



**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
intelligentes



**HCI STOCKAGE
SAUVEGARDE**

Stockage, sauvegarde
et haute disponibilité

SOLUTIONS IT

CYBERSÉCURITÉ

CLOUD

INFRASTRUCTURE RÉSEAU

STOCKAGE

PROTECTION

Hillstone Security Management (HSM) for SD-WAN



Reshape.Security
Embrace Cyber Resilience

Agenda

1

Business Problems

2

Hillstone HSM Value Proposition

3

Hillstone HSM Portfolio

4

Deployment Scenarios & Winning Cases

Business Problems

Digital Transformation and Cloud Adoptions Brings New Challenges



Security Operation Management

- Security Devices Sprawl
- Policy Configuration Complexity
- Infrastructure Upgrade Inefficiency

SD-WAN Management

- Fast Network and Business Evolving
- No Visibility into Business Traffic
- Evolving Network Security Challenges

Secure Access Control

- Evolving Threat Landscape
- Compliance Requirements
- Data Protection

Lack of Adequate Tools For Centralized Monitoring and Management

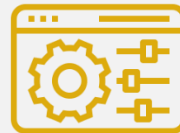
Security devices sprawl

Too many security devices lacking effective centralized management greatly reduces the efficiency of O&M.



Policy configuration complexity

- Manual configuration of large amounts of complex security policies and routing configuration might lead to mistakes.

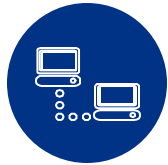


Infrastructure upgrade inefficiency

Repetitive operations of software upgrades and signature upgrades result in operation inefficiency.



Fast Network and Business Evolving



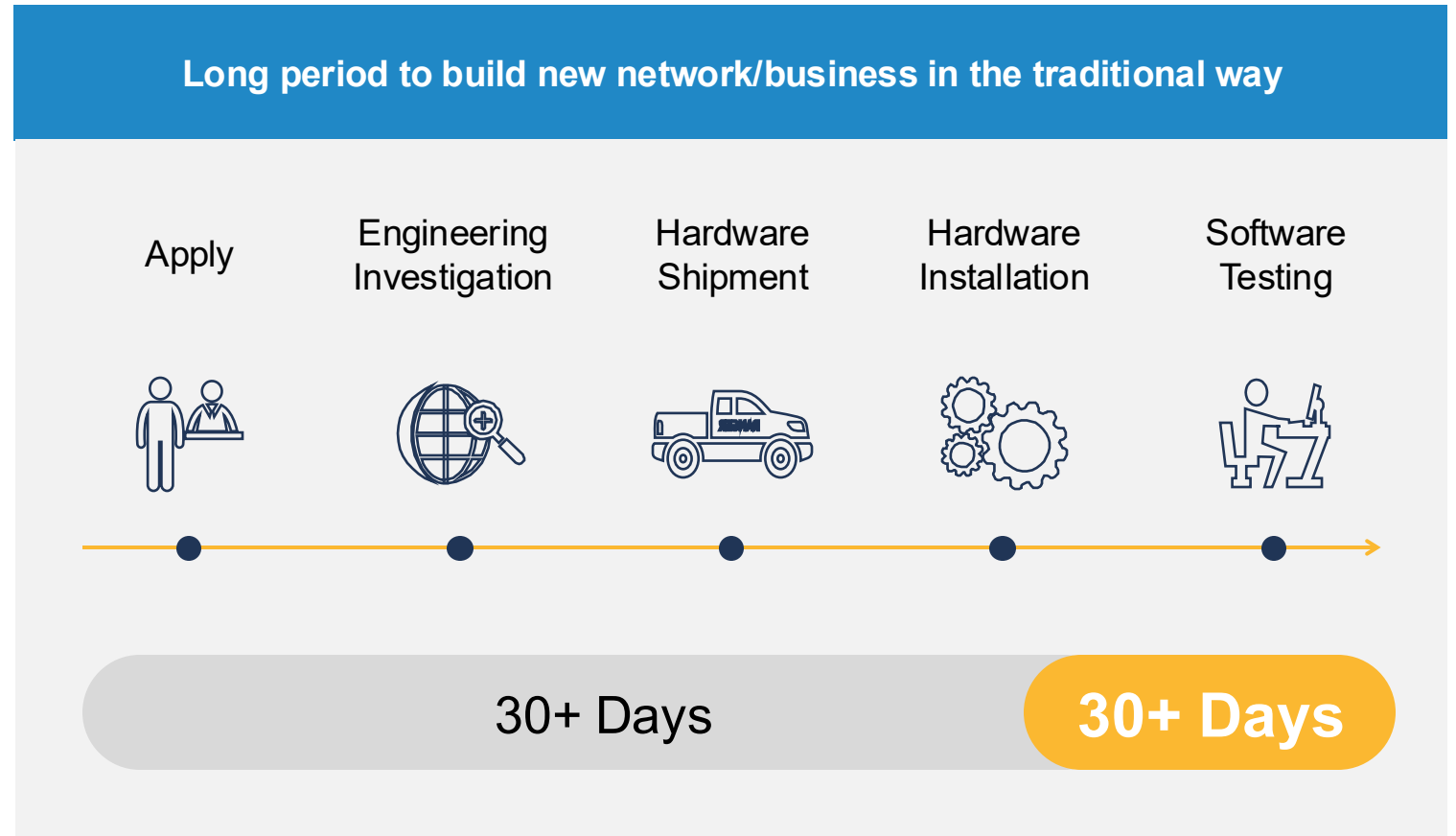
New Branch

Slow to build private network for VPN requirement.



New Business

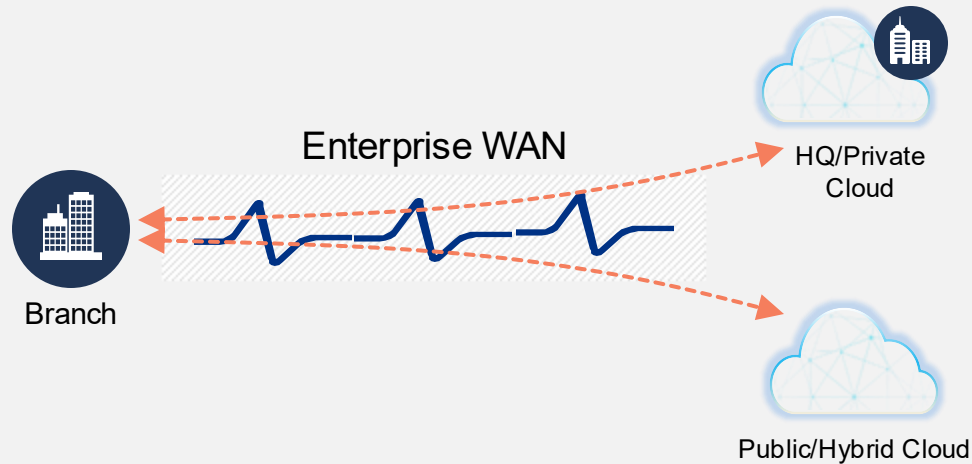
Multi-type services require fine-grained access control, higher security, and better user experience.



No Visibility into Business Traffic Makes Operation Difficult

Rich services with difficulty to monitor and schedule traffic

Large number of sites increases O&M cost and decreases efficiency



5000+

chain stores

100+

sites

- Manually adjusting bandwidth results are untimely and error-prone
- Difficulty in troubleshooting

- High local maintenance cost
- No flexible centralized management

Rapid Changes In Network Bring New Challenges



Cloud



Virtualization



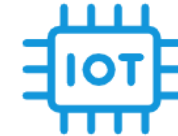
Containerization



BYOD



Remote Access



IoT



M2M

Rapid Changes In Network Bring New Challenges

Evolving Threat Landscape

Compliance Requirements

Data Protection

Integration Of New Technologies And Business Brings New Challenges

Traditional Perimeters

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

The disrupting Perimeter

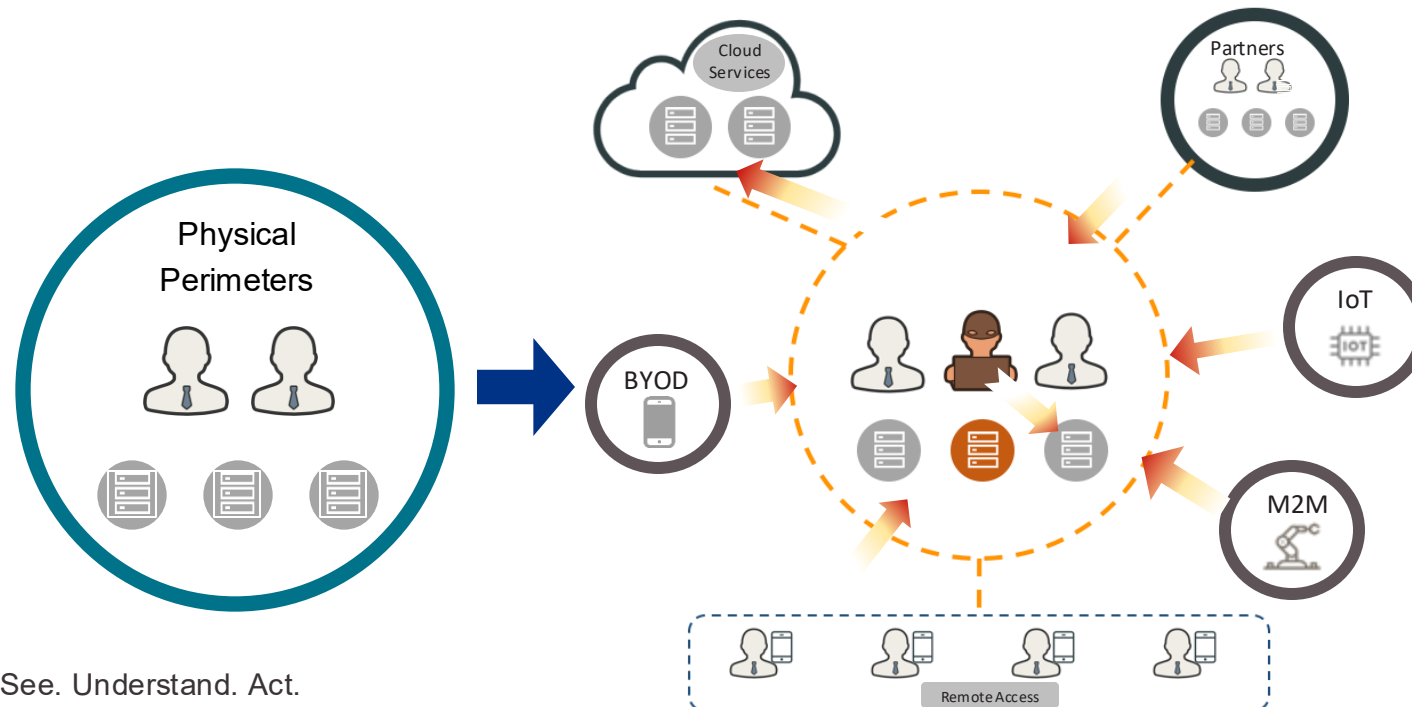
- Out-of-date static FW policies
- Resource-intensive endpoint monitoring
- No identity and context awareness

Challenges From Technology

- Cloud Computing
- Network Virtualization
- Known VPN vulnerability

Challenges From Business

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



The Evolving Network Security Challenges



The Applications are out of control!

Advanced Threat/Attacks Evolving Fast !

Security compromise to performance!

