity stores. Integration with authentication, authorization, and auditing (AAA) systems via RADIUS, TACACS+, and support for multi-factor authentication (MFA), including SecureID, allows rapid deployment into enterprise networks. User identity and role information store within enterprise directories (Active Directory, LDAP) can be extracted and used as part of intelligent access policies. For instance, user group information can help determine if subsets of employees should even have network reachability to sensitive corporate systems, such as finance and accounting servers.

Client Authentication Across Major Operating Systems

To ensure complete coverage, Hillstone's ZTNA client agents support all major enterprise operating systems, including Windows, macOS, Linux, Apple iOS, and Android. Hillstone's client agents incorporate extensive checking of devices, including operating system patch levels, MAC address binding, device identity (hardware certificate, software certificate), antivirus software, and browser security and patch levels. Upon initial authentication, all device posture elements are checked against configured policies to provide an intelligent decision on access rights based on user, client and other contextual information.

Continuous Session and Posture Monitoring

Comprehensive ZTNA requires client agents that can reliably report on device posture at initial log in and as part of ongoing validation. Hillstone's agents perform continuous checking to ensure that the device remains in compliance with corporate policies during the entire life of the session. This is of enormous importance in WFH scenarios where laptops might be connected for extended periods of time and where they can get infected even while connected.

Intelligent and Precise Enforcement

By leveraging a proven enterprise-class and carrier-grade NGFW platform, Hillstone ensures that fine-grained enforcement does not disrupt the performance of security devices or employees' productivity. Hillstone's NGFW ZTNA solutions are aided by the intelligent capabilities of our NGFW family, with built-in application intelligence and a rich set of existing features.

Our NGFWs continue to inspect traffic and enforce protection after the initial zero-trust authentication and authorization decision is made, adhering to Gartner's CARTA recommendations and ensuring continuous security

Centralized Management

Hillstone recognizes that a solution that is hard to deploy and maintain will negatively impact CISOs and their overburdened SecOps teams. Hillstone offers centralized policy management and global visibility of ZTNA settings with our Hillstone Security Manager, allowing one-click set-up and deployment from a central console. Our advanced security templates can be deployed simultaneously across multiple remote devices with push-button simplicity. This central control is coupled with an effortless zero-touch deployment that allows units to be brought up in remote locations where experience IT staff might not always be available.

Award-Winning Enterprise-Grade Security Foundation

Hillstone's ZTNA features are substantial, but our true differentiation is that we are a leading security platform. Built from the ground up to be one of the most comprehensive security platforms in the industry, Hillstone's expertise in security shines in our ZTNA solution. With an integrated next-generation firewall, unique breach, and malware detection capabilities, Hillstone's security components are already used by over 20,000 enterprises worldwide and recognized by leading analysts like Gartner across multiple solutions classes. Our extensive set of capabilities, including sandboxing, anti-spam, botnet C&C prevention, IP reputation, application identification, intrusion prevention, antivirus, URL, and content-filtering have been battle-tested in many vertical industries worldwide.

The advantage of using Hillstone's ZTNA solution is that it is built on this trusted and proven secure foundation. And Hillstone will continue to invest in R&D to broaden our ZTNA features. Soon, we will be adding a ZTNA Broker deployment option, allowing cloud-based authentication and control, and helping with the scaling up of distributed deployments. Further, we will evolve user device options, extending the platform to support clientless operation in the near future. This will allow rollout of our ZTNA solution to non-employees or accommodate situations where employees find themselves not near their mobile devices or laptops

With our superior security foundation, Hillstone's ZTNA solution can serve many use cases and industries effectively. While not limited to the use cases that we'll discuss here, we believe that highlighting our unique benefits will translate into ideas on how we can help you regardless of your industry.

For Remote Employees

The WFH reality will not go away. Companies worldwide now realize that employees can be as productive at home as in the office. Many companies expect to retain a blended workplace strategy with a mix of WFH and in-office work. This means that ongoing extended access from home or other remote locations will continue.

