
HAFS
Distributeur à valeur ajoutée
VOTRE PARTENAIRE TECHNOLOGIQUE
POUR DES INFRASTRUCTURES IT SÉCURISÉES ET PERFORMANTES
EXPERTISE
Des solutions adaptées à chaque environnement
CONFIANCE
Un partenaire fiable à vos côtés
PERFORMANCE
Des infrastructures sécurisées et évolutives
SUPPORT
Un accompagnement technique de qualité
HAFS
Distributeur à valeur ajoutée
Des solutions IT innovantes pour un monde connecté et sécurisé
WIRELESS RADIO
Connectivité sans fil haute performance
RÉSEAUX & SÉCURITÉ IT
Des réseaux fiables et sécurisés
VIRTUALISATION CLOUD
Des solutions Cloud flexibles et évolutives
CYBERSECURITY
Protéger vos données et vos systèmes
VIDÉO PROTECTION
Solutions de vidéosurveillance intellligentes
HCI STOCKAGE SAUVEGARDE
Stockage, sauvegarde et haute disponibilité
SOLUTIONS IT | CYBERSÉCURITÉ | CLOUD | INFRASTRUCTURE RÉSEAU | STOCKAGE | PROTECTION

Agenda

- Hillstone Networks cooporate overview
- Introduction to the A-Series NGFW
- Gateway ZTNA solution overview
- Demo ZTNA

Global Presence Across 60+ Countries

Hillstone Regional Offices

Hillstone Customer Territories

Business Snapshot

2006 Founded by NetScreen Veterans	**340+** Core Patents (authorized/pending)	**280K+** Hardware Devices Shipped
26,000+ Customers	**100+** Fortune 500 Customers	**60+** Countries
2000+ Employees Worldwide	**30%+** Employees in R&D	**3** R&D Centers in US & China

Over a Decade of Continuous Innovation

2008 - 2009
One of the first vendor released multicore firewall

2010
One of the first 100G firewall platform in the industry

2013
360G fully distributed firewall architecture

2014
First vendor to release an AI-based firewall

2015
CloudHive, one of the first solutions to support Openstack & Vmware

2016
CloudEdge, first virtual NGFW supporting major public clouds and NFV

2017
AI-based NDR Solution

2018
1T Data Center Firewall Platform

2019
Secure SD-WAN Solution

2021
AI-powered XDR Solution

2022
CWPP Solution: CloudArmour

2023
3.5T Data Center Firewall Platform

ZTNA

Centralized Security Analytics, Management and Operations

iSource
Hillstone Security Operation Platform

HSM/vHSM
Hillstone Security Management Platform

HSA/vHSA
Hillstone Security Audit Platform

CloudView
Cloud Security Monitoring & Analytics

EDGE PROTECTION

A-Series
Next-Gen Firewall (NGFW)

X-Series
Data Center NGFW

S-Series
Network intrusion Prevention System (NIPS)

CLOUD PROTECTION

CloudArmour
Cloud Workload Protection Platform

CloudHive
Micro-segmentation Solution

CloudEdge
Virtual NGFW Solution

SERVER PROTECTION

I-Series
Server Breach Detection System (sBDS)

APPLICATION PROTECTION

AX-Series
Application Delivery Controller (ADC)

W-Series
Web Application Firewall (vWAF)

SD-WAN

ZTNA

Micro-Segmentation

CWPP

NDR

XDR

A Visionary in the Gartner Magic Quadrant for Network Firewalls

4 Consecutive Years of ***Customers' Choice*** in the Gartner Peer Insights Voice of the Customer for Network Firewalls

Strong Performer in the 2023 Gartner Peer Insights Voice of the Customer for Network Detection and Response

Introducing the Hillstone Future-Ready A-Series Next Generation Firewall

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

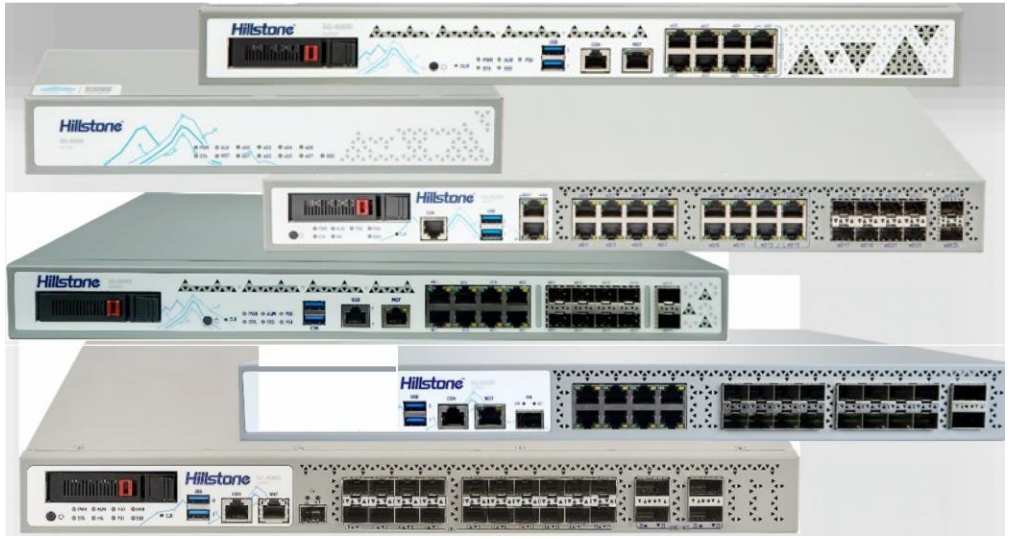
A Future-Ready NGFW

A-Series with Advance Hardware Architecture

- High Performance
- Excellent Expansion Capability
- Advanced Threat Protection
- Smart Policy Operation
- Multiple Deployment Scenarios

The Hillstone A-Series: An Overview

Product name:
SG-6000-A-Series NGFW



Product Highlights

- Built on a new generation of firewall hardware architecture.
- Excellent application security protection performance, high-density ports, large-capacity local and optional expansion storage, at a better TCO.
- Based on Hillstone innovative operating system, StoneOS.
- Hillstone's evolution in AI will continue to provide robust advanced threat detection in the future.

Better Analytics and Visibility with Increased

eMMC (4/8/64GB)
Standard

- Store configuration files, signature databases, images, etc.
- Store network/event/configuration logs, reports
- Cloud Sandbox logs or threat logs should be sent to HSM, HSA or CloudView for longer term storage
- The storage size of each module is specified by the system and cannot be configured

eMMC (8/64GB)
Standard

\+

Hard Drive (256GB to 1.92TB)
Optional

- eMMC stores:
  - configuration files, signature databases, images, etc.
- Hard drive stores:
  - Network/event/configuration/threat/cloud sandbox logs (up to 6 months)
  - More comprehensive reports
- More analytics capability, including IPS threat packet capture
- The storage size of each module is specified by the system by default, and it can be configured

Platform	A200-IN	A200W-IN	A1000-IN	A1100-IN	A2000-IN	A2600-IN	A2700-IN	A2715-IN	A2800-IN	A2815-IN	A3000-IN	A3600-IN	A3615-IN	A3700-IN	A3800-IN	A3815-IN	A5100-IN	A5155-IN	A5200-IN	A5255-IN	A5500-IN	A5555-IN	A5600-IN	A5800-IN	A6800-IN	A7600-IN
Local Storage	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	0	0	256 GB SSD	256 GB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD	480GB / 960GB / 1.92TB SSD