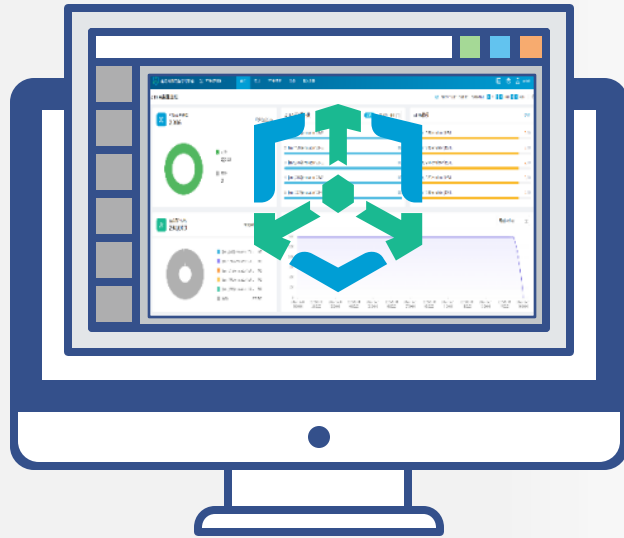
- | | | | |
|---|--|--|---|
| <ul style="list-style-type: none"> • Engineering Investigation | <ul style="list-style-type: none"> • 0-Day/APT | <ul style="list-style-type: none"> • Unknown Threats | <ul style="list-style-type: none"> • High Latency |
| <ul style="list-style-type: none"> • Excessive Bandwidth Consumption | <ul style="list-style-type: none"> • Threat Evasion | <ul style="list-style-type: none"> • SPAM/PHISHING/C&C... | <ul style="list-style-type: none"> • Network Down |
| <ul style="list-style-type: none"> • Unencrypted Traffic | <ul style="list-style-type: none"> • Locky Ransomware | <ul style="list-style-type: none"> • DoS/DDoS | <ul style="list-style-type: none"> • Excessive Security Investment |
| <ul style="list-style-type: none"> • Data Breach | <ul style="list-style-type: none"> • Shutting Down Business | <ul style="list-style-type: none"> • | |

Hillstone HSM Value Proposition

Hillstone HSM Highlights



Security Operation Management



Hillstone Security Management Device Manager



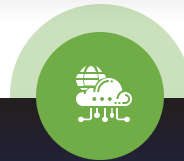
Device Monitoring

- NGFW Resource usage monitoring
- NGFW Remote access



Policy Management

- Global/Individual device policy
- SNAT policy



Configuration

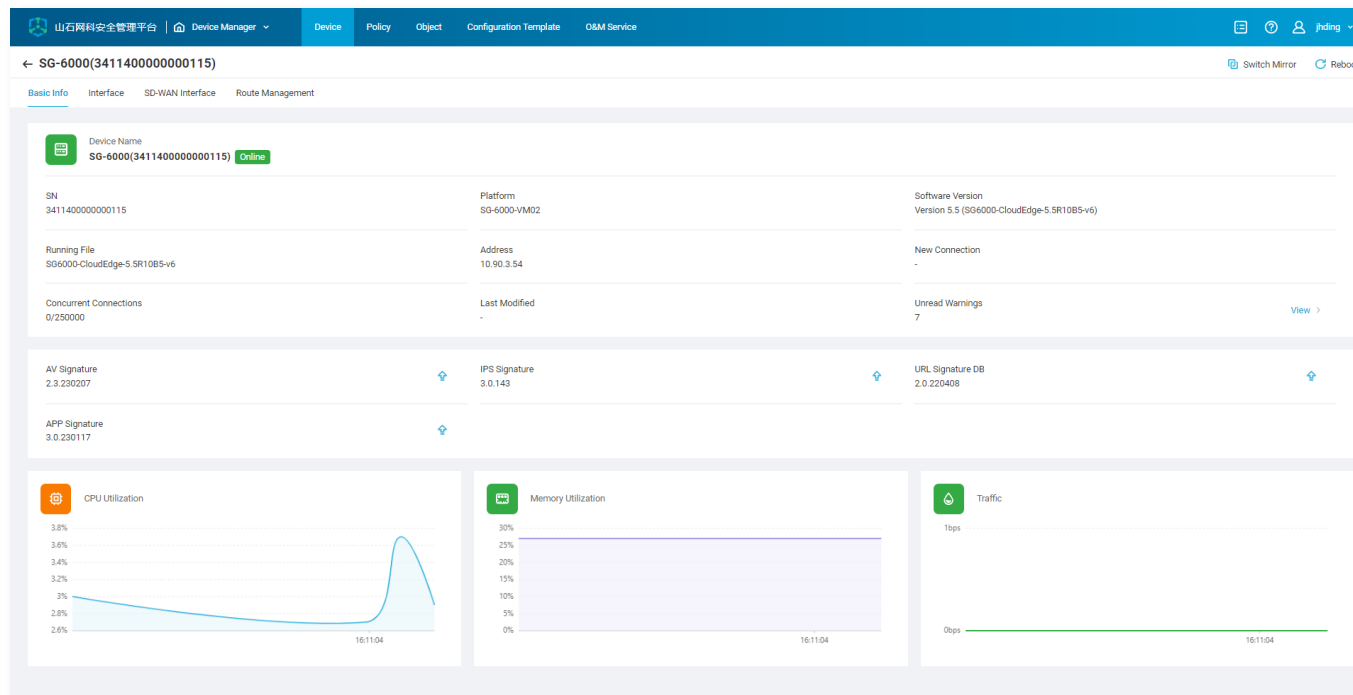
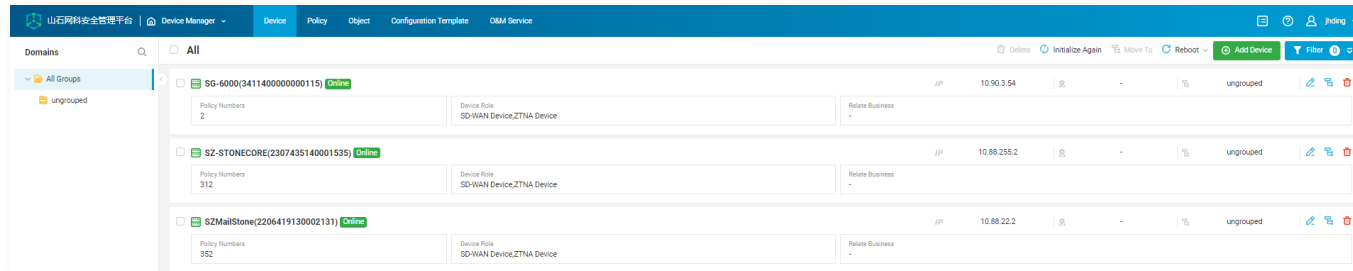
- Routing configuration
- Interface configuration



O&M

- Software upgrade
- Signature database upgrade

Centralized Configuration and Management



Dimensions



Device Management

- Grouped or Ungrouped
- Device configuration
- Device resource usage monitoring
- Remote access for FW WebUI/CLI



Configuration Template Management

- Network template configuration
- System template configuration



O&M Management

- License Management
- Signature database updates
- Firmware upgrade
- Configuration file management

Global Policy/Individual Device Policy Management

Global Policy

- Global configuration can be pushed to all managed devices

The screenshot shows the 'Global Security Policy' management page. The top navigation bar includes 'HSM', 'Device Manager', 'Device', 'Policy', 'Object', 'Configuration Template', and 'O&M Service'. Below the navigation, there are tabs for 'Global Policy' and 'Device Policy'. The main content area features a 'Global Security Policy' header with 'Batch Delete', 'New', and 'Filter' buttons. A table below lists policy rules with columns for Name, Policy Rules, Managed Device, Status, Description, and Operation.

Individual Device Policy

- Private configuration for individual device
- Support IPv4 SNAT rules
- SNAT policy configuration including *add, edit, delete and query* for individual device

The screenshot shows the 'All Groups' management page. The top navigation bar is identical to the previous screenshot. Below the navigation, there are tabs for 'Global Policy' and 'Device Policy'. The main content area features a search bar and a table titled 'All Groups' with columns for Name, Policy Numbers, SNAT Numbers, and Operation. The table lists several groups with their respective policy and SNAT counts.

Name	Policy Numbers	SNAT Numbers	Operation
SG-6000(3411400000000115)	2	0	[Icon]
SZ-STONECORE(2307435140001535)	312	0	[Icon]
SZMailStone(2206419130002131)	352	15	[Icon]
(M) SZ-STONE(5823619215007756)	364	10	[Icon]
BJSTONE(2206450172006742)	232	2	[Icon]

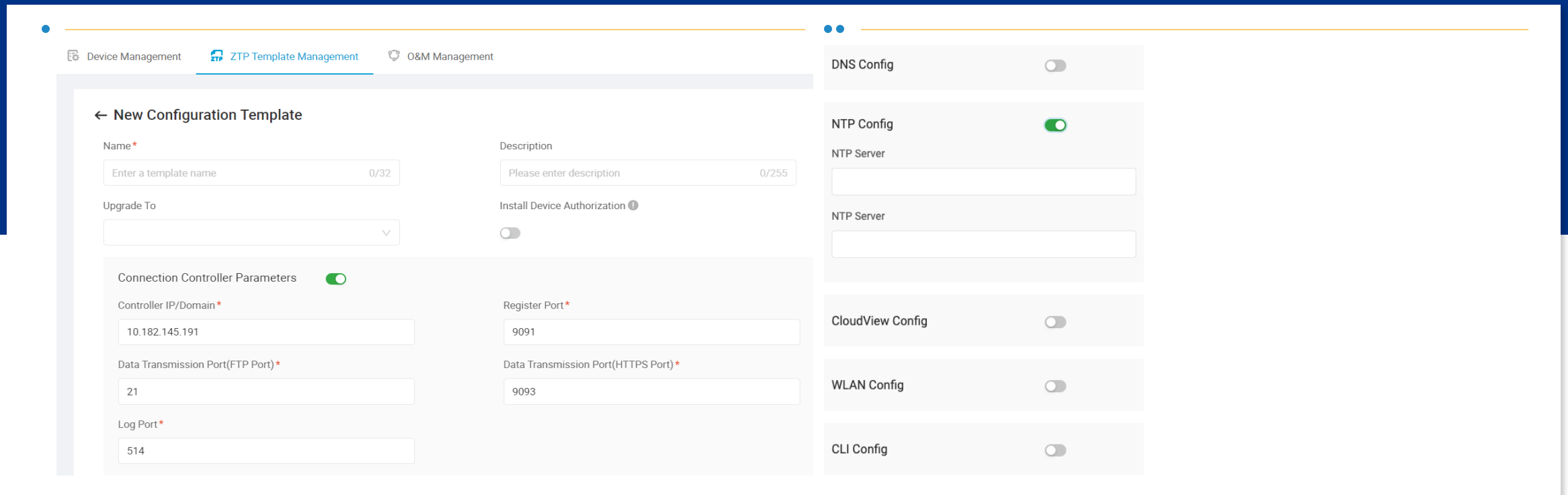
Zero Touch Provisioning

FEATURES

- USB plug-and-play in device provisioning
- Support device license installation
- Auto firmware upgrade during deployment
- Auto network joining/ establishment
- Preconfigured and custom templates

BENEFITS

- Reduce time and efforts for deployment
- Eliminates the human errors that come with repetitious typing at the CLI.
- Simplified firmware upgrades
- Reduce TCO



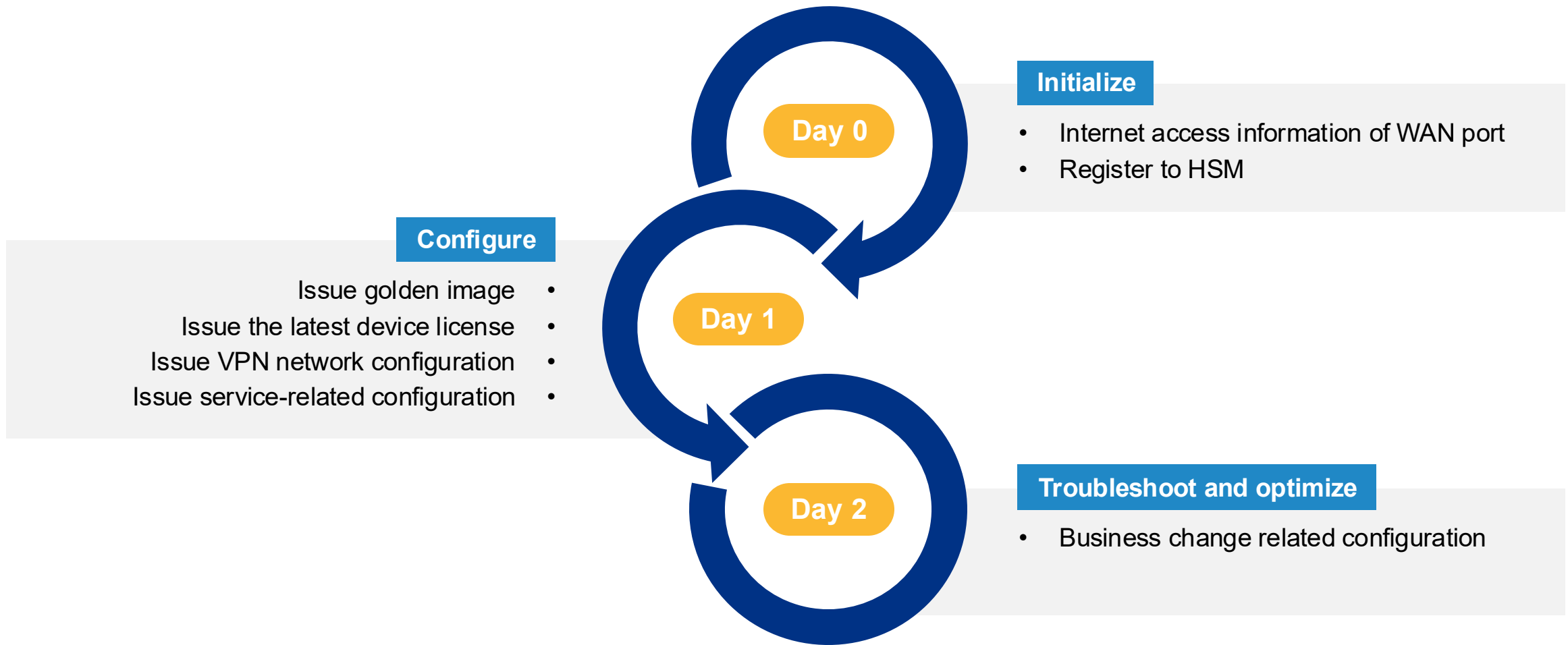
The screenshot displays the ZTP configuration interface. The top navigation bar includes 'Device Management', 'ZTP Template Management', and 'O&M Management'. The main content area is titled 'New Configuration Template' and contains the following fields and options:

- Name***: Text input field with placeholder 'Enter a template name' and character count '0/32'.
- Description**: Text input field with placeholder 'Please enter description' and character count '0/255'.
- Upgrade To**: Dropdown menu.
- Install Device Authorization**: Toggle switch (currently off).
- Connection Controller Parameters**: Toggle switch (currently on).
- Controller IP/Domain***: Text input field with value '10.182.145.191'.
- Register Port***: Text input field with value '9091'.
- Data Transmission Port(FTP Port)***: Text input field with value '21'.
- Data Transmission Port(HTTPS Port)***: Text input field with value '9093'.
- Log Port***: Text input field with value '514'.

