Hillstone
Zero Trust Network Access (ZTNA) Solution Introduction

February, 2023

Reshape.Security

Embrace Cyber Resilience

Digital Transformation Brings New Challenge To Network Security

Cloud Virtualization Containerization BYOD Remote Access IoT M2M

Rapid Changes In Network Bring New Challenges

Evolving Threat Landscape | **Compliance Requirements** | **Data Protection**

Changing Perimeter

Traditional Perimeters

- Connect first, then authenticate
- Firewall based perimeter protection
- Trust anything inside by default

The disrupting Perimeter

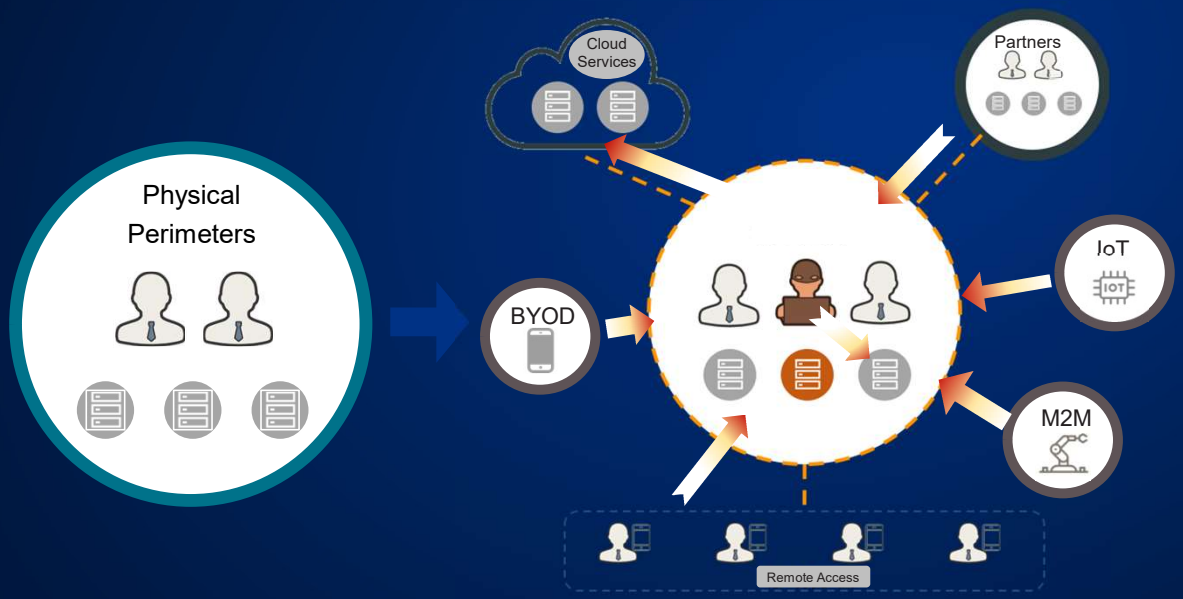
- Out-of-date static FW policies
- Resource-intensive endpoint monitoring
- No identity and context awareness

Challenges From Technology

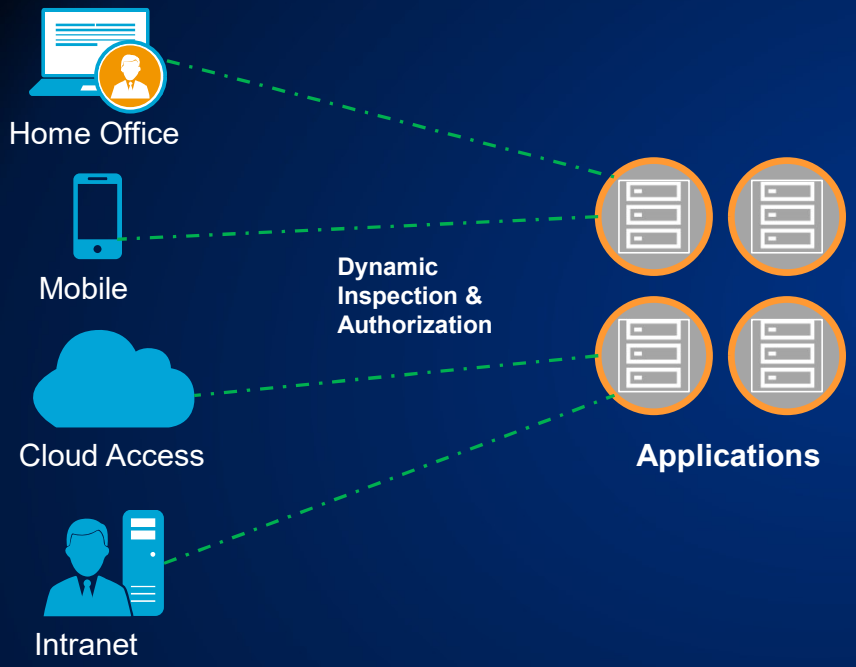
- Cloud Computing
- Network Virtualization
- Known VPN vulnerability