Hillstone ZTNA provides the flexibility to accommodate this WFH and WFA world while keeping the attack surface contained. Our ZTNA solution can ensure that only corporate-registered devices are used to access the corporate network and that antivirus software is running, and the operating system is up-to-date. This will help avoid situations where attackers take advantage of a known vulnerability on a system and leverage it as a jumping-off point into corporate systems via remote VPN. Suppose the operating system is not patched and updated. In that case, the employee will either be blocked from accessing the corporate network and asked to remediate separately or put into a quarantine zone with no access to sensitive corporate resources, where they can connect to the internet and other resources helpful in remediating the system.

Similarly, a ZTNA solution will prevent employees from using compromised or home PCs with weak security and no anti-malware agents from connecting to corporate networks, exposing corporate resources to potential infection and attacks.

For Mobile Employees

As the world unlocks, travel will return, and employees will again embrace the flexibility of working from airports, coffee shops, and other locations. Just as ZTNA protects WFH employees, it can defend mobile employees too. With our support for mobile devices, CISOs can mandate tighter security when employees are on the road or in hotels.

ZTNA can ensure that employees get the necessary access to critical information to do their jobs while limiting read or modify access to sensitive data. For example, a corporate finance employee who is traveling might be able to access their email but not allowed to connect to the finance or accounting systems while they are on the road and accessing public locations. Once she arrives at a branch office and is viewed to be in a secured site, she will gain access to the finance systems. This intelligent, context-based, least-privilege approach does an excellent job of managing risk and balancing security against productivity. ZTNA provides CISOs with the tools to surgically implement their policies, as opposed to the blunt hammer of all-access or no-access.

For Government Agencies or Regulated Industries

ZTNA can provide the necessary additional layer of protection for government entities and enterprises with stricter compliance requirements. Both are categories of organizations at higher risk of compromise from malware and ransomware. ZTNA aligns with the philosophy of many of these agencies and industries, who themselves advocate a policy of least-privileged access and a need-to-know, need-to-access mindset.

For example, ZTNA policies can mandate that traveling government employees use multi-factor authentication and trusted devices for remote access. Hillstone can be programmed to block access otherwise or allow limited access to systems like email.

Hillstone's secure platform coupled with ZTNA can be advantageous for these organizations, making remote employee locations like home or mobile employee locations like airports and hotels more resilient to attacks, protecting access to critical data even in the face of potential device compromise.

For Services Providers

Service providers looking to help their customers secure their company IT resources in the face of WFH and WFA will find added value in Hillstone's ZTNA solution. Many small and medium enterprises (SMEs) are under threat from ransomware but have little to no in-house IT expertise. In addition to reliable connectivity for their digital assets, they need help with security. By layering ZTNA on top of Hillstone's NGFW solutions, service providers can provide these SMEs with a value-add managed solution that improves their security posture significantly.

ZTNA can easily be provided as a service to these SMEs, allowing them to benefit from the advanced policies while trusting the service provider to manage the security policies on their behalf.

Why Hillstone?

Hillstone Networks' proven Infrastructure Protection solutions provide enterprises and service providers with the visibility and intelligence to comprehensively see, thoroughly understand, and rapidly act against multi-layer, multistage cyberthreats. Favorably rated by leading analysts and trusted by over 20,000 global companies, Hillstone protects all organizations from the edge to the cloud with improved total cost-of-ownership. With a reputation for "security that works," Hillstone's holistic product suite includes ZTNA, NGFW, breach detection, SD-WAN as well as VM and cloud security. Hillstone's cutting-edge solutions leverage AI/ML and integrate seamlessly into SecOps frameworks, assuring CISOs that their enterprises are well-protected.

Hillstone has been recognized by Gartner 7 years in a row in its Magic Quadrant for Network Firewalls, and included as representative vendor in Market Guide for Network Detection and Response, Market Guide for Intrusion Detection and Prevention Systems, and Gartner Market Guide for Cloud Workload Protection Platforms.

Hillstone NETWORKS

Visit **www.hillstonenet.com** to learn more

or contact Hillstone at **inquiry@hillstonenet.com**