On the right side, there is a vertical list of configuration options, each with a toggle switch:

- DNS Config**: Toggle switch (currently off).
- NTP Config**: Toggle switch (currently on).
- NTP Server**: Text input field (empty).
- NTP Server**: Text input field (empty).
- CloudView Config**: Toggle switch (currently off).
- WLAN Config**: Toggle switch (currently off).
- CLI Config**: Toggle switch (currently off).

DAY 0~2 Full Configuration Process

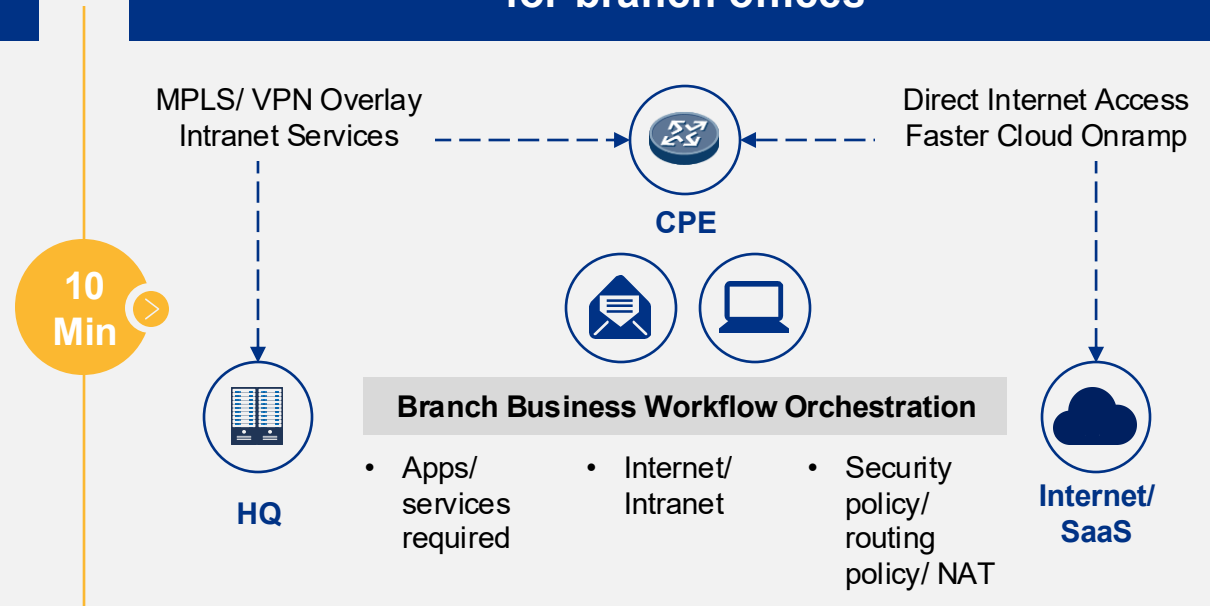


Business Goes Online Faster

Challenges in opening traditional branch services

- Technical Barrier - Need on-site deployment by professional IT engineers
- Low Efficiency - Distributed devices, complicated configurations, long operation time
- Risk in Mis-operation – Easy to make mistakes when manually configuring

Fast business workflow orchestration for branch offices



No on-site configuration needed

Auto network service orchestration
Quick business enablement

Optimized network;
Better user experience;

Fast and Simplified VPN Overlay Automation

Complex Multi-branch VPN Network Configuration

Difficult to Configure

- Need to configure lots of parameters
- Require related skills

Low Efficiency

- Have to configure each individual branch VPN network

Auto-configuration of VPN Network Branch Networks Can Be Quickly Deployed in Batch

Template based VPN Overlay Configuration

- Support hub-spoke (star topology): Single hub and dual hub
- Support spoke-spoke (mesh topology): full mesh and partial mesh
- VPN resource auto collection

Multiple Types of WAN Link

- Interface types: Ethernet interface/ Ethernet sub-interface/ Aggregated port
- Line types: Internet/ Dedicated line

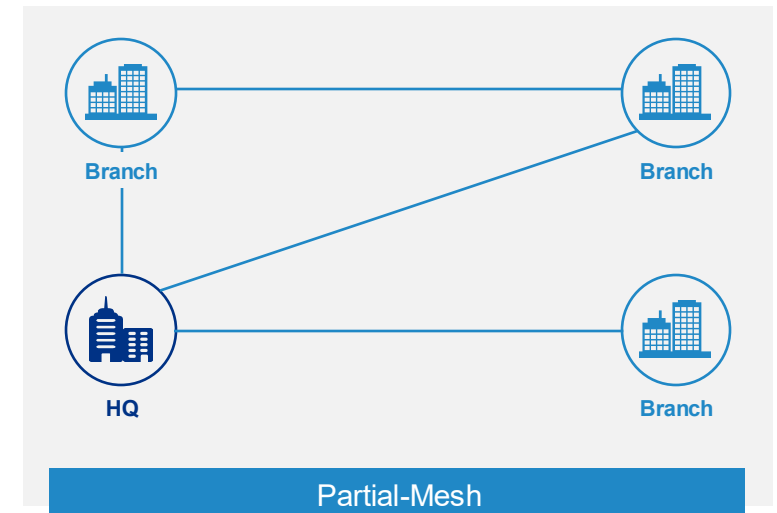
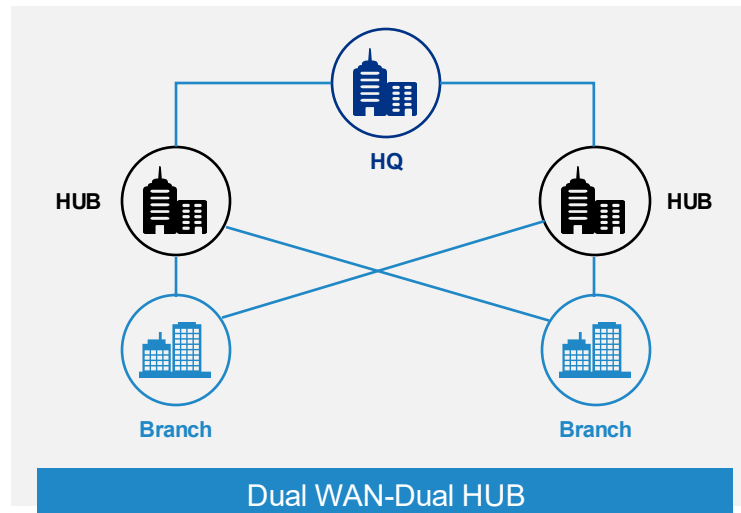
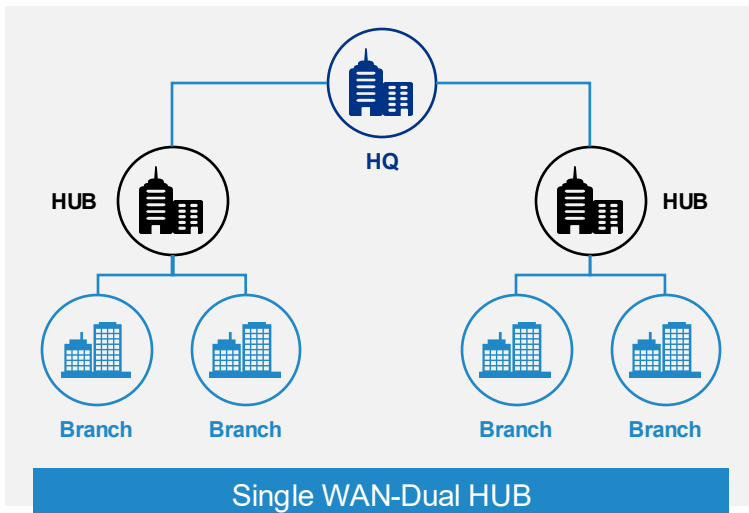
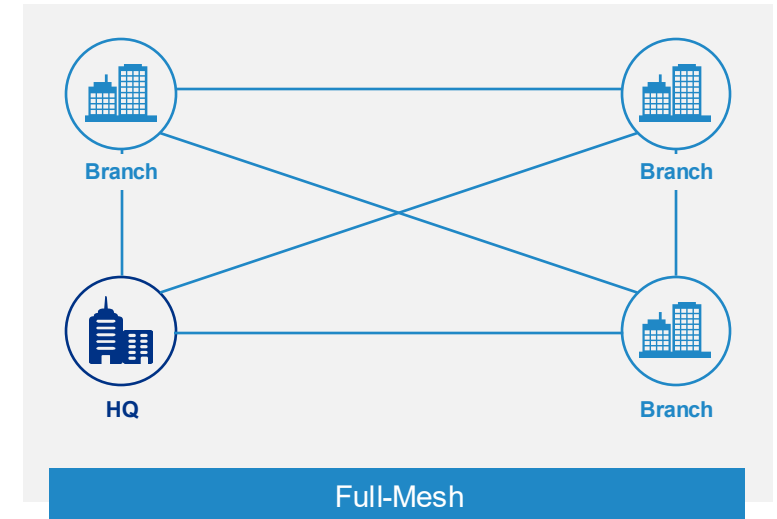
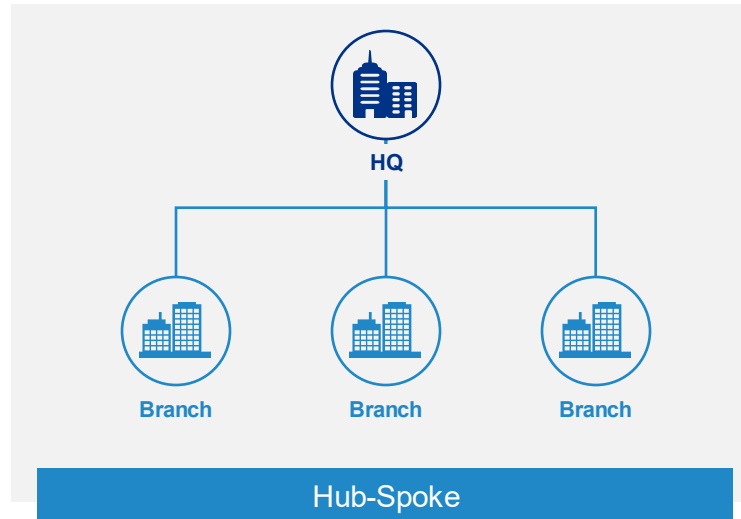
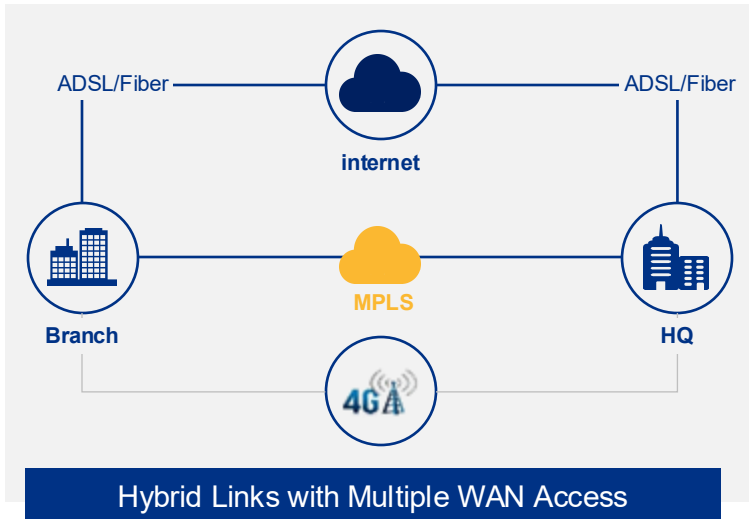
10
Min