Excellent Access Capability with Advanced Interface

Hillstone NETWORKS

Interface Highlights

- Large amount of fixed, high-speed I/O ports (high-density up to 4 QSFP28)
- A2715-IN/A2815-IN/A3615-IN/A3700-IN/A3800-IN/A3815-IN/A5K-IN/A6800-IN/A7600-IN models support expansion
- Native bypass pairs in A1100-IN/A2K-IN/A3K-IN/A5K-IN rackmount models
- All rackmount models provide two USB3.0 interfaces

Benefits

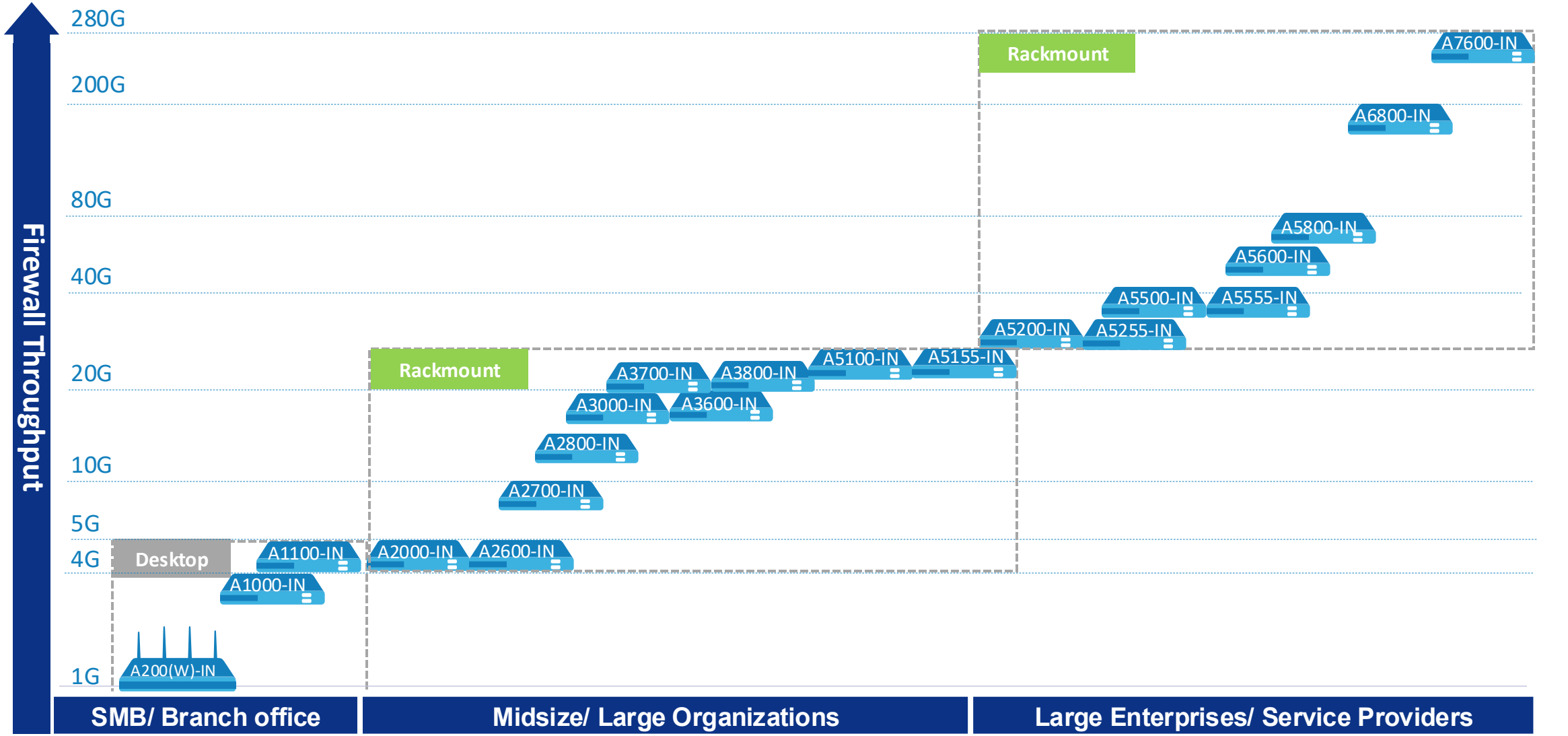
- NGFW can also act as a switch and router; fast data rate support
- Throughput increase by adding expansion module : A3700-IN/A3800-IN: 20 Gbps -> 30 Gbps, A5100-IN/A5155-IN: 25 Gbps -> 50 Gbps, A5200-IN/A5255-IN: 32 Gbps -> 65 Gbps, A5500-IN/A5555-IN: 40 Gbps -> 80 Gbps, A5600: 60 Gbps -> 85 Gbps, A5800-IN: 80 Gbps -> 95 Gbps, A7600: 280 Gbps -> 320 Gbps
- Bypass capability ensures business continuity
- 4G access capability

Value

- Cost Savings
- Increased Performance
- High Availability
- Future Ready

Platform	A200-IN	A200W-IN	A1000-IN	A1100-IN	A2000-IN	A2600-IN	A2700-IN	A2715-IN	A2800-IN	A2815-IN	A3000-IN	A3600-IN	A3615-IN	A3700-IN	A3800-IN	A3815-IN	A5100-IN	A5155-IN	A5200-IN	A5255-IN	A5500-IN	A5555-IN	A5600-IN	A5800-IN	A6800-IN	A7600-IN
Fixed I/O Ports	5 * GE, 1 * SFP	5 * GE, 1 * SFP	4 * GE	8 * GE(RJ45) (1 bypass pair)	8 * GE(RJ45) (1 bypass pair)	8 * GE(RJ45) (1 bypass pair)	2 * SFP+ 8 * SFP 8 * GE	8 * SFP, 8 * GE (2 bypass pairs)	2 * SFP+ 8 * SFP 8 * GE	8 * SFP, 8 * GE (2 bypass pairs)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	8 * SFP, 8 * GE (2 bypass pairs)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	2 * 10GE(SFP+) 8 * GE(SFP) 16 * GE(RJ45) (2 bypass pair)	8 * SFP, 8 * GE (2 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE（2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE（2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	6 * SFP+, 16 * SFP, 8 * GE（2 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE (4 bypass pairs)	2 * QSFP+, 16 * SFP+, 8 * GE(RJ45) (4 bypass pairs)	4 * QSFP28 (or 2 * QSFP+, 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP	4 * QSFP28 (or 2 * QSFP+, 2 * QSFP28) 12 * SFP+ 8 * SFP+/SFP
Wi-Fi/ 4G Dongle	4G Dongle	IEEE802.11 a/b/g/n/ac, 4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	4G Dongle	N/A	N/A
Expansion Slots	-	-	-	-	-	-	-	1	-	1	-	-	2	1	1	2	1	1	1	1	1	1	1	1	1	1
Expansion Module Option	-	-	-	-	-	-	-	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN	-	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN	-	-	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN IOC-A-4SFP+-IN IOC-A-2QSFP+-IN IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-F-4SFP+-IN IOC-A-F-8SFP+-IN IOC-A-F-8GE-IN IOC-A-4SFP+-IN IOC-A-2QSFP+-IN IOC-A-2MM-BE-IN IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN	IOC-A-4SFP+-IN, IOC-A-2QSFP+-IN, IOC-A-2MM-BE-IN, IOC-A-2SM-BE-IN
USB	1 × USB2.0	1 × USB2.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0	2 × USB3.0

A-Series Product Positioning



Advanced Threat Protection for Known and Unknown Malware

IPS blocks vulnerability exploitation

IP Reputation blocks risky IPs from accessing servers

URL Filtering controls user access to specified websites

Anti-Virus filters viruses in files of different types and over different protocols