Challenges From Business

- Increased internal devices
- Extended types of users
- Hybrid architectures



ZTNA Matches The Evolving Business Requirements

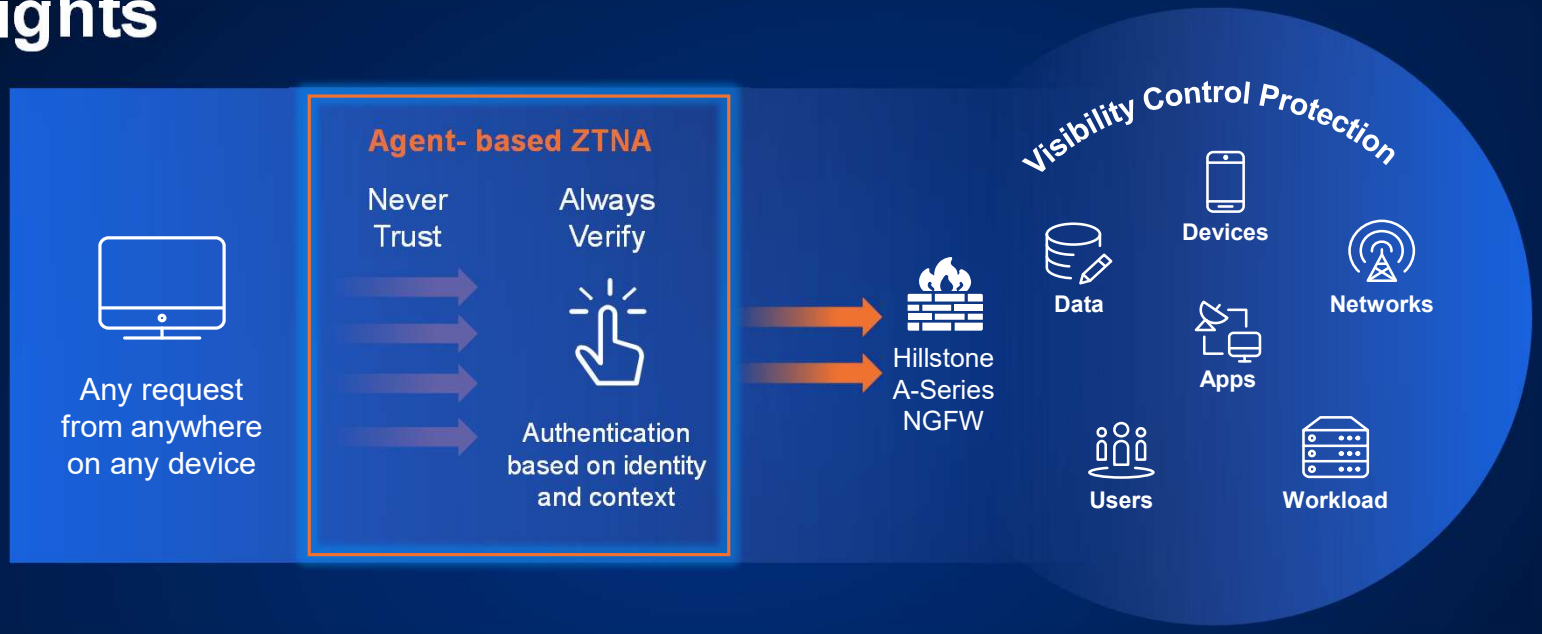


Always Verify, Never Trust

Hillstone ZTNA Brings

- Granular authentication before access
- Limited network connectivity& app exposure
- App-centric & policy-based authorization