Simplified overlay deployment and Management

Highly improved O&M efficiency

Great for massive deployment

Multiple WAN Links and VPN Topologies

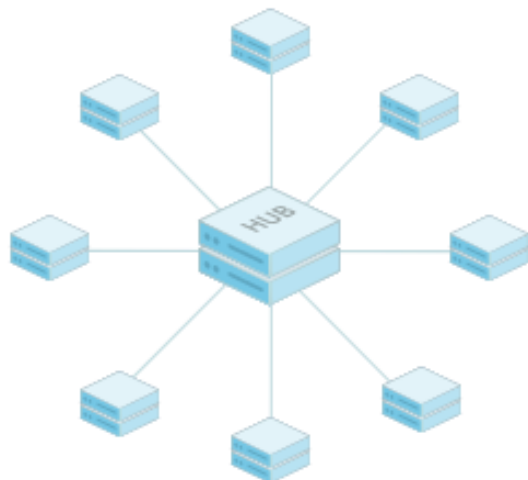


VPN Overlay - Star Network (Hub-Spoke)

Topology

Star Network

- Devices are connected through the hub device(s)



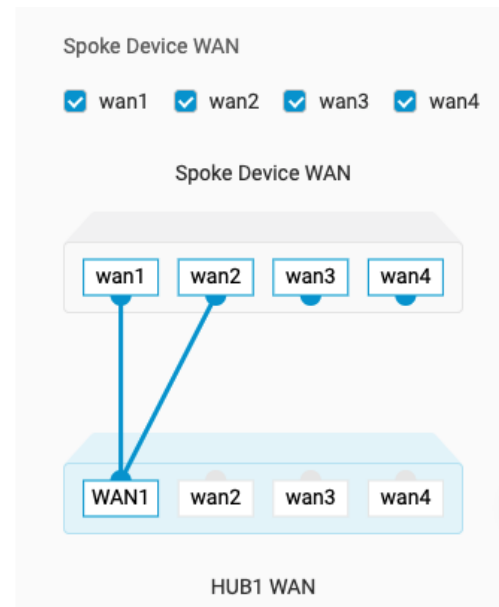
Hub-Spoke

Custom WAN Interconnections

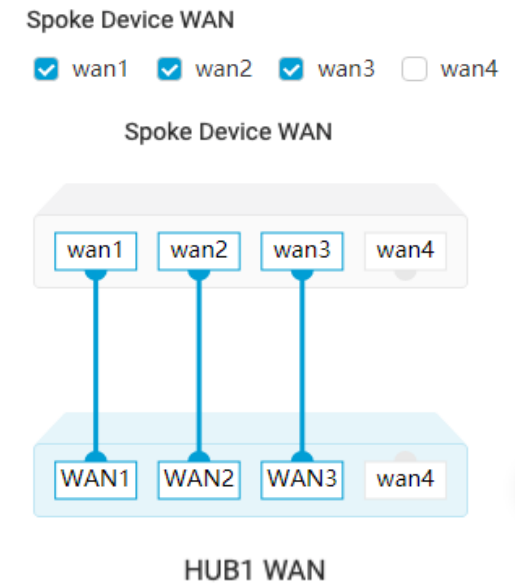
Model:

- Define how the spoke device(s) and hub device(s) establish link connections.
- Up to 20 models in one star network.

Model 1

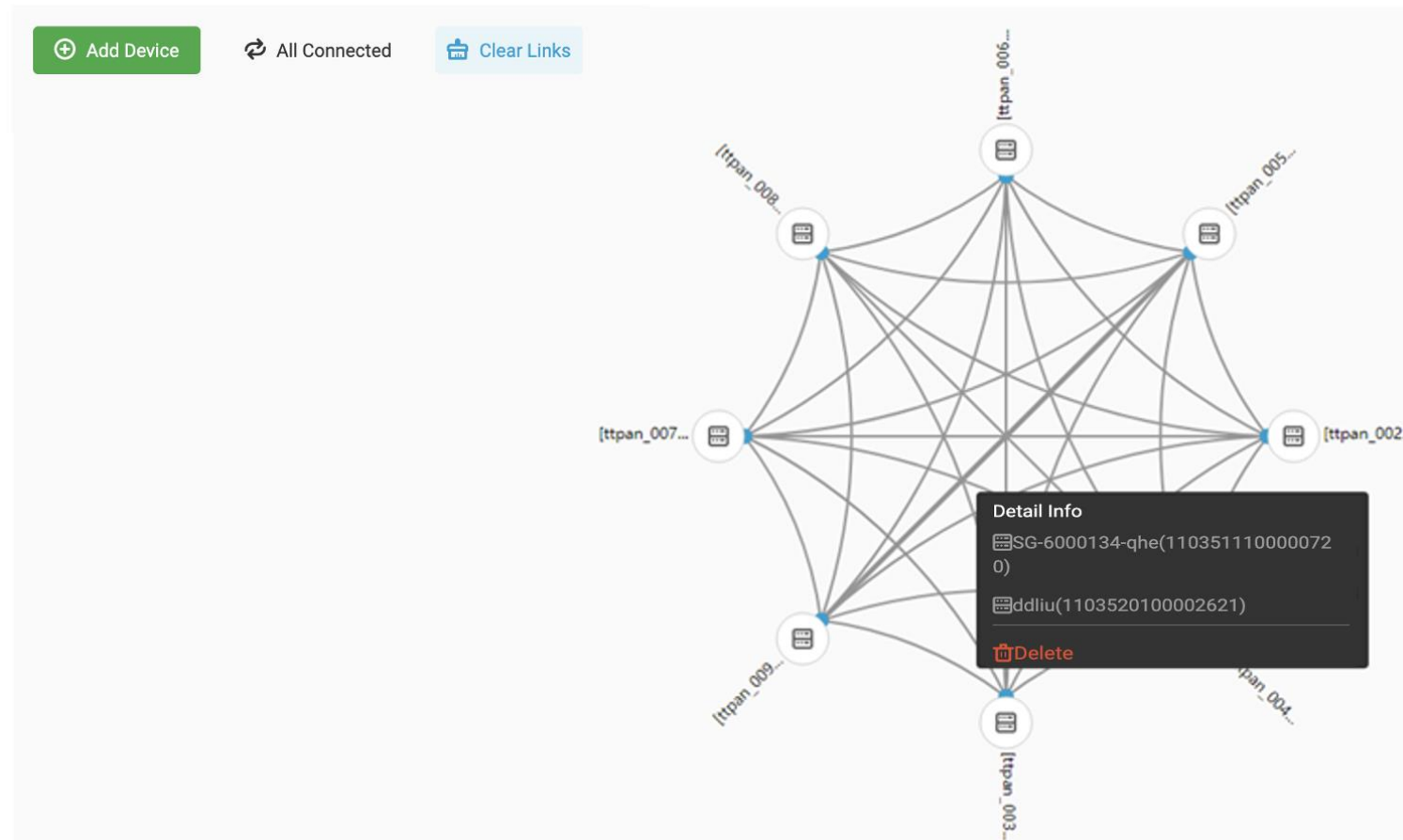


Model 2



VPN Overlay - Mesh Network (Spoke-Spoke)

Grid View Topology View



Graphic Topology View

- Support list view and topology view of the devices in the network
- Support editing in both view

Visual Editing

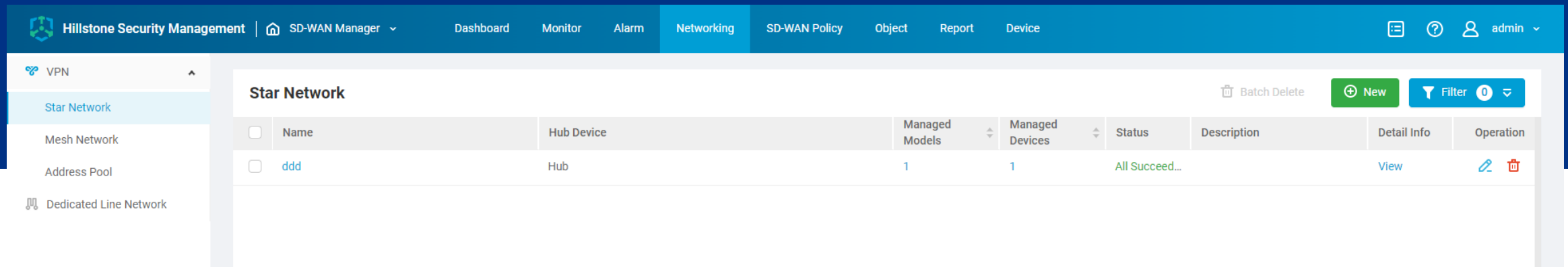
- Support edit in grid view and topology view
- Add new device to establish new connections
- Disconnect specific link between two devices
- Reconnect all devices to establish a full mesh network

Size of Mesh Network

- Up to 20 devices

VPN Resource Collections

VPN resources used in the configuration will be collected by HSM after a spoken device is unassociated with a network.

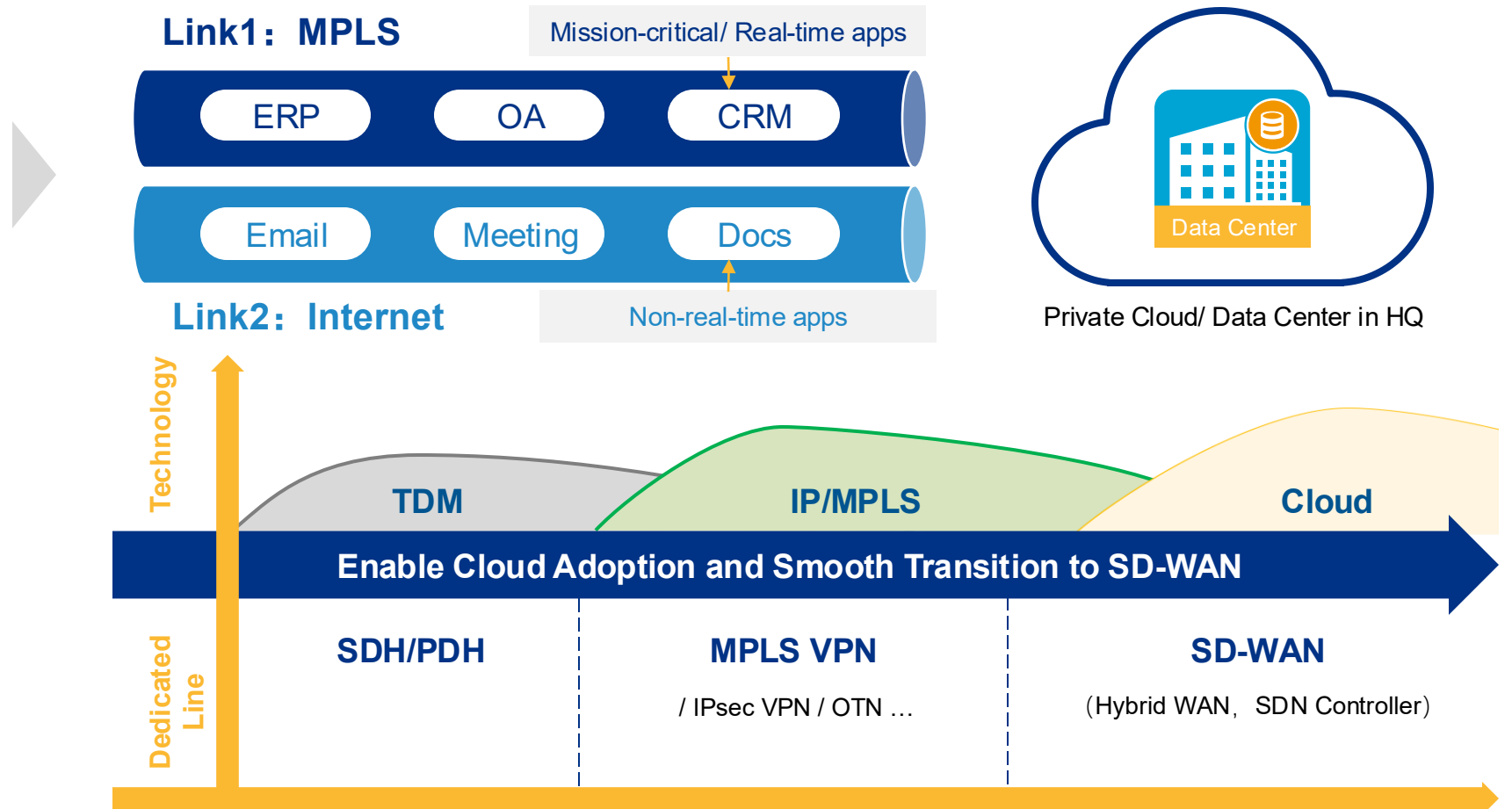


The screenshot displays the Hillstone Security Management interface. The top navigation bar includes 'Hillstone Security Management', 'SD-WAN Manager', and various menu items like 'Dashboard', 'Monitor', 'Alarm', 'Networking', 'SD-WAN Policy', 'Object', 'Report', and 'Device'. The left sidebar shows a tree view with 'VPN' expanded, containing 'Star Network', 'Mesh Network', 'Address Pool', and 'Dedicated Line Network'. The main content area is titled 'Star Network' and features a table with the following data:

<input type="checkbox"/>	Name	Hub Device	Managed Models	Managed Devices	Status	Description	Detail Info	Operation
<input type="checkbox"/>	ddd	Hub	1	1	All Succeed...		View	Edit Delete