Anti-Spam classifies and prevents potential spam

Anti-Virus responds to known

Cloud Sandbox responds to unknown viruses

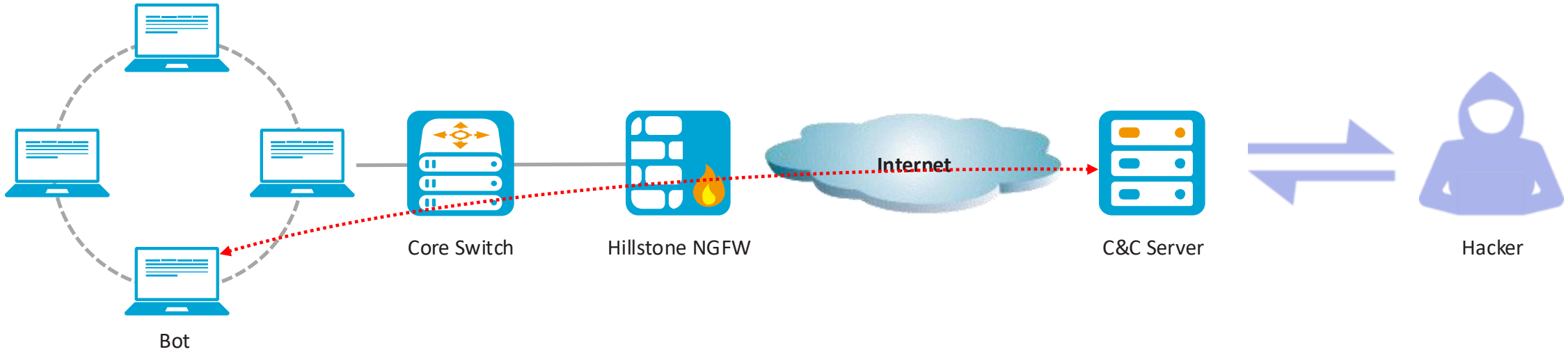
Botnet C&C Prevention blocks the control channel and catches intranet bots

Pre-breach | **Breach** | **Post-breach**

Intrusion Prevention | IP Reputation | URL Filtering | Anti-Spam | Anti-Virus | Cloud Sandbox | Botnet C2 Prevention

Application Control

Complete Botnet C&C Prevention



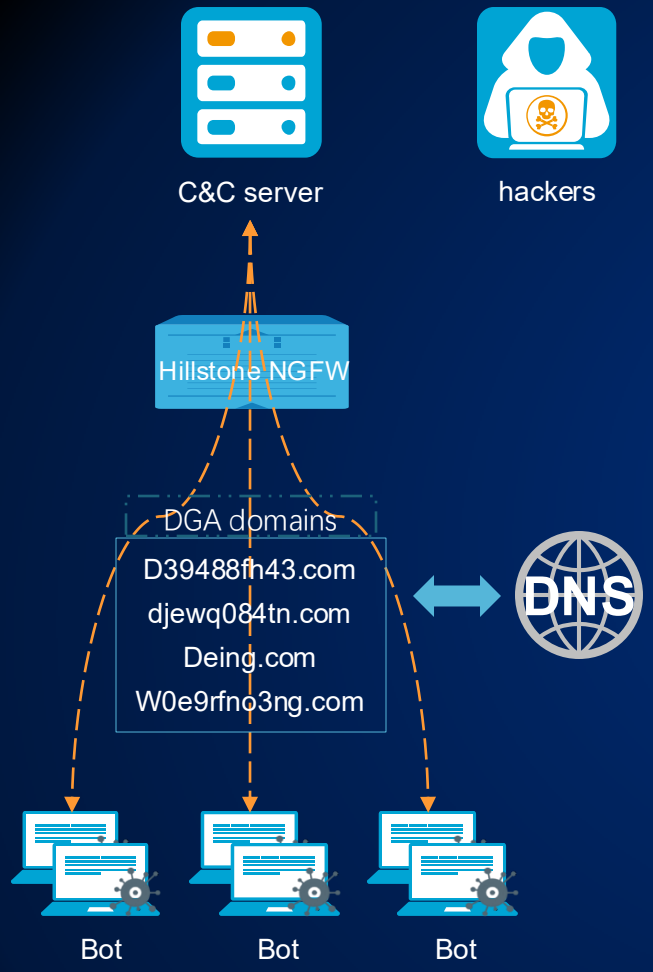
C2 Address Database

DNS Sinkhole Detection

DNS Tunnel Detection

DGA Domain Detection

ML powered DGA optimization



Improved detection accuracy

- New Machine learning based algorithm for detection model
- New characters of the algorithm introduced

Live update of the detection model

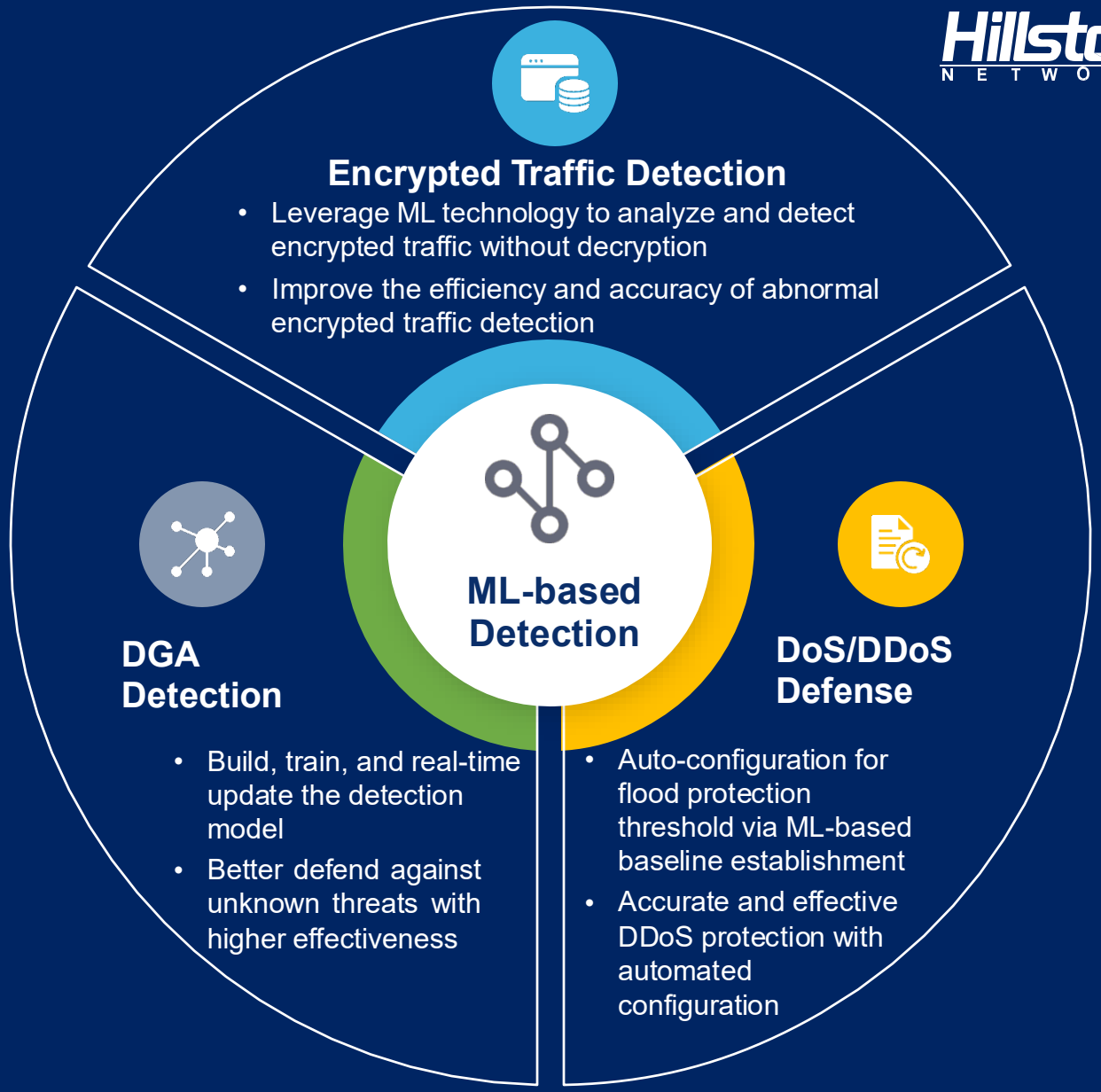
- Trained with latest DGA domain database
- Live update of the detection model every week