Zero Trust Network Access (ZTNA) Solution Highlights

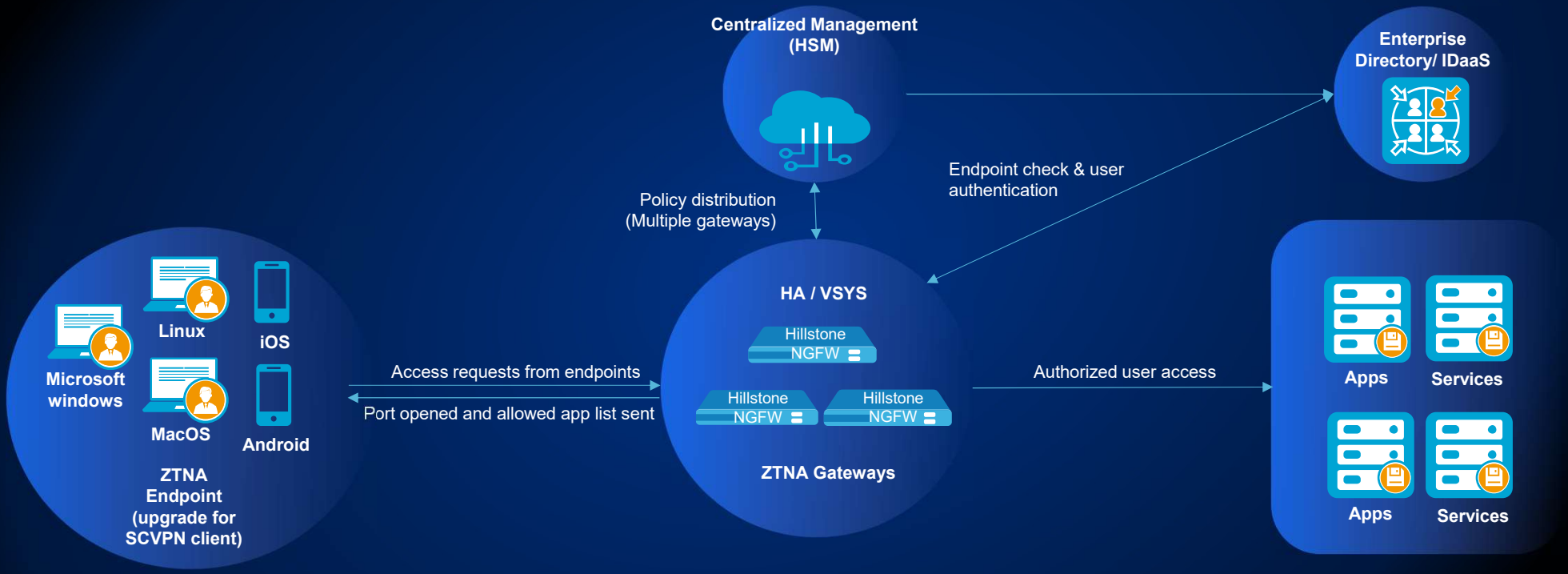


Zero Trust

Highlights

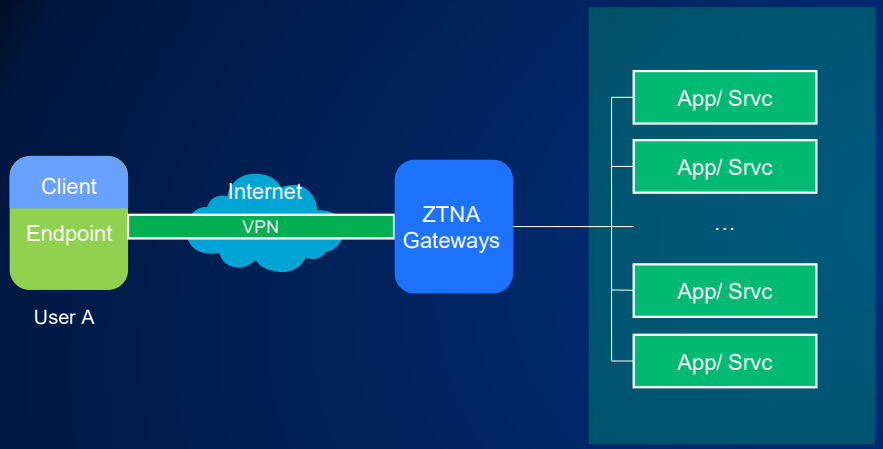
- Identity-Based, Least-Privileged Secure Access
- Context-Aware, Adaptive Access Control
- Centralized and Efficient Management
- Award-Winning Enterprise-Grade Security Foundation

Hillstone ZTNA Solution Architecture