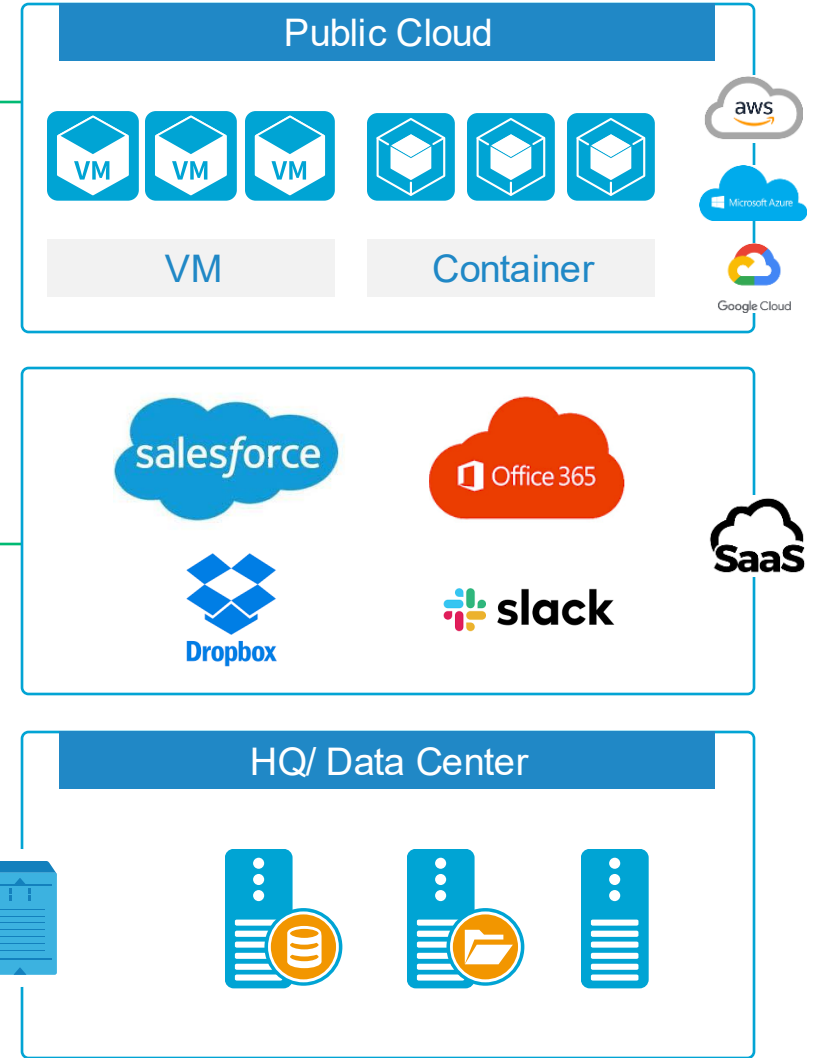
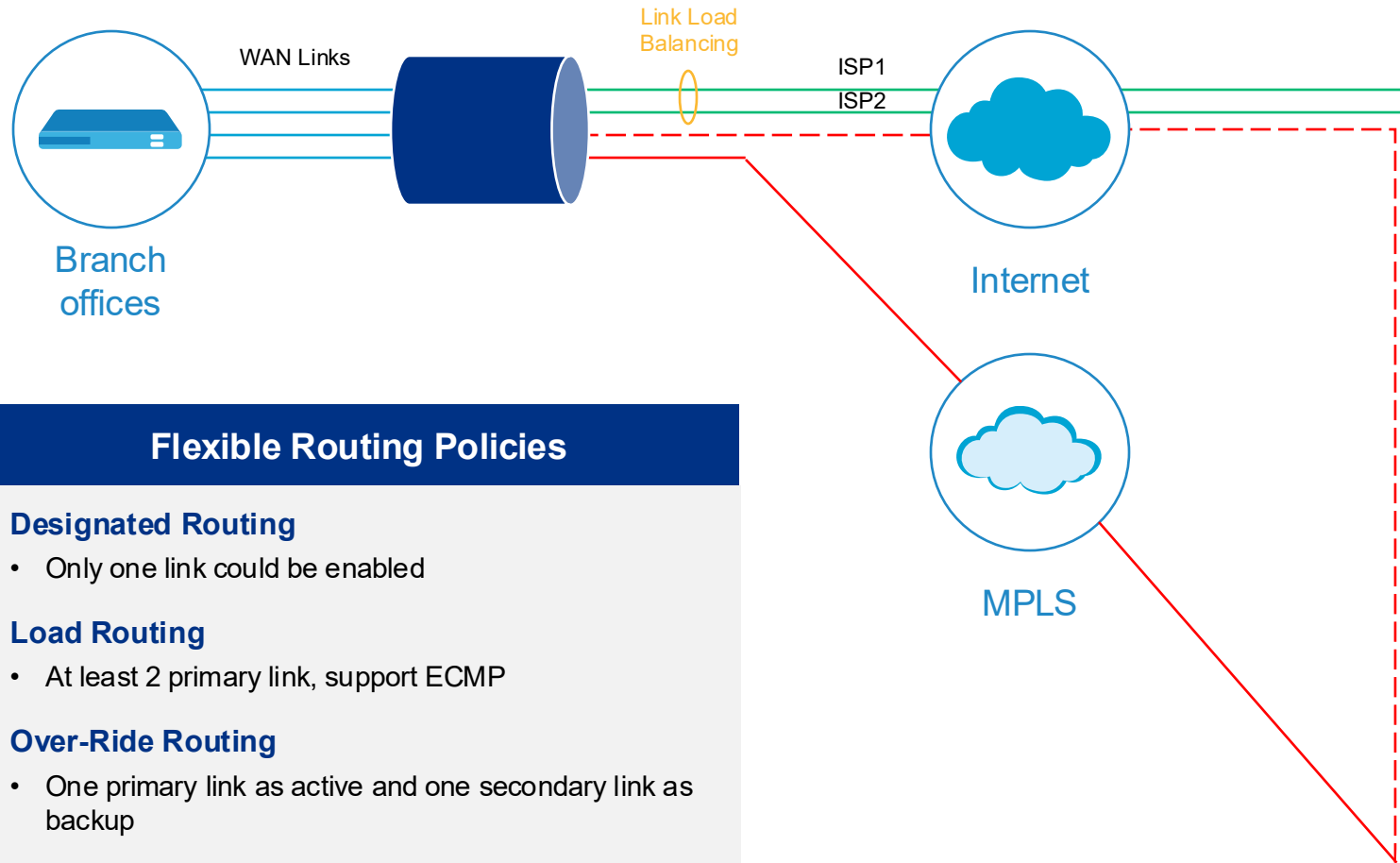
Application-aware Traffic Steering

- 600+ Mobile Apps
- 300+ SaaS Apps
- ...



- App recognition based on
- Protocols
- Behaviors

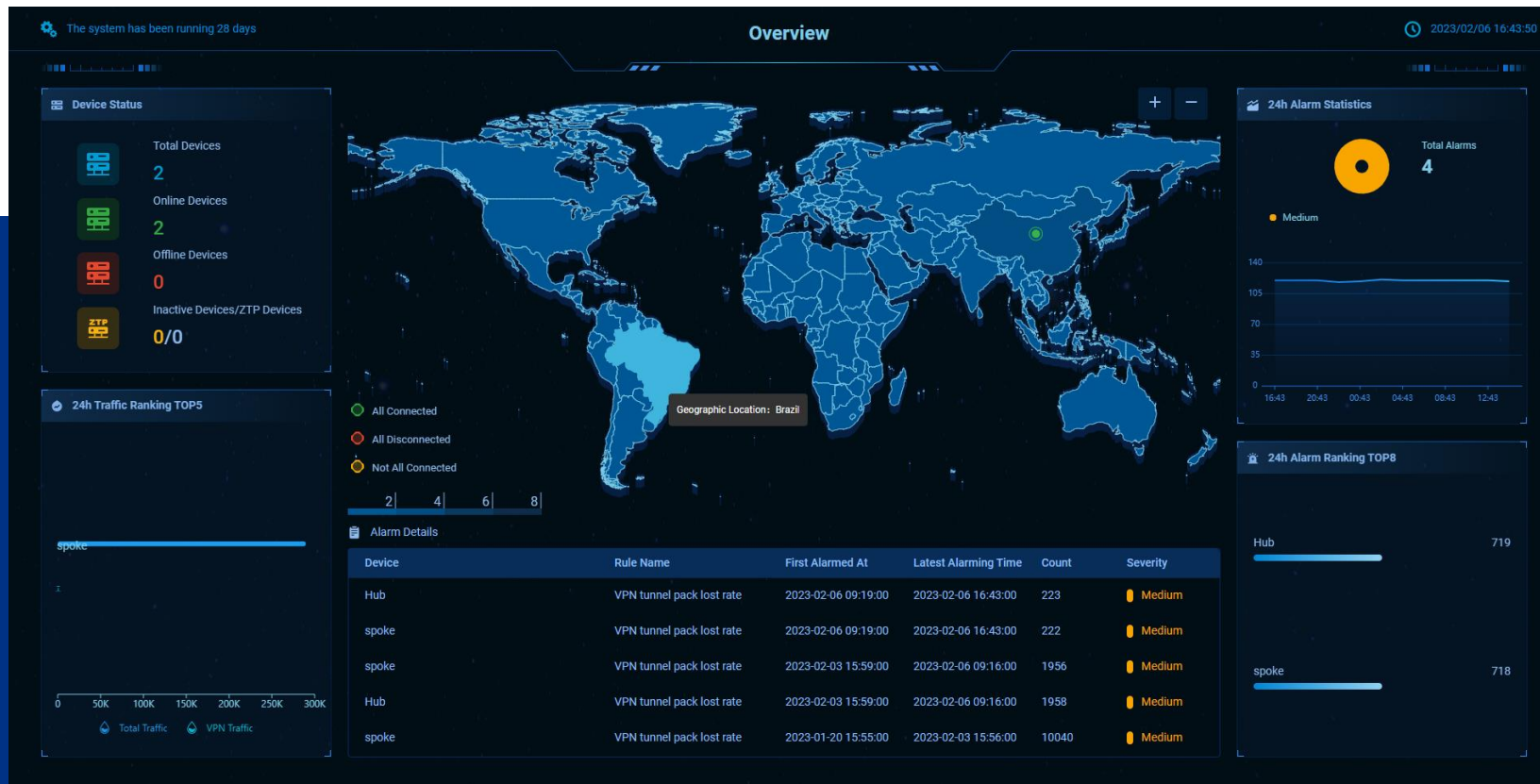
Smart Routing



Flexible Routing Policies

- Designated Routing**
 - Only one link could be enabled
- Load Routing**
 - At least 2 primary link, support ECMP
- Over-Ride Routing**
 - One primary link as active and one secondary link as backup
- Custom Routing**
 - At least 1 primary link, and up to 16 links for either primary or secondary.

SD-WAN Centralized Management - Dashboard Full Screen Mode



Designed for Operation

- No login timeout
- Full information as non-full screen mode
- Connections/ devices status in map view
- Real time alarm with details

SD-WAN Device Management

Dimensions



Device Management

- Grouped or Ungrouped
- Device configuration
- Choose device from device manager
- Remote access for FW WebU/CLII



ZTP Template Management

- Template configuration
- Pre-configured templates for different platform and versions

The screenshot shows the 'Device Management' page in the SD-WAN Manager. The top navigation bar includes 'HSM', 'SD-WAN Manager', and various menu items like 'Dashboard', 'Monitor', 'Alarm', 'Networking', 'SD-WAN Policy', 'Object', 'Report', and 'Device'. The main content area is titled 'ZTP Template Management' and displays a list of devices. Each device entry includes a checkbox, a device ID (e.g., SG-6000, SZ-STONECORE, SZMailStone, SZ-STONE, BJSTONE), a status indicator (Online, Master, Slave), an IP address, and a 'Business' field. Below each device ID are fields for 'ZTP Status', 'ZTP Configuration Template', and 'VPN Net'. Action buttons like 'Initialize Again', 'Reboot', and 'Add Device' are visible at the top right of the device list.

The screenshot shows the 'ZTP Template Management' page. It features a navigation bar with 'HSM', 'SD-WAN Manager', and menu items. The main content area has tabs for 'Configuration Template' and 'Platform Preconfiguration'. Below the tabs is a table with columns for 'Name', 'Description', 'Created By', 'Created At', and 'Operation'. A single row is visible with the name 'dddddd', description 'yfding', and creation time '2022/12/05 18:00:33'. Action buttons like 'Batch Delete' and 'New' are located above the table.