ML-based Intelligent Treat Detection and Protection

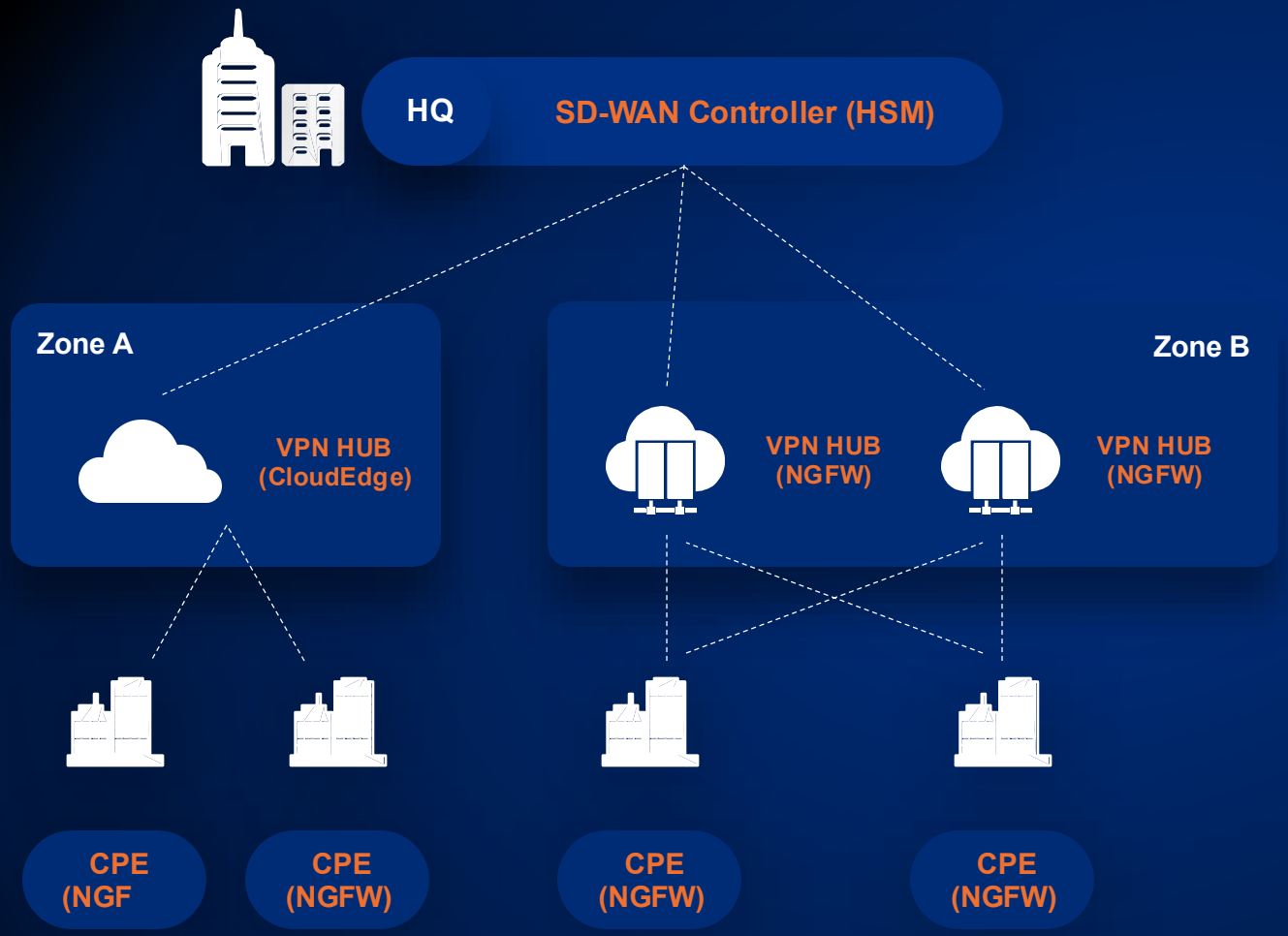
Encrypted Traffic Detection

DoS/DDoS Defense

DGA Detection



Hillstone Secure SD-WAN Solution Overview



SD-WAN Controller

HSM at HQ

- Full range of HSM products

VPN HUB

Hillstone NGFW at Hub or CloudEdge in the cloud

- Mid to high-end series of firewalls or CloudEdge

CPE

Hillstone NGFW at each branch

- Low-end series of firewalls

Enable Multiple Use Cases with High Performance

Network Edge

- Powerful network security capabilities to defend agai n more advanced threats
- Expedited execution of various security services wi strong CPU power

Data Center

- High throughput to handle massive volumes of traffic in data center
- Twin-mode HA maintains high reliability of data center communication

SD-WAN

- High security performance of built-in NGFW brings faster, lower-cost and secure local internet connections at remote location

Remote Access with ZTNA

- Context and identity-aware, and least-privileged secure access control guarantee the security and effectiveness for the remote access

Hillstone ZTNA: Build Zero Trust into Your Security

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

Digital Transformation Brings New Challenge to Network Security

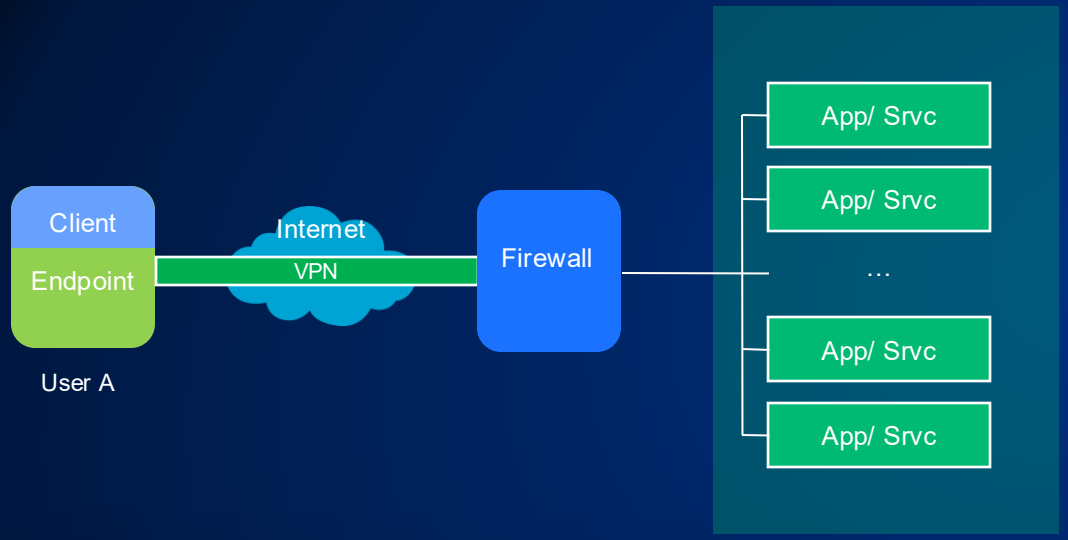
Cloud | Virtualization | Containerization | BYOD | Remote Access | IoT | M2M