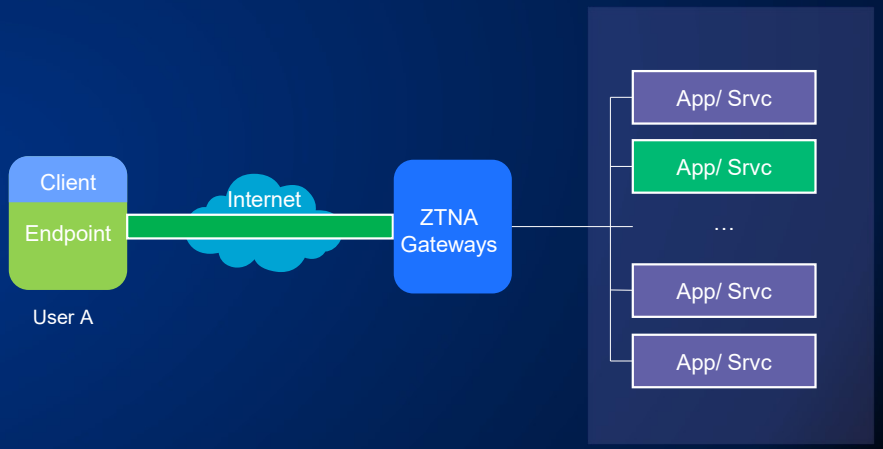
Identity-Aware, Least-Privileged Secure Access

Traditional VPN



Default Trusted
The user's endpoint has the visibility to all the apps/services

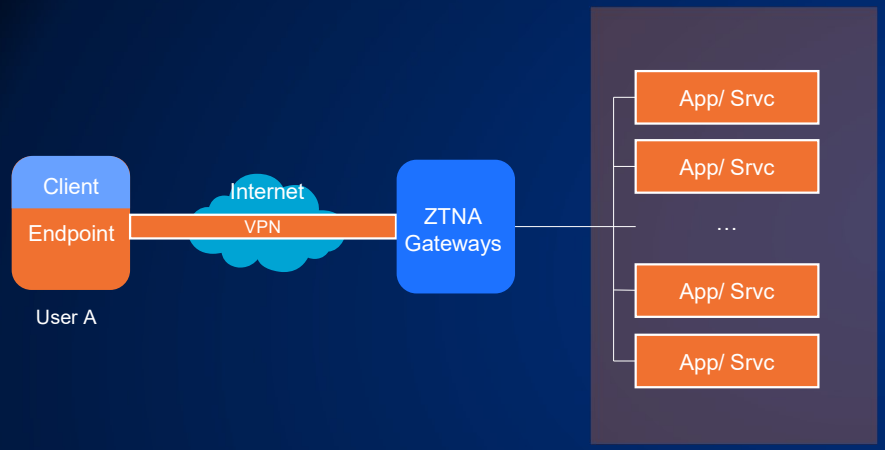
ZTNA



Identity-Aware, Least Privileged
user can only access the authorized apps/services
Single Packet Authorization (SPA) Support
reduce the attack surface and mitigate DoS attacks over TLS

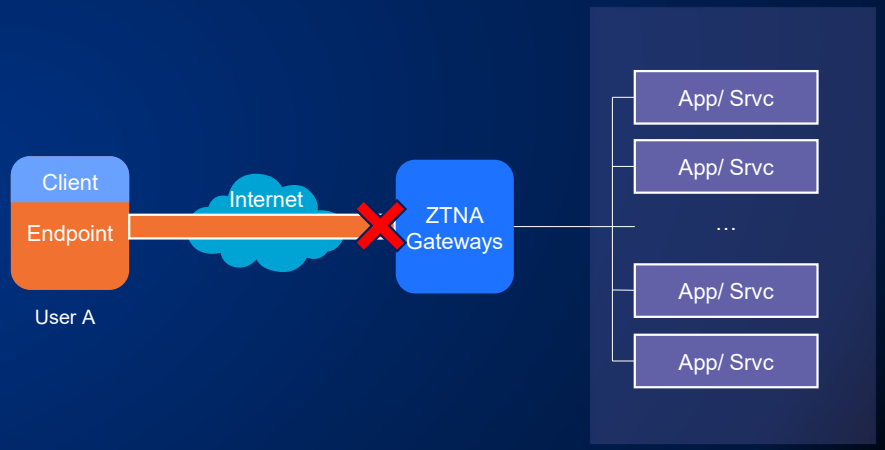
Context-Aware Adaptive Access Control

Traditional VPN



No context awareness
The attacker or malware can easily perform port/ IP scanning and attack the hosts and applications if the endpoint were compromised by spam/ phishing/ malware.

ZTNA



Continuous Trust Evaluation
The ZTNA agent on the endpoint will monitor and evaluate the endpoint's status to see if it is secure for connection.
Once compromised, the endpoint will be blocked by the ZTNA gateway.

Award-Winning Enterprise-Grade Security Foundation

A-Series Next-Gen Firewall

X-Series Data Center Firewall

CloudEdge

Virtual Firewall

Hillstone Next-Gen Firewall Products Highlights

FAST

High Performance

Leading application layer performance meets real network security needs

EFFECTIVE

Advanced Threat Prevention

Protection against known and unknown threats

FUTURE

Scalability as Needed

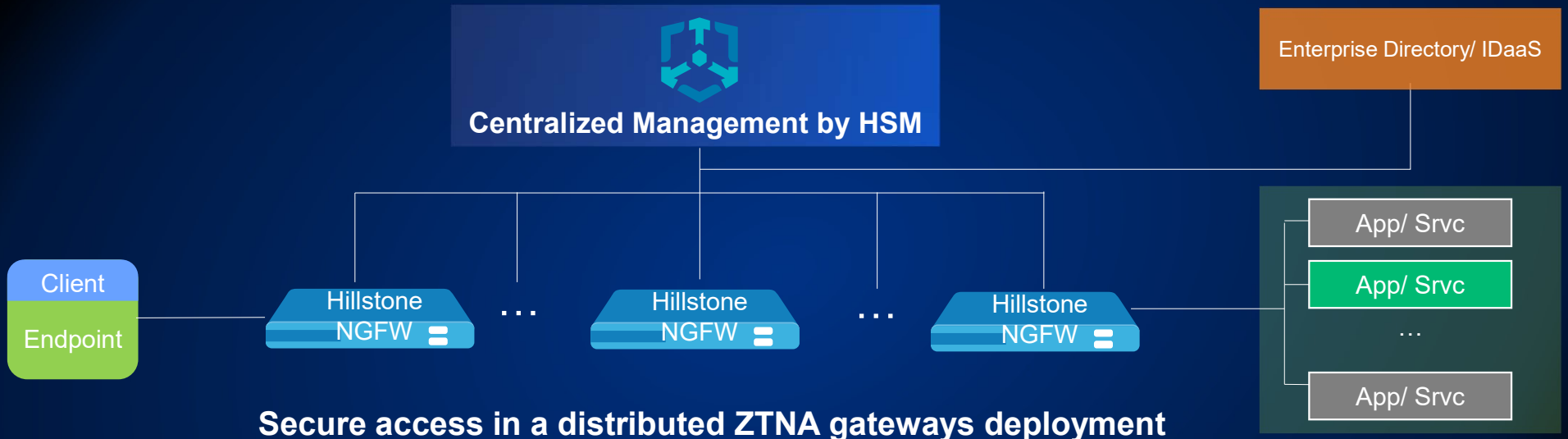
High-density ports ensure excellent access capability, while large storage options allow for deeper analytics and better visibility

EFFICIENT

Smart and Automated Operation

Security operation made easy

Centralized and Efficient Management for ZTNA gateways



Secure access in a distributed ZTNA gateways deployment

Integrated Device Management

Centralized ZTNA Policy Management

Comprehensive Security Monitoring

Comprehensive Endpoint Visibility

Monitor and evaluate the endpoint's status

- OS
- Patch
- AV
- DLP
- Time
- Location

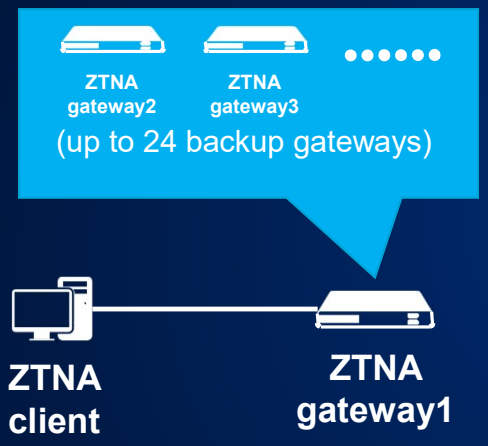
Multiple mainstream OS support

- Microsoft Windows
- Mac OS
- Linux
- iOS
- Android

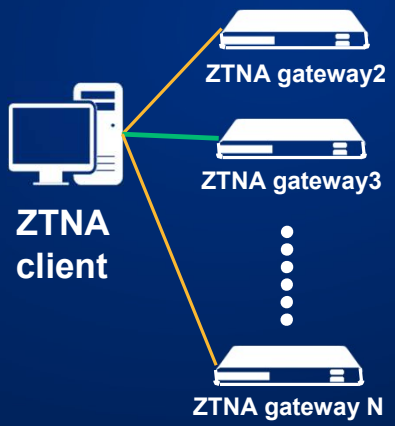
ZTNA Gateway High Availability (Multi-gateway)

Hillstone NETWORKS

Multiple GWs

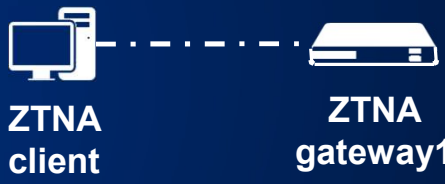


Link quality detection



Multiple GWs

Failover when connecting



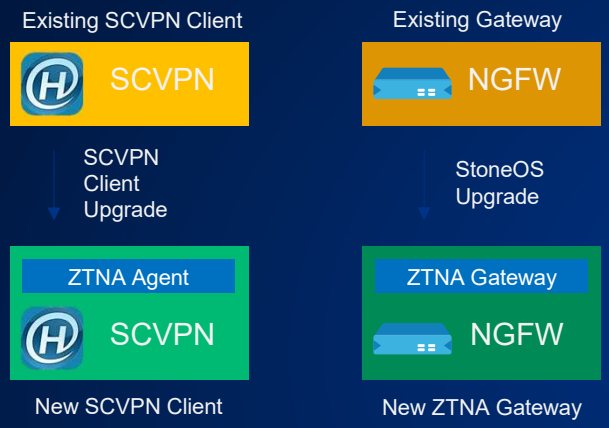
Client will automatically connect to the optimal backup gateway.

Failover when connected

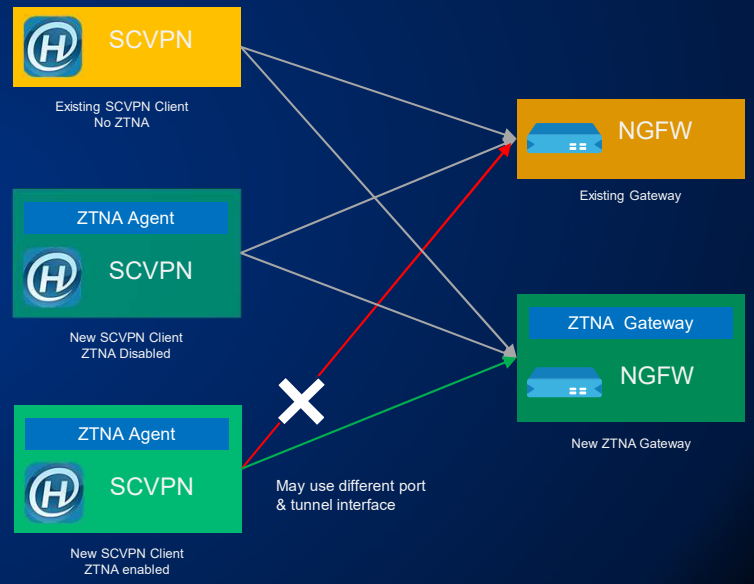
Client will automatically switch to the optimal backup gateway without re-authentication.

Smooth Transition To ZTNA

Just a Software Upgrade



Backward Compatible



- Support the same user authentication services
  (local, LDAP, TACACS+, Radius)
- Support two factors authentication
- Support NGFW HA and VSYS

Typical Use Cases

Remote Office & Mobile Worker

- only authorized devices are allowed to access with least privileges
- The OS is up-to-date & antivirus software is running
- Access will be blocked or limited once compromised
- Reduce the attack surfaces for this blended workplace strategy
- Protect corporate data/ resources/ assets from exposure or loss

Partner Access

- Remote access to proper resources with a secure connection
- Protect the assets of Intranet while enabling necessary access
- Enable easy collaboration without compromising any security

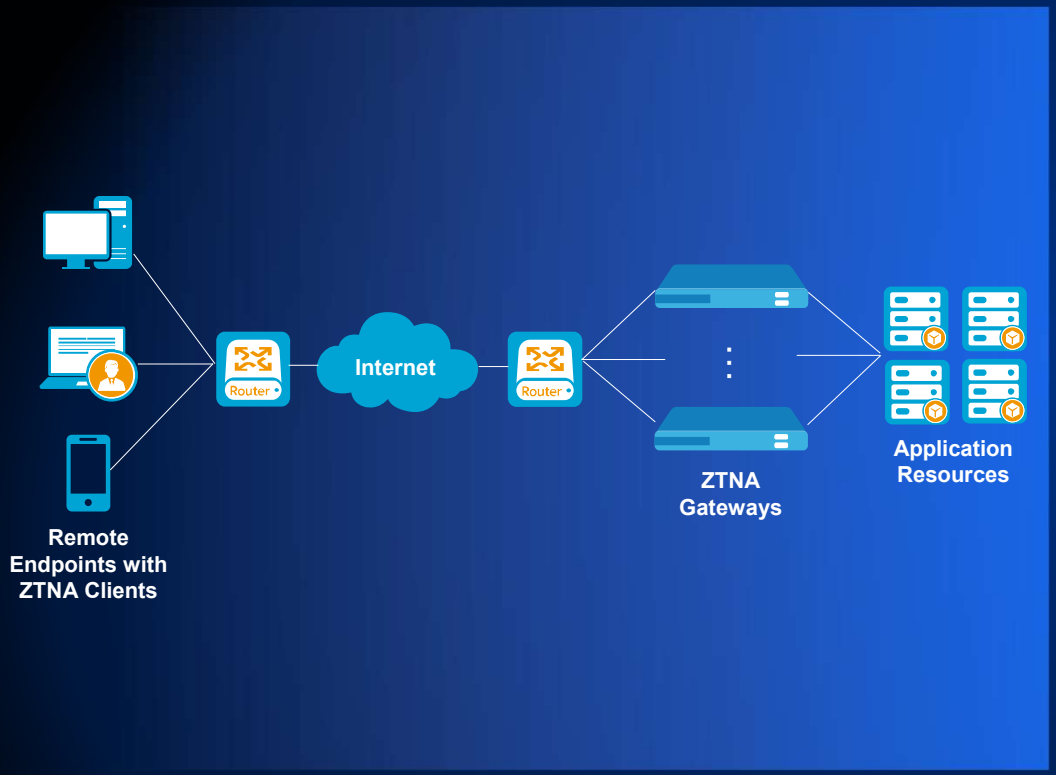
Government Agencies / Regulated Industries

- The security policy with least-privileged access based on a need-to-know, need-to-access philosophy
- Leverage multi-factor authentication and trusted devices for remote access.
- Aligns with the industrial compliance and strict security requirement
- Protect critical data even in the face of potential device compromise

Service Providers

- Enable ZTNA-based security services for customers of small-to-medium organizations.
- Additional add-on security services beyond the reliable and secure connections
- Cost-effective solution without requiring in-house security experts

Customer Cases



Case 1

- **Customer profile:** Financial institution
- **Challenge and requirement:** Since some internal applications are quite sensitive, the access with the least privileges is highly needed to meet different access demands and limitations of various departments
- **Hillstone solution:** Deploy two NGFWs with 400 ZTNA licenses at the perimeter, working as ZTNA gateways. The zero-trust access helps further ensure access security.

Case 2

- **Customer profile:** Telecommunication enterprise
- **Challenge and requirement:** The enterprise has high requirement for remote access, because many departments are located in different places. And there are also some compliance requirements for the operating systems and endpoints, thus traditional SSL VPN can not be applied
  Hillstone solution: Deploy one data center firewall with 250 ZTNA licenses at the perimeter, working as ZTNA gateway. The application of ZTNA enables the zero-trust access of telecommuting for all employees

2023 ZTNA Roadmap

Intranet Access Support

- ZTNA clients connect to firewalls through intranet: supports users authentication without creating tunnels, distributing host routes, creating virtual NICs and assigning IP to the host
- Intranet access control: host information collection, terminal tags matching, ZTNA policy matching and control
- Access to whitelist configuration before authentication

Agentless Access Support

- Supports global portal for agentless access, applicable to scenarios including SSLVPN, ZTNA, and intranet access
- Supports application resources of HTTP/HTTPS proxy, and the application resources are invisible to end users

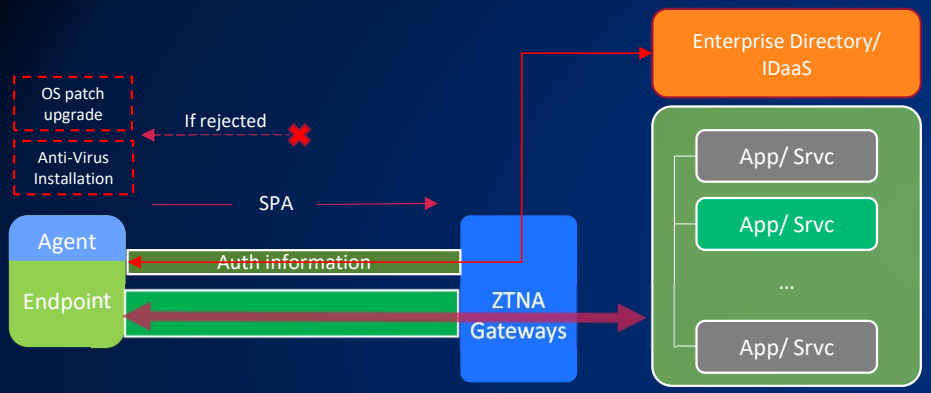
Security that Works!

+1 408 508 6750
inquiry@hillstonenet.com
5201 Great America Pkwy, #420
Santa Clara, CA 95054
www.hillstonenet.com

Hillstone NETWORKS

Single Packet Authorization

What is SPA



Benefits

- Reduce attack surface
- Mitigate DoS attacks over TLS
- Protect assets