Deep SD-WAN Network Visibility

Link/ User/ Application List View

WAN Link Monitor | Tunnel Link Monitor | User Monitor | Application Monitor

WAN Link Monitor List

Device Name	WAN Name	Line Type	Access Method	Operator	Status	Upstream Rate(bps)	Downstream Rate(bps)	Applications	Delay(ms)	Jitter(ms)	LossRate(%)
	WAN1	Dedicated Line	Static IP	Other	Active	0	0	0	-	-	-
vfw-132(0010055646750792)	WAN2	Internet	Static IP	China Unicom	Active	0	0	0	-	-	-
	WAN3	Internet	Static IP	China Telecom	Inactive	0	0	0	-	-	-

WAN Link Monitor | Tunnel Link Monitor | User Monitor | Application Monitor

Tunnel Link Monitor List

Tunnel Interface(tunnelName)	srcDevice/WAN	dstDevice/WAN	Status	Upstream Rate(bps)	Downstream Rate(bps)	Delay(ms)	Jitter(ms)	LossRate(%)	Applications
tunnel1(ike_0010087211378758...	vfw-142/WAN1	vfw-131(0010087211378758)/WAN1	Active	0	0	0	0	0	0

WAN Link Monitor | Tunnel Link Monitor | User Monitor | Application Monitor

User Monitor Overview

Quantity Overview

Top10 IPs by Average Rate

IP	Unit:bit/s
10.88.7.10	403

Users

User	Device Name	Average Rate(bps)	Upstream Rate(bps)	Downstream Rate(bps)	New Sessions	Forwarding Rate(pps)
10.88.7.10	vfw-131(00100872113...	403	0	403	18	0

WAN Link Monitor | Tunnel Link Monitor | User Monitor | Application Monitor

Top10 Apps by Average Rate

App	Unit:bit/s
DNS	400

Application in Device

Application Name	Device Name	Average Rate(bps)	New Sessions
DNS	vfw-131(0010087211378758)	381	18

- Support monitoring for physical and tunnel interface, as well as user and application status
- Rich parameters for analysis and troubleshooting

Dedicated Line Status Map View



- Real time update
- Map view
- Full screen support
- Good for operation and monitoring

Custom SD-WAN Alarm Rules

Custom Alarm Rules for HW Resources/ System Status/ VPN

Rule Name	Status	Trigger	Device	Severity	Notification	Type	Operation
CPU Utilization	On	CPU Utilization for 1 min(s) is higher than 60%	All Devices	Critical	Disable	Predefined	Edit Delete
Memory Utilization	On	Memory Utilization for 1 min(s) is higher than...	All Devices	Critical	Disable	Predefined	Edit Delete
HDD Utilization	On	HDD Utilization for 1 min(s) is higher than 10%	All Devices	Critical	Disable	Predefined	Edit Delete

Rule Name	Status	Trigger	Device	Severity	Notification	Type	Operation
VPN Tunnel Traffic ...	On	VPN Tunnel Traffic Beyond Threshold for 1 ...	All Devices	Critical	Disable	Predefined	Edit Delete
VPN Tunnel Delay	On	VPN Tunnel Delay for 1 min(s) is higher than ...	All Devices	Medium	Disable	Predefined	Edit Delete
VPN tunnel pack lo...	On	VPN tunnel pack lost rate for 1 min(s) is high...	All Devices	Medium	Disable	Predefined	Edit Delete
VPN Tunnel Interrupt	On	VPN Tunnel Interrupt exceeds 30 s	All Devices	Critical	Disable	Predefined	Edit Delete

Rule Name	Status	Trigger	Device	Severity	Notification	Type	Operation
Signature Database...	On	Signature Database Update Successfully	All Devices	Critical	Disable	Predefined	Edit Delete
Port Traffic Beyond ...	On	Port Traffic Beyond Threshold for 1 min(s) l...	All Devices	Critical	Disable	Predefined	Edit Delete
Device Name Modi...	On	Device Name Modification	All Devices	Critical	Disable	Predefined	Edit Delete
Add Interface	On	Add Interface	Specified devices	Critical	Disable	Predefined	Edit Delete
Modify Interface	On	Modify Interface	Specified devices	Critical	Disable	Predefined	Edit Delete
Delete Interface	On	Delete Interface	Specified devices	Critical	Disable	Predefined	Edit Delete
Add Zone	On	Add Zone	Specified devices	Critical	Disable	Predefined	Edit Delete
Delete Zone	On	Delete Zone	Specified devices	Critical	Disable	Predefined	Edit Delete
Link Down	On	Link Down	All Devices	Critical	Disable	Predefined	Edit Delete

Predefined and custom alarm rules

For HW resources:

CPU/ Memory/ HDD utilization

For VPN:

Delay, packet loss, etc.

For system status:

Add/ delete/ modify device/ interface/ zone, link down, signature database upgrade status, etc.

SD-WAN Alarm Dashboard



Navigation: HSM | SD-WAN Manager | Dashboard | Monitor | Alarm | Networking | SD-WAN Policy | Object | Report | Device

Sub-navigation: Alarm Board | Alarm Rule

Alarm Overview in the Last 24 hours

- Unread: 8
- Critical: 8
- High: 0
- Medium: 0
- Low: 0
- Notification: 0

Alarm Board

Mark All as Read | Filter 0

Device	Severity	Alarm Rule	Details	Latest Alarming Time	First Alarmed At	Count	Operation
SZMailStone(2206419130002...)	Critical	VPN Tunnel Interr...	Tunnel MailTOBJSTONEAB has been interrupted	2023-02-13 04:14:31	2023-02-13 04:14:31	1	[Icon] [Icon]
BJSTONE(2206450172006742)	Critical	VPN Tunnel Interr...	Tunnel CNC_SZMAIL(root) has been interrupted	2023-02-13 04:14:31	2023-02-13 04:14:31	1	[Icon] [Icon]
SZ-STONE(5823619215007756)	Critical	Signature Databa...	av signature database upgraded successfully	2023-02-13 00:47:38	2023-02-13 00:47:38	1	[Icon] [Icon]
SG-6000(341140000000115)	Critical	Signature Databa...	av signature database upgraded successfully	2023-02-12 22:52:10	2023-02-12 22:52:10	1	[Icon] [Icon]
SZMailStone(2206419130002...)	Critical	VPN Tunnel Interr...	Tunnel SZMailTOUSA has been interrupted	2023-02-12 17:20:41	2023-01-13 16:33:57	53	[Icon] [Icon]
SZMailStone(2206419130002...)	Critical	Signature Databa...	av signature database upgraded successfully	2023-02-12 13:43:37	2023-02-12 13:43:37	1	[Icon] [Icon]

Total: 268

20 Row < 1 2 3 4 5 ... 14 >

Features

- Designed for operations
- Support statistics of alarms
- Support details info of each alarm: severity, trigger rule, alarm detail, last alarm time, first alarm time, count. Etc.
- Notification over Email or WeCom app

Benefits

- Quick access to an alarm
- Rich data for analysis and troubleshooting
- Efficient Operation and management

Comprehensive SD-WAN Report



Report Overview

- List all reports
- Provide statistics on operation status of device, traffic and tunnel in the network
- Support export report in PDF

The screenshot shows the 'Overview of Hub Device Hub' section. It includes device details for a 'Hub' device, a 'CPU/Memory Trend Chart' showing usage over time, and two tables for 'Average CPU Utilization of Spoke Devices' and 'Average Memory Usage of Spoke Devices'. A 'Suggestions' box at the bottom provides monitoring advice.

Overview of Hub Device Hub

Device Name: Hub
SN: [redacted] IP: [redacted]
Software Version: SG6000-CloudEdge-5.5R9F3

Average CPU Utilization: 2.3% (CPU Utilization Exceeds 90%)
Average Memory Usage: 24.0% (Memory Usage Exceeds 90%)

CPU/Memory Trend Chart

Time	CPU (%)	Memory (%)
2023/02/11 00:00:00	~2.3	~24.0
2023/02/11 05:57:30	~2.3	~24.0
2023/02/11 11:55:00	~2.3	~24.0
2023/02/11 17:52:30	~2.3	~24.0
2023/02/11 23:50:00	~2.3	~24.0

Average CPU Utilization of Spoke Devices (TOP 5)

Device	SN	IP	Average CPU Utilization
spoke	[redacted]	[redacted]	3.62%

Average Memory Usage of Spoke Devices (TOP 5)

Device	SN	IP	Average Memory Usage
spoke	[redacted]	[redacted]	37.03%

Suggestions
Keep monitoring your SD-WAN gateway and analyze the CPU and memory of network devices. If the CPU utilization or bandwidth usage is high for a long time, check whether the gateway runs normally at the earliest opportunity.

Report Task

- Generate reports periodically (daily/weekly/monthly)
- On-demand report

The screenshot shows the 'New/Task Configuration' dialog box. It includes fields for Name, Type (Daily, Weekly, Monthly), Report Template (SD-WAN Report), VPN Network, and SD-WAN Device (All). A 'Description' field is also present. 'Save' and 'Cancel' buttons are at the bottom.

New/Task Configuration

Name: [redacted] (0/255)

Type: Daily Weekly Monthly

Daily: 04:00:00

Report Template: SD-WAN Report

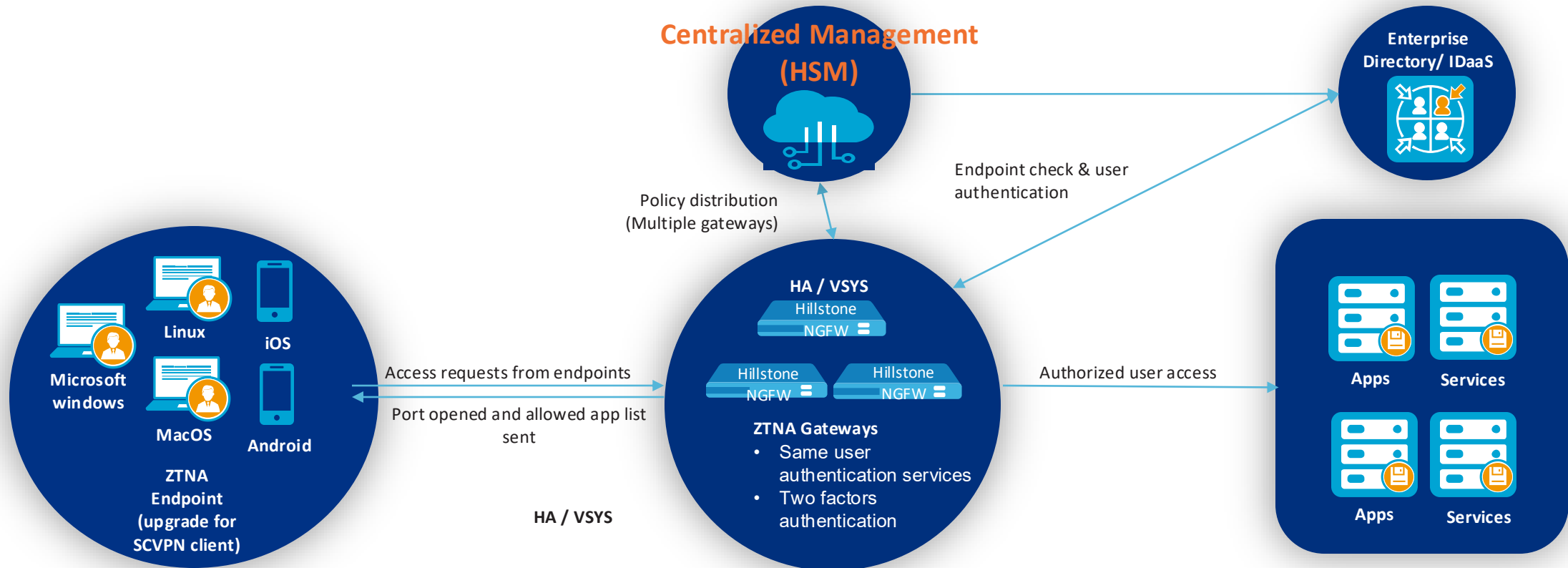
VPN Network: [redacted]

SD-WAN Device: All (Specify: 0 >)

Description: [redacted] (0/255)