Rapid Changes In Network Bring New Challenges

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

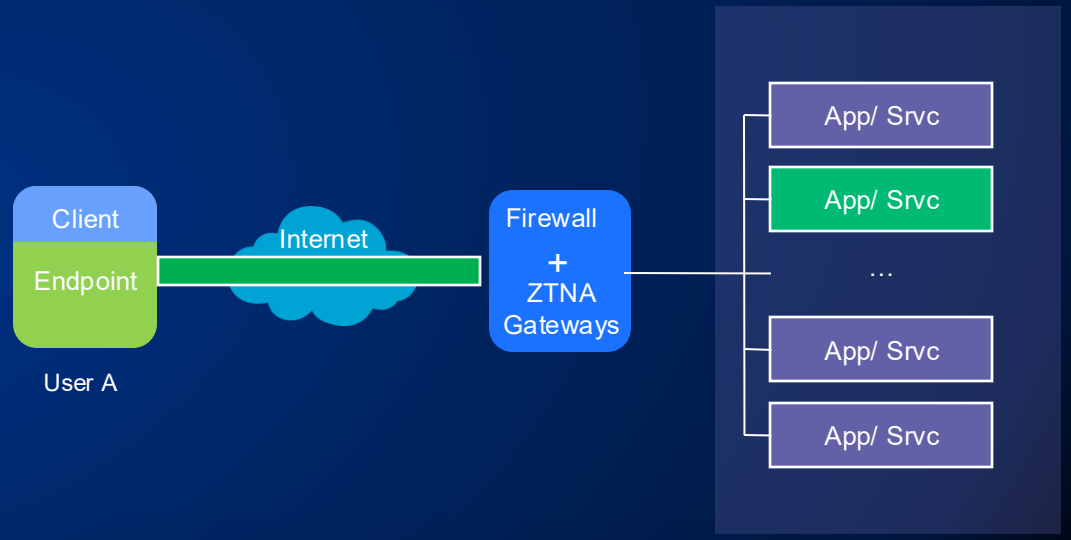
Identity-Aware, Least-Privileged Secure Access

Traditional VPN



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

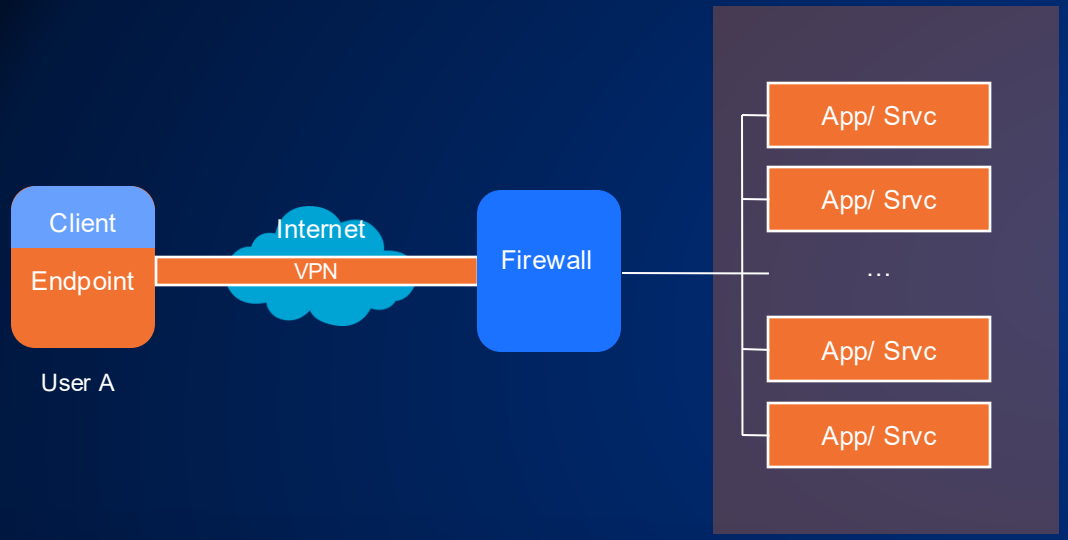
ZTNA



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

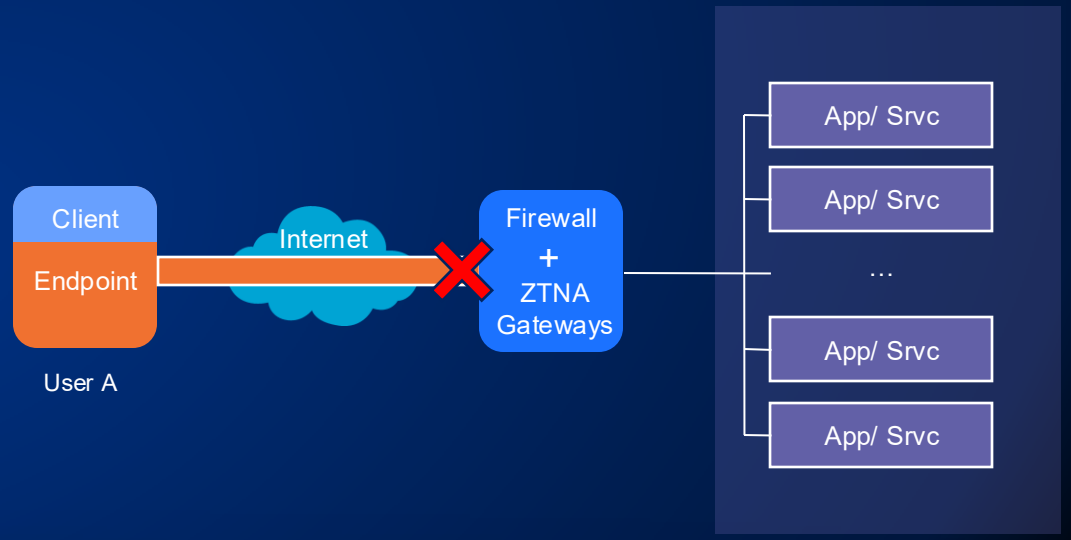
Traditional VPN



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.