Buttons: Save, Cancel

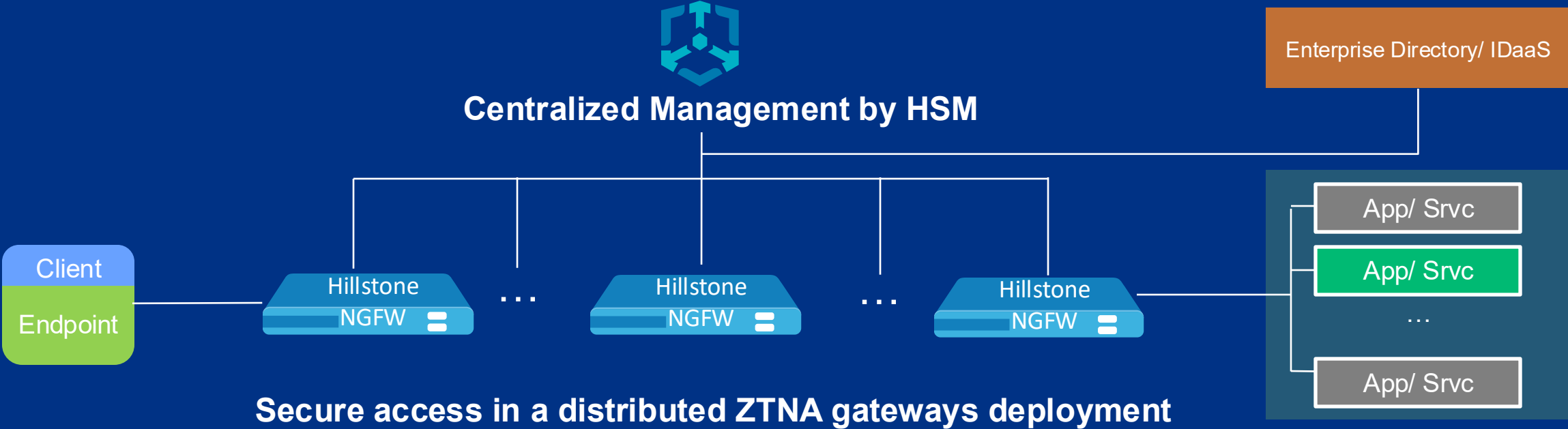
Hillstone ZTNA Solution Overview



Highlights

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

Centralized ZTNA Management



Integrated Device Management

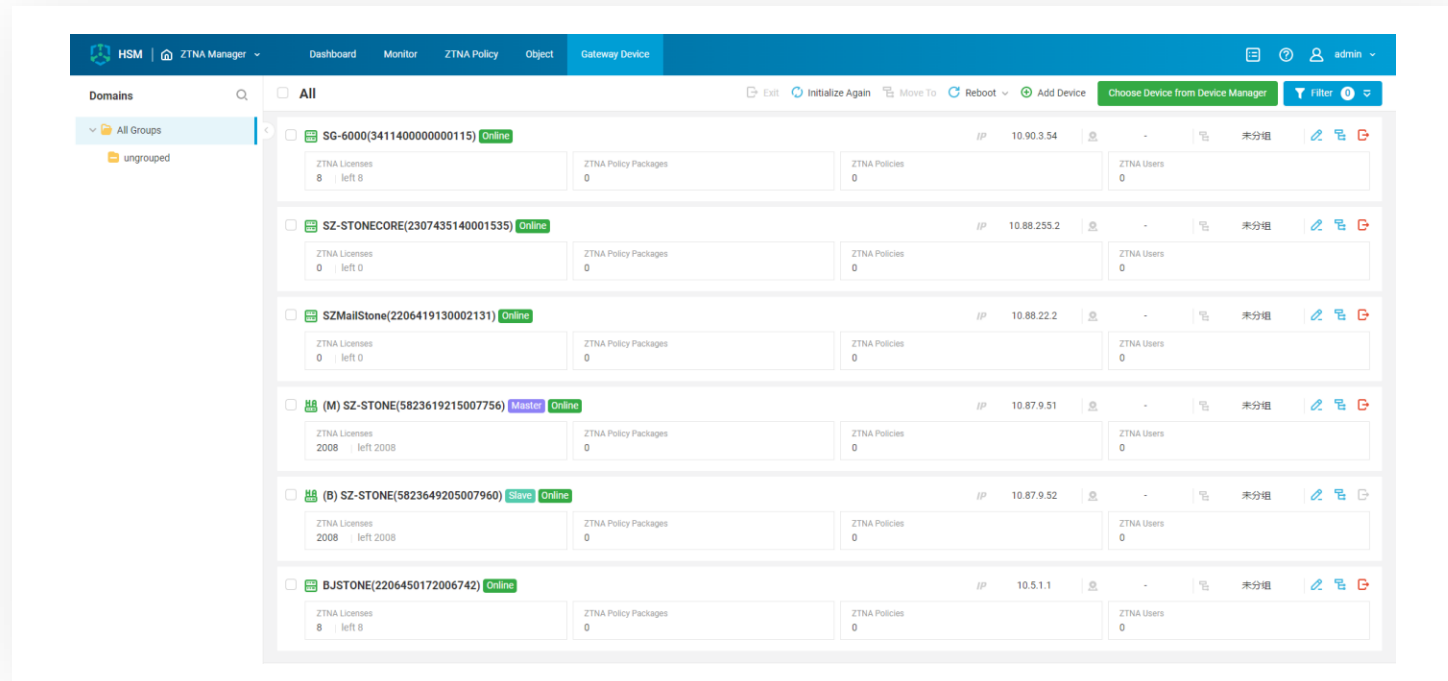
Centralized ZTNA Policy Management

Comprehensive Security Monitoring

Centralized ZTNA Gateway & Policy Management

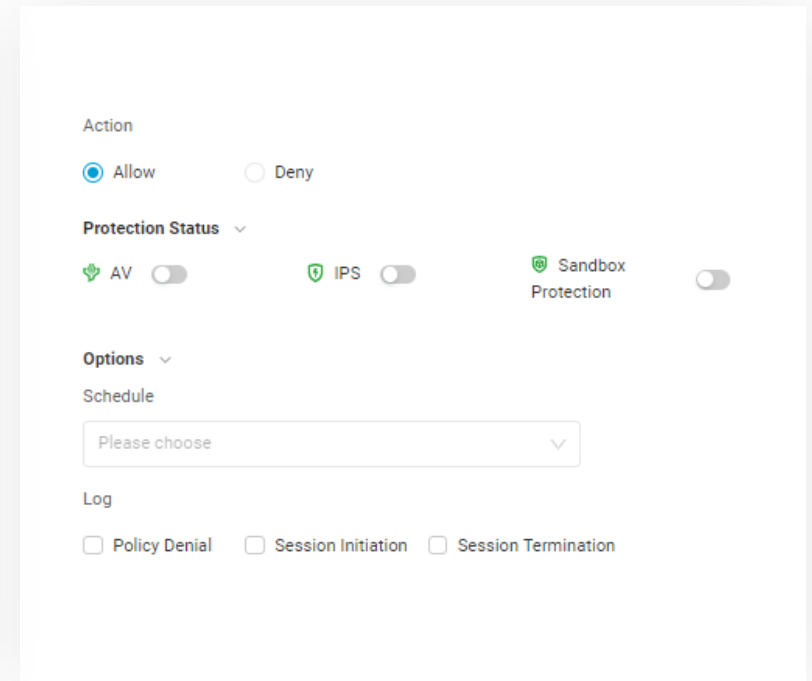
ZTNA Gateway

- Support automatic discovery of ZTNA gateways
- Support choosing device from device manager
- Statistics of ZTNA licenses, ZTNA policies, ZTNA authorized access users, device overview

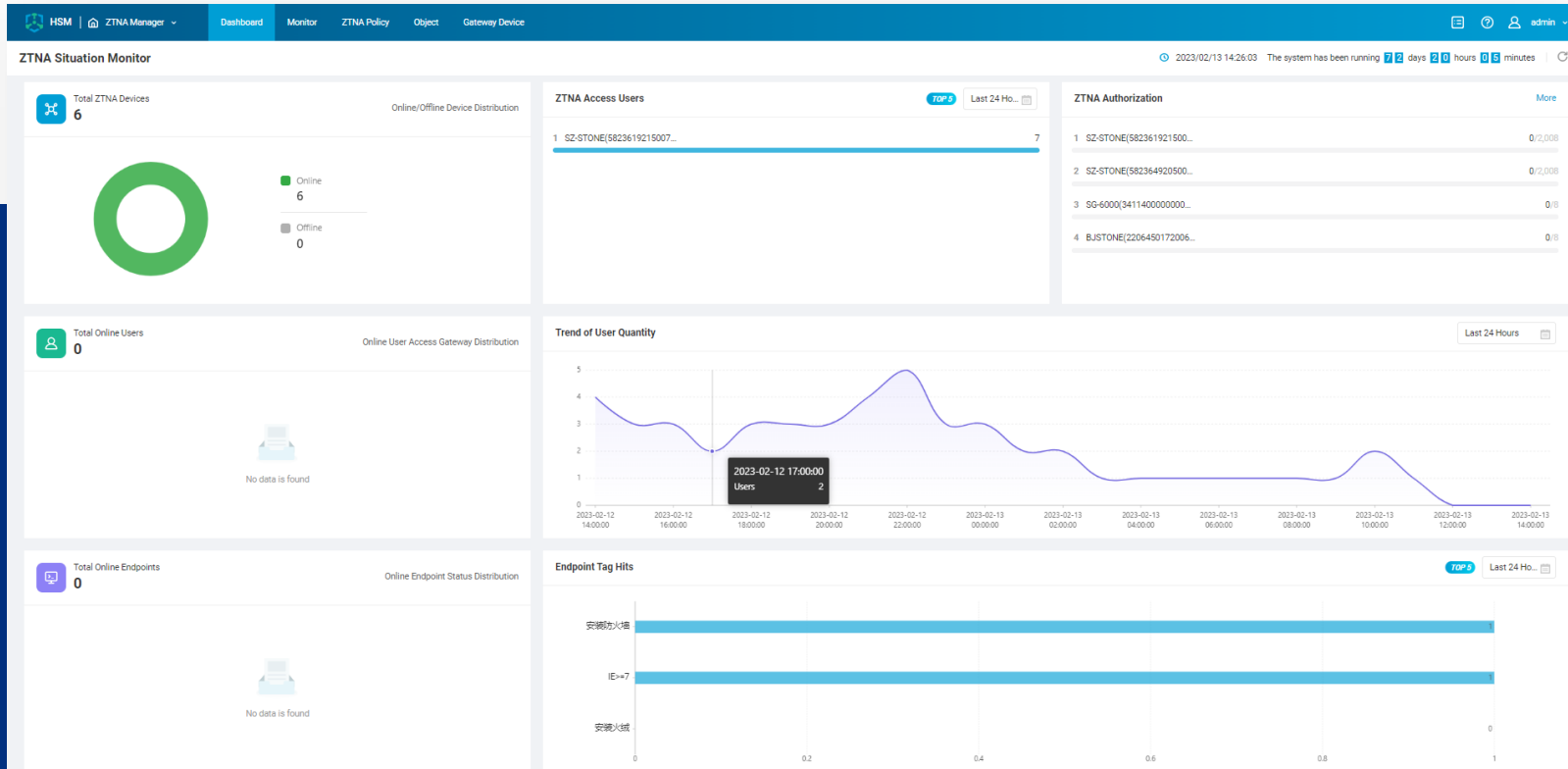


ZTNA Policy

- ZTNA policy package enforcement
- ZTNA individual device policy enforcement



ZTNA Monitoring Dashboard



ZTNA Situation Monitor

- Online/offline device distribution
- Online user access gateway distribution
- Online endpoint status distribution
- ZTNA authorized access users
- ZTNA total users
- Endpoint tag hits