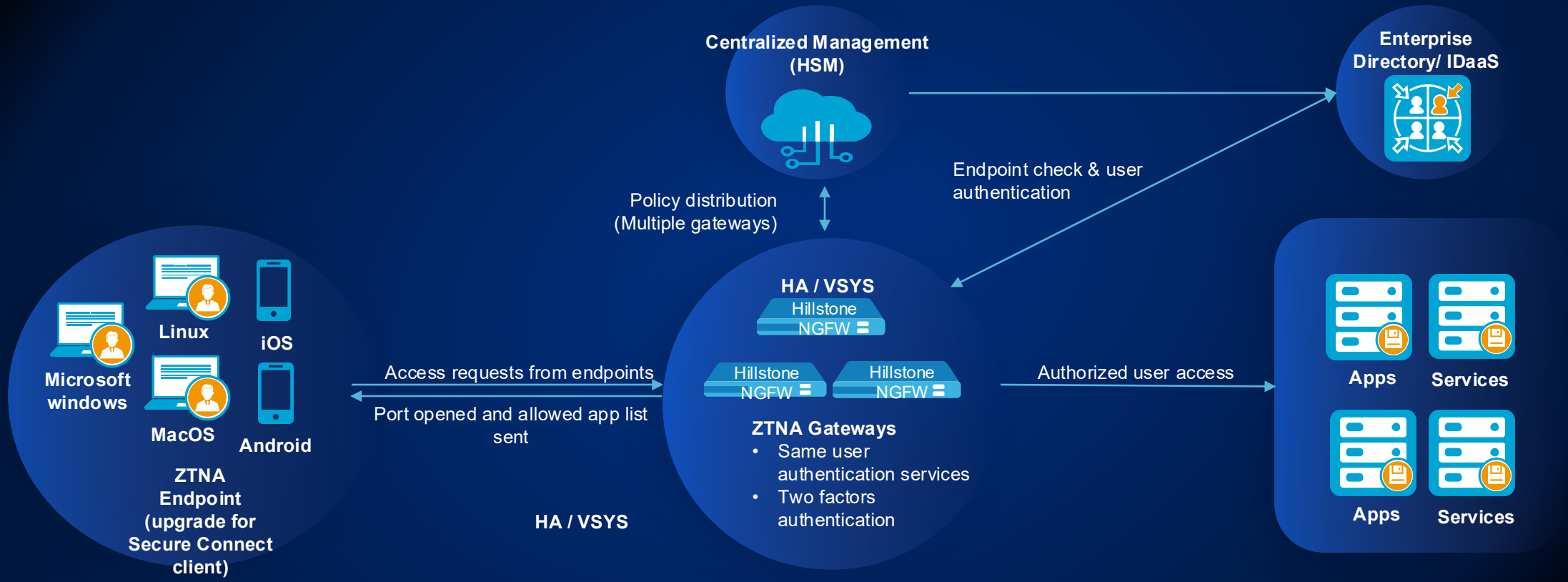
ZTNA



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.

Hillstone ZTNA Solution Overview



Hillstone ZTNA Solution Highlights

Always Verify, Never Trust

- Identity-Aware, Least-Privileged, Secure Access
- Context-Aware Adaptive Access Control
- Award-Winning, Enterprise-Grade Security Foundation
- Centralized and Efficient Management
- High Availability of Distributed ZTNA Gateways
- Single Packet Authorization

Hillstone's NGFW in ZTNA Solution

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

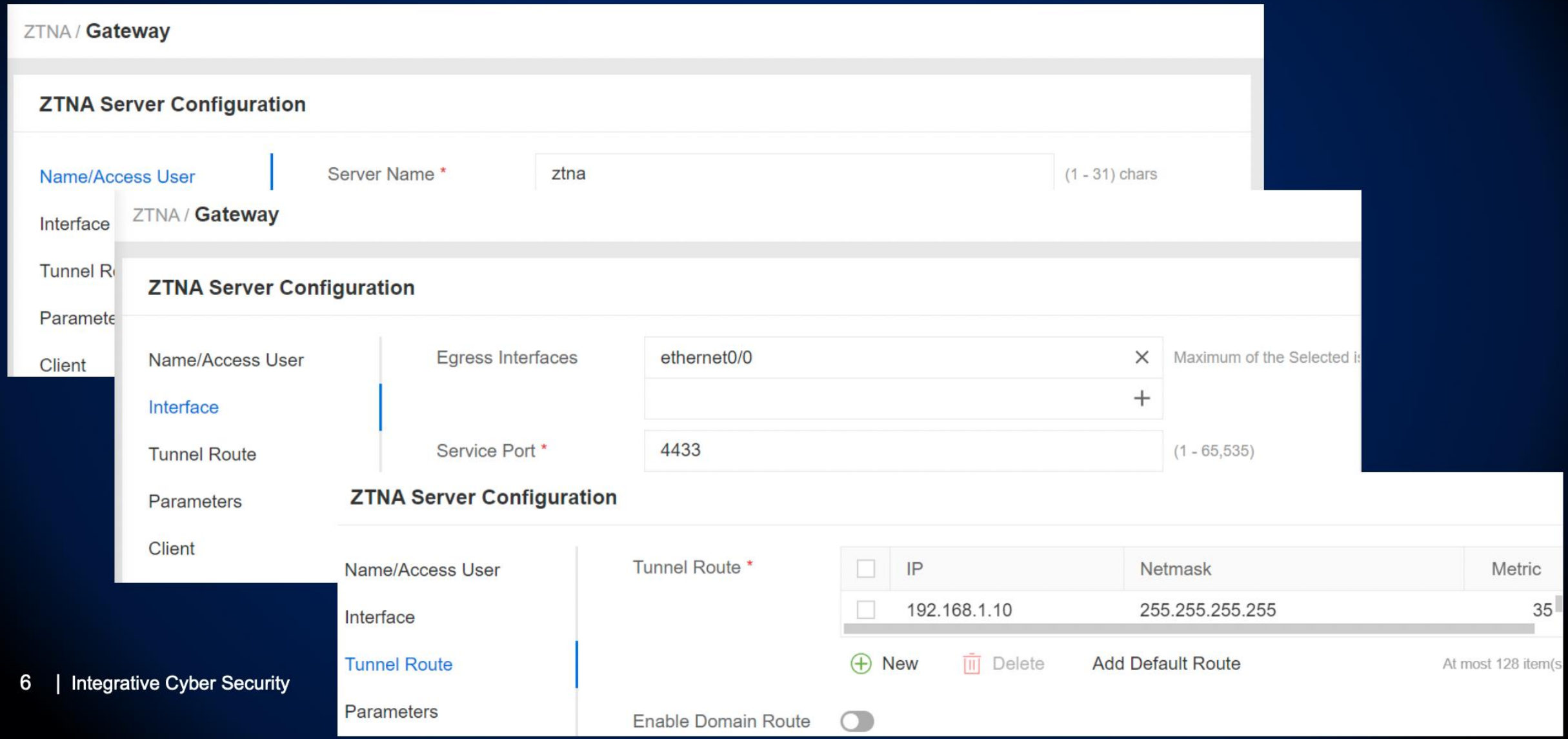
EFFICIENT

Smart and Automated Operation

Security operation made easy

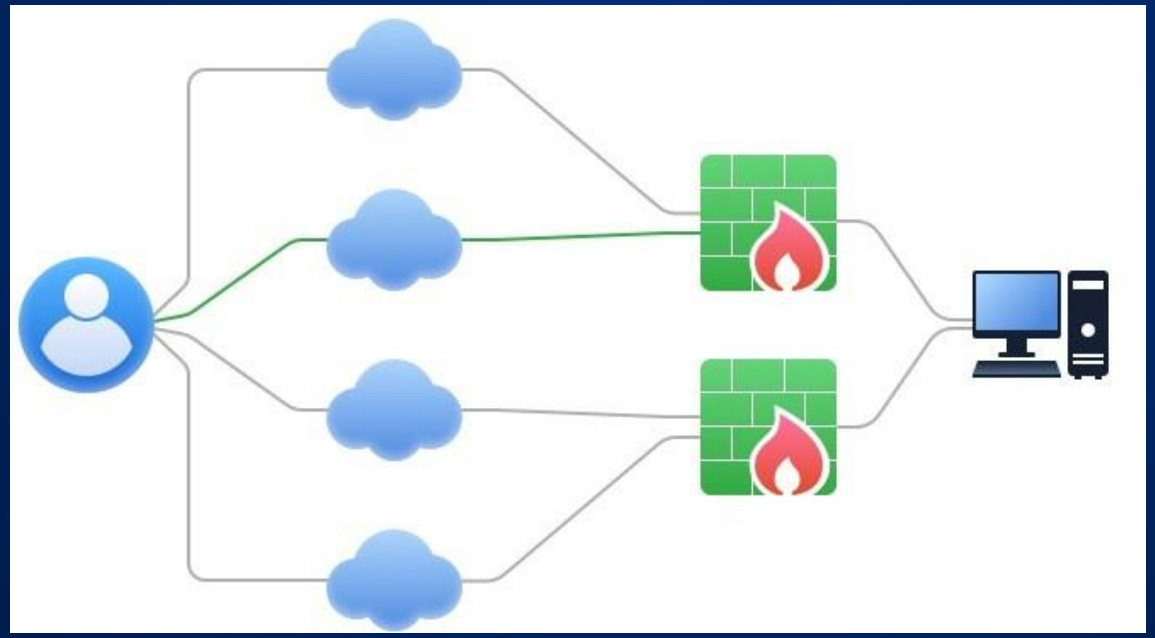
ZTNA Gateway

ZTNA Gateway



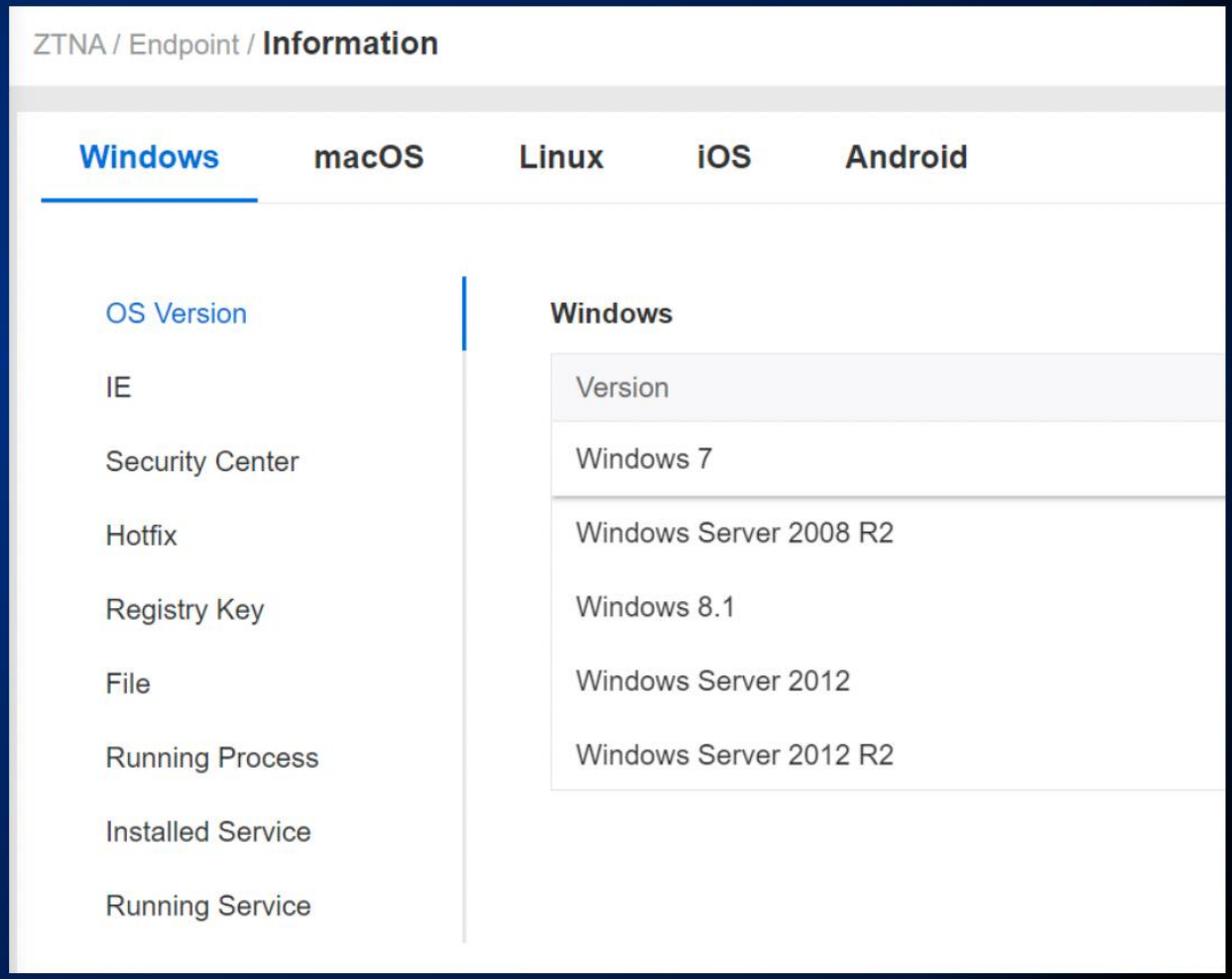
Multi-gateway Address Scenario

- To prevent single point failure, enterprises adopt technologies such as multiple public network exits and High Availability (HA) redundancy to ensure the continuity of their services.