Native Security with Hillstone NGFW



Intrusion Prevention



IP Reputation



URL Filtering



Anti-Virus




Cloud Sandbox



Botnet C2 Prevention

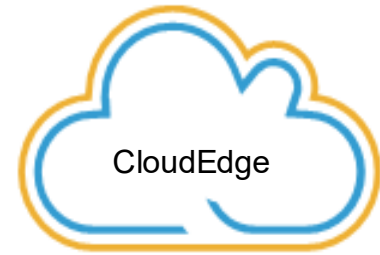
Supported HW Models

Supported VM Models

 **E/E-Pro/X Series**

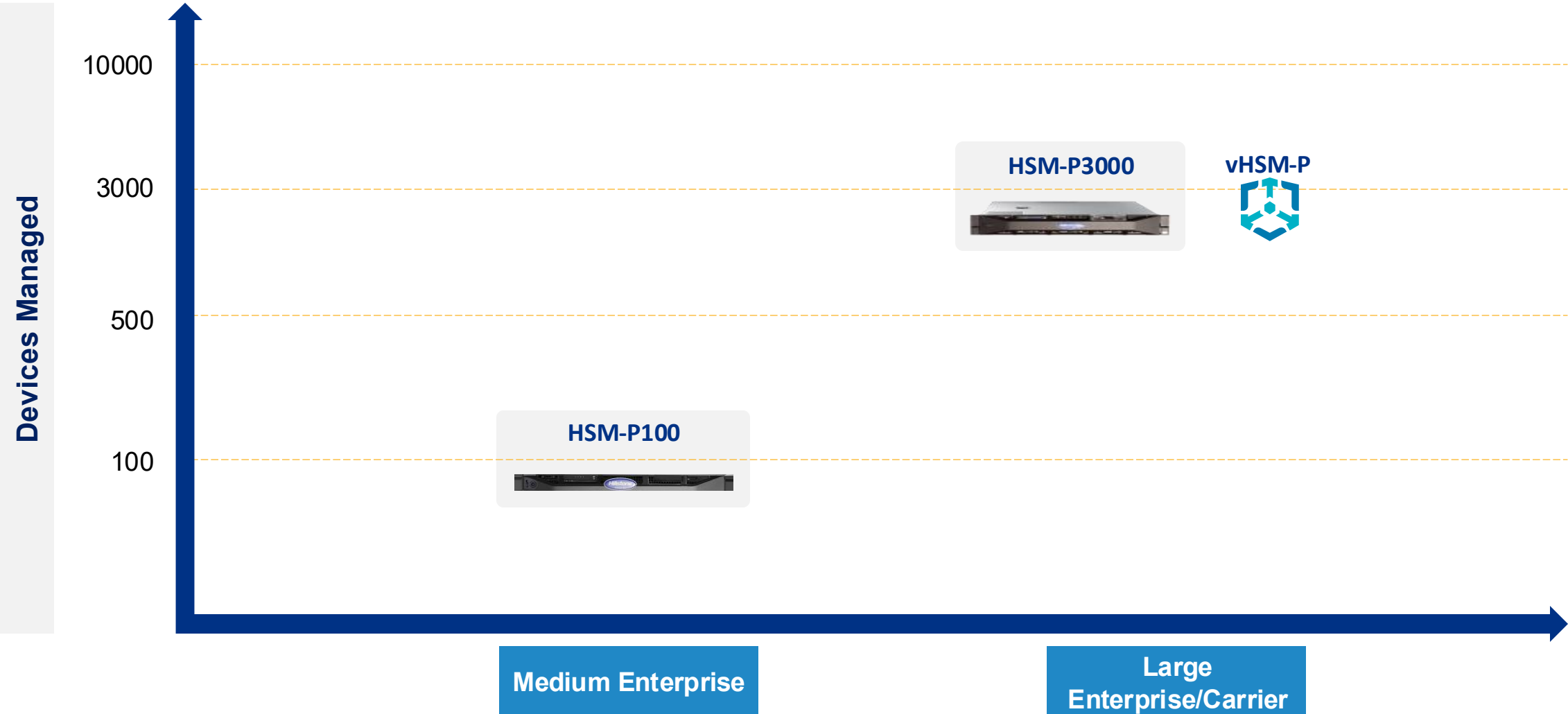
 **A Series**

 **CloudEdge**



Hillstone HSM Product Portfolio

HSM Product Positioning



HSM Hardware Platform

HSM Platform



HSM-P100



HSM-P3000

HSM Platform

	HSM-P100	HSM-P3000
Supported Devices	100	3000
Storage	SATA:2T	SSD:480G*2, SATA:8T*3
Network Interfaces	2* GE	6* GE
RAID	RAID 0	RAID 5
Power Supply	Single, 250W	Dual, 750W
Form Factor	1RU	2RU

Recommended Hardware Configuration for vHSM-P



Management Capability (Default / Maximum) *	0 / 100	0 / 500	0 / 1000	0 / 3000
vCPU Requirement	8 core	16 core	24 core	16 core (Hyper-Threading)
Memory Requirement	16GB	32GB	64GB	128GB
Port Requirement	2 ports	2 ports	2 ports	2 ports
Hard Disk Requirement (Minimum)	250 GB	250 GB	250 GB	250 GB
Virtual Environment Requirement	Vmware Workstation/ ESXi (6.5 or above)/ KVM (virtmanager 1.5.3 or above)/ AWS/ Huawei Cloud / Alibaba Cloud			

* No device management license by default for vHSM platform. Managed device amount can be obtained by purchasing device management licenses.

HSM SKU



Category	SKU	Definition	Term
Platform	SG-6000-HSM-P100-IN12/24/36/48/60	HSM-P100 Base System w/ HW&SW warranty	1-5 years
	SG-6000-HSM-P3000-AD-IN12/24/36/48/60	HSM-P3000 Base System w/ HW&SW warranty	
	SG-6000-vHSM-P-IN12/24/36	vHSM-P Base system (only platform license by default)/ software upgrade service	1-3 years
Subscription Service	SGSV-vHSM-IN12SU/24SU/36SU	Incremental software upgrade service for vHSM-P platform	1-3 years
Renewal Service	SGSV-HSM-P100-IN12U/24U/36U/12R	Incremental platform service for HSM-P100 (HW & SW maintenance service)	1-3 years for in service renewal and 1-yr for out of service renewal
	SGSV-HSM-P3000-AD-IN12U/24U/36U/12R	Incremental platform service for HSM-P3000 (HW & SW maintenance service)	
Other	SG-6000-HSM-P-DEV-IN	Device management license for each device (applicable to HSM-P100, HSM-P3000 and vHSM-P)	1 device (NGFW)

How to Order



Example 1

- 1 HSM-P100 with 1-year warranty
- Support 100 CPE devices

Order Item	SKU	Quantity
Platform	SG-6000-HSM-P100-IN12	1
License	SG-6000-HSM-P-DEV-IN	100

Example 2

- 1 HSM-P3000-AD with 2-year warranty
- Support 500 CPE devices

Order Item	SKU	Quantity
Platform	SG-6000-HSM-P3000-AD-IN24	1
License	SG-6000-HSM-P-DEV-IN	500

Example 3

- 1 vHSM-P with 1 year upgrade service
- Support 100 devices management

Order Item	SKU	Quantity
Platform	SG-6000-vHSM-P-IN12	1
License	SG-6000-HSM-P-DEV-IN	100

SD-WAN Deployment Scenarios & Winning Cases

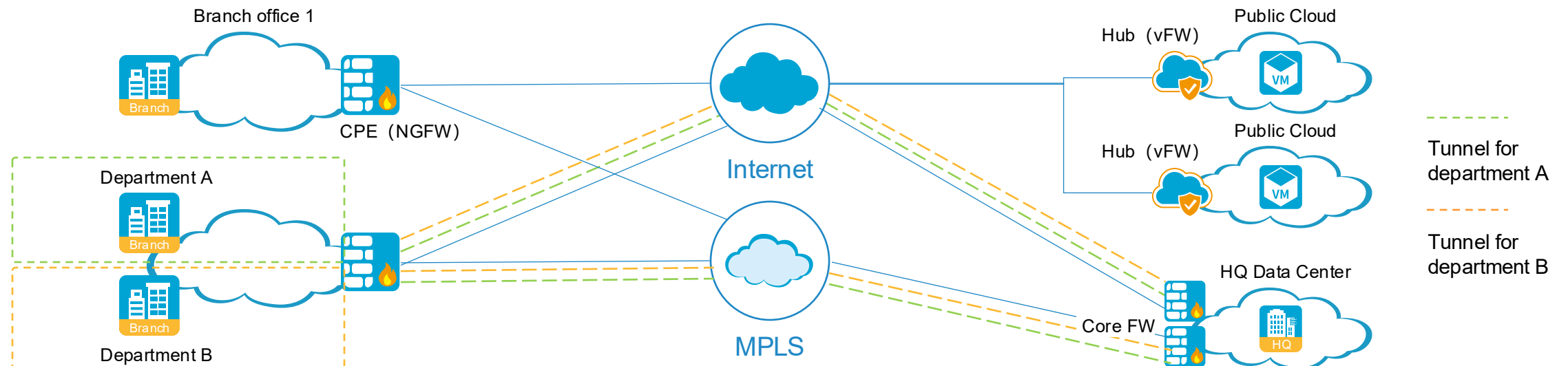
Deployment Scenario Large Enterprise and Government Branches

Challenges and requirements

- Multiple branches country-wise or globally
- Secure connections between headquarter and branches
- Centralized management and configuration
- Flexible traffic steering policy
- Improved user experience for cloud apps

HSM benefits

- VPN Overlay automation and fast business orchestration
- ZTP for quick and efficient deployment
- Centralized management and monitoring with deep visibility
- Native security powered by StoneOS



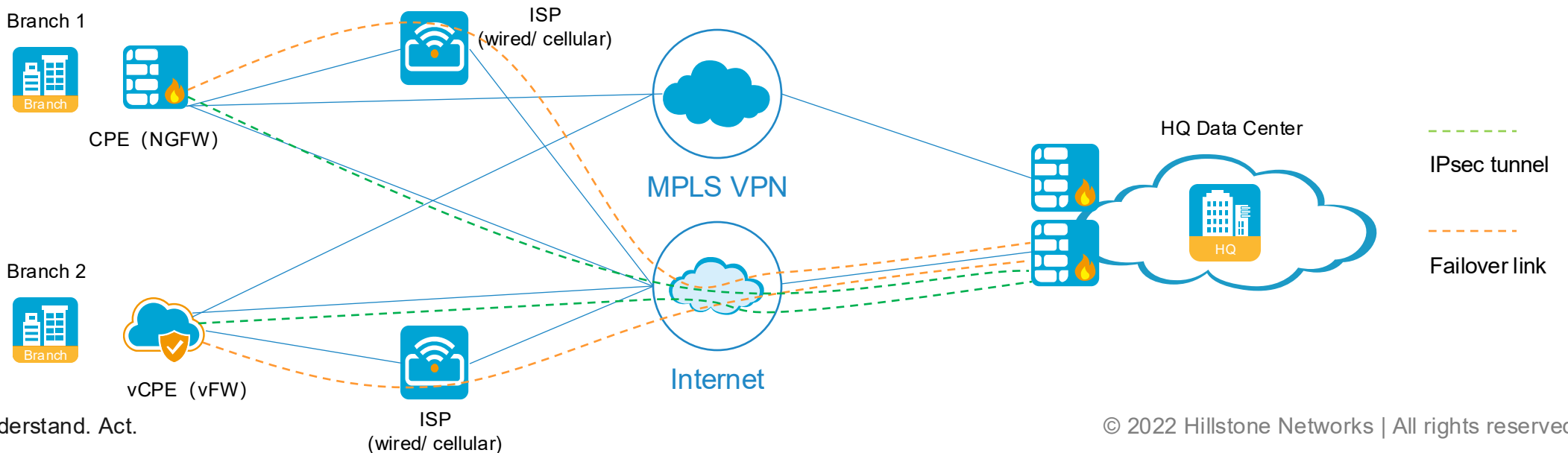
Deployment Scenario Financial Service Industry

Challenges and requirements

- Ensure critical apps/ services are guaranteed
- Improve user experience for multiple apps and services
- Require high security and high availability
- Low efficiency in managing a large number of branches

HSM benefits

- Smart traffic steering for apps/ services
- Link auto failover, aggregation and load balancing for high performance and high availability
- ZTP and Fast business orchestration
- Centralized management and monitoring



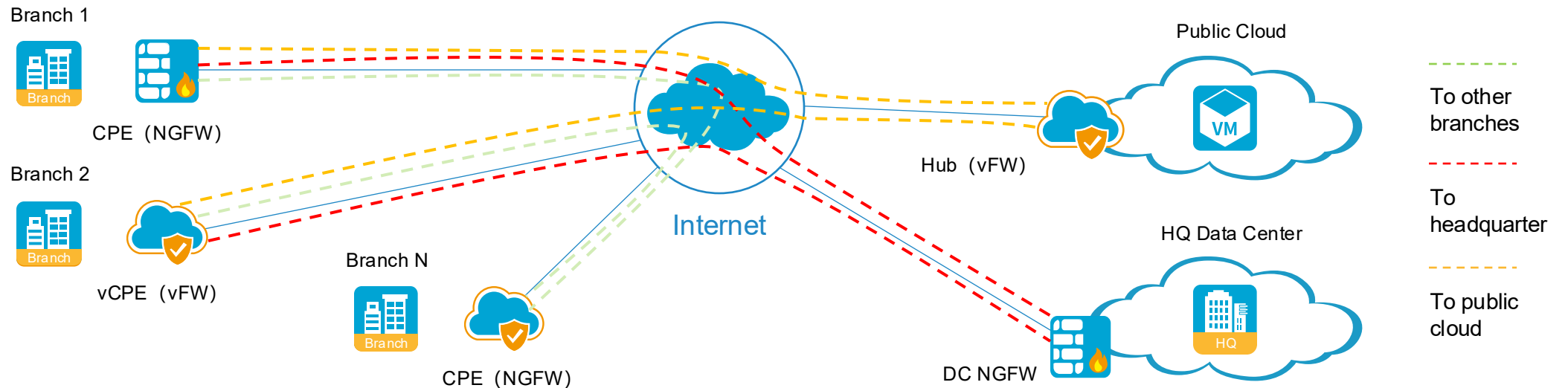
Deployment Scenario Retail

Challenges and requirements

- Massive deployment across different regions with different network condition
- Interconnection between branches and HQ, and among branches.
- Multiple apps/ services, such as CRM, supply chain management, payment, etc.

HSM benefits

- VPN Overlay automation reduce the effort and TCO
- Smart traffic steering for apps/ services
- Quick deployment and business orchestration
- Centralized management and monitoring



Winning Cases: HSM



Cable Color
ISP
Honduras, vHSM



Maxis Berhad
ISP
Malaysia, HSM50



CENACE
Energy
Mexico, HSM50



Grupo ICE
Energy
Costa Rica, HSM50



China Mobile
ISP
China, HSM50



The Secretariat of the
Senate
Government
Thailand, HSM50



CN Care
Other
China Hong Kong,
SD-WAN, HSM



Dubai International School
Education
UAE, HSM50



First Capital Securities
Finance
China, HSM50



Hua'an Fund Management
Finance
China, HSM50



Royal Thai Embassy
Government
Thailand, vHSM



Ministry of Foreign Affairs
Government
Pakistan, HSM50



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