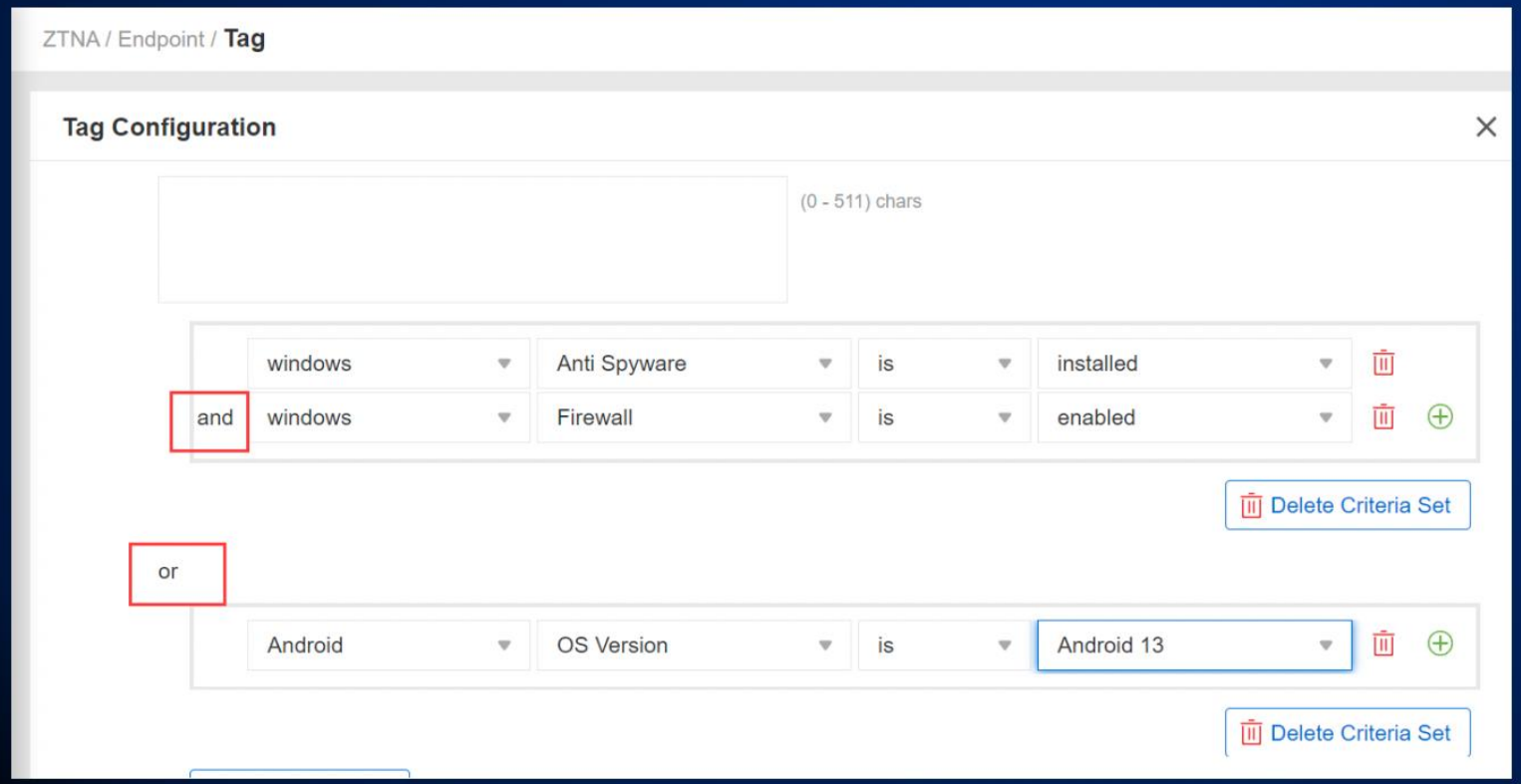
Endpoint Information

- The StoneOS has built-in the endpoint information database file, which defines the endpoint information items that can be collected, and the enpoint information database can only be upgraded by upgrading the StoneOS version.
- Supported systems:
  - Windows
  - MacOS
  - Linux
  - IOS
  - Android

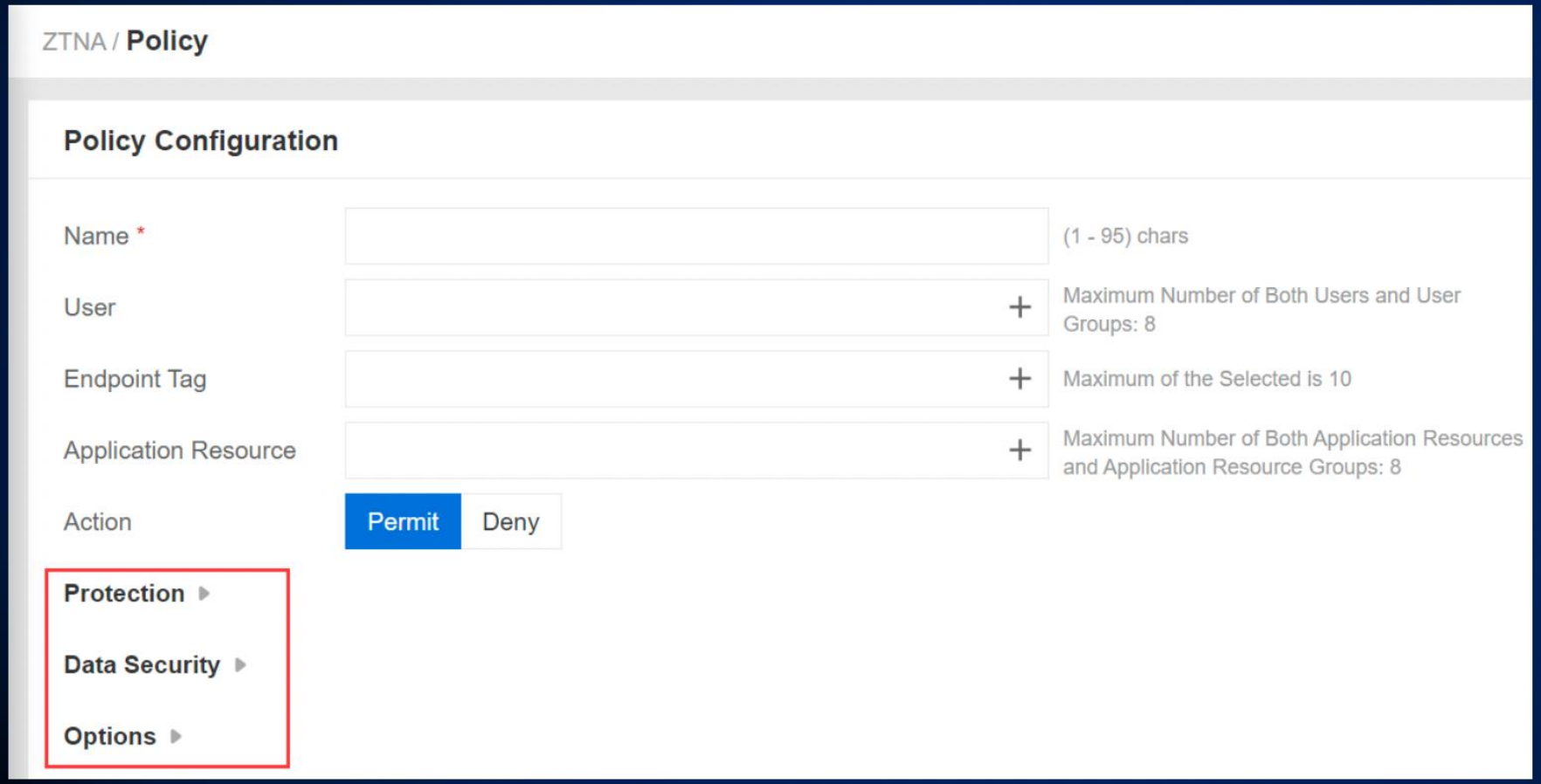


Endpoint Tag

- Endpoint tags are used to identify the status of a user's endpoint. The firewall will assign corresponding endpoint tags based on the endpoint information carried by the user. These tags will be used as matching conditions for ZTNA policies.



ZTNA Policy



ZTNA Policy Matching

- Match from top to bottom

Matching Conditions	User/User Group	When the user's username or the user group to which the user belongs matches the username/user group bound in the ZTNA policy, the policy is considered to have been hit in this dimension.
	Endpoint Tag	When the user's endpoint tag matches the endpoint tag bound in the ZTNA policy, it is considered a hit in this dimension.
	Application Resource/Application Resource Group	When the application resources accessed by the user match the application resources or application resource groups bound in the ZTNA policy, it is considered a hit in this dimension.
	Schedule	When user's access time matches the effective time of the schedule bound in the ZTNA policy, then it is considered a hit in this dimension.
	Usage Status	It will only be matched when ZTNA Policy's status is enabled
Actions	Permit	When traffic matches the specified ZTNA policy, access to the application resources bound in the policy is allowed.
	Deny	When traffic matches the specified ZTNA policy, access to the application resources bound in the policy is denied.
	Default Action	If traffic does not match any ZTNA policy, it will hit the default ZTNA policy and be processed according to the control actions configured in the default policy.

ZTNA License

The ZTNA function is usable by default.

- A new ZTNA license can expand the maximum number of online ZTNA users.
- The X series and K9180 have 128 built-in ZTNA concurrent users, while other platforms have 8 built-in ZTNA concurrent users.

SG-ZTNA-IN-0010	10-user ZTNA License	ZTNA license for 10 concurrent users
SG-ZTNA-IN-0025	25-user ZTNA License	ZTNA license for 25 concurrent users
SG-ZTNA-IN-0100	100-user ZTNA License	ZTNA license for 100 concurrent users

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

More Than 26,000 Customers from All Verticals

Global Technology Certification and Validation

Hillstone's complete range

Département Commercial

WCA

HAFS

Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY Vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision