

WHITE PAPER

---

Hillstone Networks  
Next-Gen SD-WAN

# **Building on a Secure Foundation**

# Introduction

## Enterprise WAN Needs

Businesses have an insatiable demand for bandwidth and connectivity. Every year, we experience a relentless growth in enterprise data transmitted over networks, with aggregate data scaling from gigabytes to terabytes to petabytes to exabytes. In the meantime, the number of enterprise locations needing connectivity is expanding: data centers, corporate campuses, branches, employee home offices, coffee shops, airports, and multiple public clouds.

The nature of this connectivity is changing, with enterprise wide-area network (WAN) requirements driven by the following trends:

- **Cost-efficiency:** Push to reduce wide-area network (WAN) connectivity costs despite increased locations and bandwidth use.
- **Always-on cloud services:** Reliance on a highly available network for cloud-based applications and cloud storage.
- **Multiple connections:** Multiple WAN links, once the practice of only the largest corporations, are becoming commonplace.
- **Flexible locations:** Dynamic enterprise locations including coworking spaces, pop-up retail locations, shorter leases, or short-term sub-leases.
- **Diverse traffic patterns:** Changing traffic patterns, trading hub-and-spoke centered around corporate data centers, for partial or full meshes across multiple locations, with an increasing amount of traffic spread across public clouds and software-as-a-service (SaaS) applications.
- **Sophisticated policies:** Increased capabilities in connectivity and security policies that assist with business agility and connectivity performance. Businesses are looking for their connectivity and security solutions to be more context and content-aware to better secure business applications.
- **Security-focused:** Hyper-awareness around security attacks as headlines continue to highlight the latest in security breaches and ransomware attacks.

## Contents

The Rise of SD-WAN . . . . .	3
3 Defining SD-WAN	
4 Flavors of SD-WAN	
Hillstone Networks SD-WAN Solution . . . . .	6
Key Hillstone SD-WAN Capabilities. 6	
7 Zero-Touch Provisioning (ZTP)	
8 Support for Diverse Topologies	
9 Streamlined User Interface (UI)	
9 Unified Network Visibility	
10 Application and Context-Aware Routing	
11 Smart Workflow Orchestration	
12 Superior Security Capabilities	
Hillstone SD-WAN Architecture . . .	13
Getting Started with Hillstone SD-WAN . . . . .	14
Why Hillstone? . . . . .	15

## The Rise of SD-WAN

With the current enterprise IT backdrop, it is unsurprising that software-defined wide-area networking (SD-WAN) continues to dominate WAN refreshes and a large chunk of IT budgets. The Dell'Oro Group, a market research firm, expects the SD-WAN market to surpass \$4 billion by 2025. Meanwhile, Gartner, an analyst firm,

predicts that enterprise spending on SD-WAN products will grow at a 29.1% compound annual growth rate (CAGR) from 2018 through 2023. These growth rates and market sizes aren't surprising—after all, SD-WANs promise faster, cheaper, more scalable, more secure WAN connections that are easy to deploy and manage.

## Defining SD-WAN

Even though SD-WAN's rise has been rapid, SD-WAN is more of an evolution of existing WAN solutions rather than an entirely new category. Most analysts and industry experts view SD-WAN solutions as WAN products that exhibit the following four capabilities:

- **Centralized management with automated provisioning**—SD-WAN solutions need to provide simple configuration and provisioning, often in the form of zero-touch provisioning (ZTP). With this philosophy, the product requires no technical skills or expertise in remote bringup. This focus on low-overhead and fast bring up, coupled with a centralized cloud-controlled console, is what keeps the operating costs of SD-WAN solutions low and simplifies troubleshooting.
- **Encrypted overlay tunnels over different physical links**—One of the critical elements of SD-WAN is its ability to utilize various types of connectivity, including lower-cost direct internet access for increased bandwidth without the corresponding higher prices. Likewise, with the increased popularity of fixed 4G and 5G wireless access, SD-WAN solutions can use these cellular links to increase resiliency when wireline links fail. SD-WAN can even use such links as primary connectivity when mobile data plans inevitably fall in price. Furthermore, with IPsec or TLS encryption over these different links, enterprises can rest assured that, regardless of whether the underlying links are tied

into public networks or shared backbones, their traffic is protected from prying eyes and malicious attackers.

- **Multi-link handling and intelligent routing**—Another essential SD-WAN capability is using multiple types of links in an intelligent manner. SD-WAN solutions can send traffic over multiple connections simultaneously, taking advantage of different link characteristics and leveraging smart routing rules. For example, SD-WAN solutions can send bulk traffic over cheaper links while prioritizing performance-sensitive traffic over higher QoS private links like MPLS. Likewise, SD-WANs can direct internet-facing traffic to SaaS applications directly over broadband links, skipping the hop through corporate HQ, which is typical of legacy VPN installations.
- **Converged security and connectivity**—Enterprises today expect converged connectivity with security. Separate router and firewall setups commonplace in previous generations of corporate branch setups are no longer desired. Making a joint routing and security decision as each packet traverses a customer-premises equipment (CPE) device makes a lot of sense since it takes a single pass to understand the context and content. This reduces overhead and latency. Plus, it allows for more sophisticated and informed packet handling decisions, such as the stringency of checks based on the type and destination (or source) of the traffic.

## Flavors of SD-WAN

Many sub-categories of SD-WAN products exist in the market, with numerous evolved from yesterday's branch routers or VPN solutions. Other solutions are from the enterprise WiFi space, and yet others are extensions of cloud-based networking solutions. The origins of each sub-category of SD-WAN solutions define their feature

strengths, even as they work to close the gap between a full-fledged SD-WAN solution and where they are today. For example, a WiFi-based SD-WAN solution will have robust branch WiFi features and simple cloud-based provisioning but likely lacks strong security capabilities.

SD-WAN Origins	Strengths	Common Gaps
Branch routers	<ul style="list-style-type: none"> <li>■ Strong routing capabilities, handles complex routing topologies and rich set of routing protocol support.</li> <li>■ Often already in place as incumbent.</li> <li>■ Native support for multiple legacy connection types (MPLS, T3, T1 etc.). Usually have IPsec VPN support.</li> </ul>	<ul style="list-style-type: none"> <li>■ Limited security capabilities.</li> <li>■ Lacks awareness of traffic in layers 4-7.</li> <li>■ Often limited support for centralized provisioning and management capabilities.</li> <li>■ Direct connections between sites and into public clouds might be challenging (limited topology support, lack of virtualized instances).</li> </ul>
Network virtualization	<ul style="list-style-type: none"> <li>■ Strong overlay capabilities (usually with encryption), connectivity into private and public cloud centers well supported.</li> <li>■ Consistent networking policies across multiple sites, convenience of centralized management.</li> </ul>	<ul style="list-style-type: none"> <li>■ Lacks security capabilities in layers 4-7.</li> <li>■ Limited routing support.</li> <li>■ Basic CPE with limited interface support, often requiring a separate device.</li> </ul>
Cloud networking	<ul style="list-style-type: none"> <li>■ Centralized management capabilities with convenient ZTP support.</li> <li>■ Rich application categorization with direct routing to popular SaaS applications.</li> <li>■ Multiple PoP gateways provide convenient integration point for external security services.</li> <li>■ Private backbone options can provide better end-to-end performance when integrated into popular public cloud and SaaS applications.</li> </ul>	<ul style="list-style-type: none"> <li>■ Limited security capabilities without relying on external functions.</li> <li>■ Little to no local security functions on CPE on-premises.</li> <li>■ Little to no support for legacy branch interfaces.</li> <li>■ Limited support for complex underlay routing functions.</li> </ul>

SD-WAN Origins	Strengths	Common Gaps
Branch WiFi	<ul style="list-style-type: none"> <li>■ Convenient ZTP setup and simple centralized cloud management.</li> <li>■ Handles branch local connectivity as part of package.</li> </ul>	<ul style="list-style-type: none"> <li>■ Limited routing (including multi-link handling) and CPE capabilities restrict these solutions to smaller locations.</li> <li>■ Limited built-in local security; therefore, requires integration with external security functions (in cloud or locally) to meet enterprise security needs.</li> </ul>
WAN optimization/bonding	<ul style="list-style-type: none"> <li>■ Intelligent use of multi-path routing allows for improved performance over multiple connectivity providers.</li> <li>■ Can help generate cost savings through use of cheaper lower-QoS broadband connections without sacrificing reliability.</li> </ul>	<ul style="list-style-type: none"> <li>■ Basic routing and CPE capabilities only, which restrict the applicability of this class of solutions.</li> <li>■ Restricted security feature set.</li> </ul>
CPE providers	<ul style="list-style-type: none"> <li>■ Rich set of connectivity options, even for legacy connection types.</li> <li>■ Bare-bones functionality and streamlined basic apps (often leveraging open-source) like routing or simple stateful firewall helps keep overall costs low.</li> </ul>	<ul style="list-style-type: none"> <li>■ Limited feature set restricts this class of solutions to companies with only simple needs (CPE providers generally host VNFs from other SD-WAN providers).</li> </ul>
NGFW and other security solutions	<ul style="list-style-type: none"> <li>■ Strong security foundations and capabilities meet enterprise needs both locally at the branch and over the WAN.</li> <li>■ More established and advanced NGFWs will usually have adequate routing to meet most enterprise requirements.</li> </ul>	<ul style="list-style-type: none"> <li>■ Centralized management and ZTP capabilities have historically been lacking.</li> <li>■ Multi-link handling and intelligent application-specific routing features are usually not as mature as those in the WAN optimization categories.</li> <li>■ Not all NGFWs have proven and comparable virtual instances for public and private cloud integration.</li> </ul>

With the diversity of SD-WAN solution types, each will demonstrate varying degrees of maturity in meeting the core SD-WAN criteria above. However, with the emphasis enterprises place on cybersecurity today, an SD-WAN solution rooted in security represents the best chance at modernizing enterprise connectivity while battling ransomware and security breaches.



## Hillstone Networks SD-WAN Solution

Hillstone Networks is a leader in infrastructure protection, offering a proven, trusted, and cost-effective unified platform for end-to-end visibility, intelligence, and control that can mitigate and manage risks from the edge to the cloud. By building our SD-WAN solution on our leading next-generation firewall products (NGFW) platform, we ensure that our customers gain access to new SD-WAN features while retaining the utmost cybersecurity protection.

Hillstone's SD-WAN solution secures enterprise branch locations while defending against new multilayer, multi-stage attacks and blocking ransomware and zero-day exploits. Evolving a sophisticated security solution built around frameworks like the cyber kill-chain and MITRE ATT&CK has become a critical necessity.

Our SD-WAN solution extends our NGFW security platforms and continues to provide:

- Improved WAN visibility— To **see** what's going on across all enterprise locations, enabling greater visibility into user, device, and resource access behavior at every site.
- Advanced intelligence— To **understand** who is accessing what, from where, and which devices at each location.
- Distributed enforcement at scale— Our new HSM V5.0 release turns the Hillstone Security Manager appliances into an SD-WAN controller. Our SD-WAN software supports zero touch provisioning and sophisticated policies while leveraging the power and performance of our NGFWs to **act** rapidly, enforcing fine-grained access policies across all SD-WAN locations.

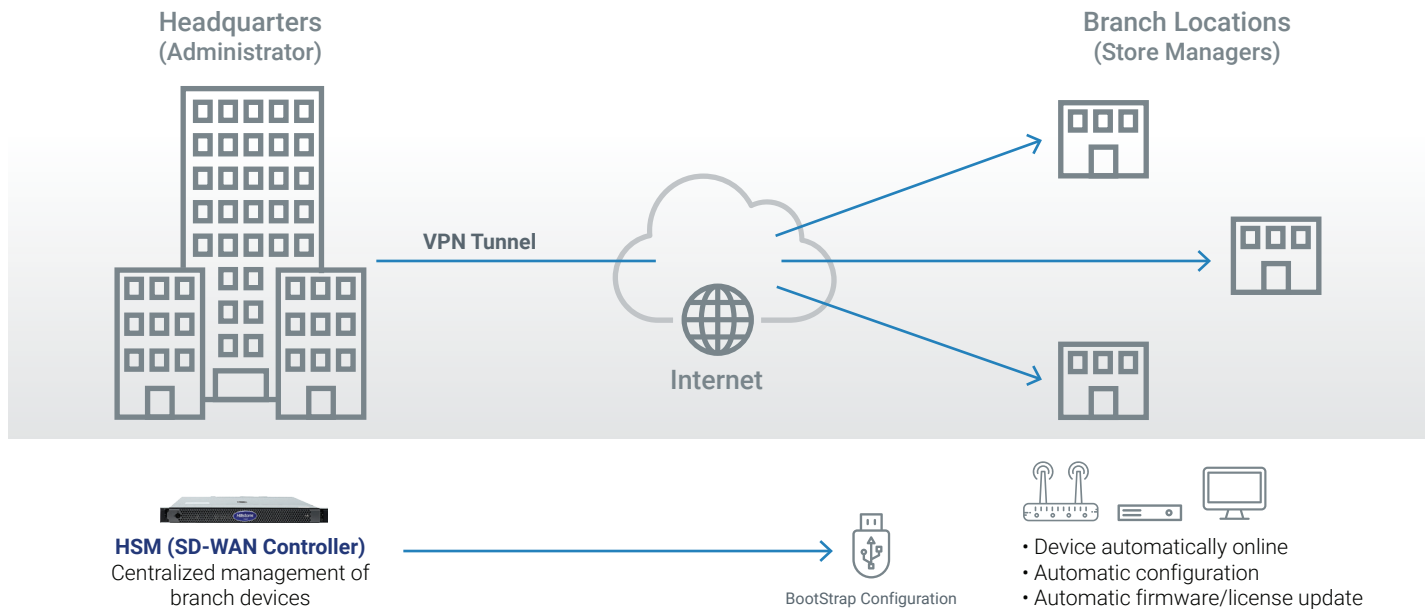
## Key Hillstone SD-WAN Capabilities

Hillstone's SD-WAN offering comes with numerous new features that enhance the value of existing and continued investment in the Hillstone NGFW platform suite. With HSM V5.0, the HSM appliances (HSM-P100 and HSM-P3000) operate as our new SD-WAN controllers, integrating with our hardware appliances (E/E-Pro/X series and our new A series) and virtual NGFW (Hillstone CloudEdge). Our new SD-WAN solutions support our leading NGFW capabilities and add a host of new features, which we'll examine in more detail.

## Zero-Touch Provisioning (ZTP)

While HSM previously provided centralized management at scale for our NGFW product lines, our new SD-WAN controller capabilities take provisioning to new levels. The zero-touch-provisioning (ZTP) feature supports the creation of templates for auto-provisioning of system settings but also supports license installa-

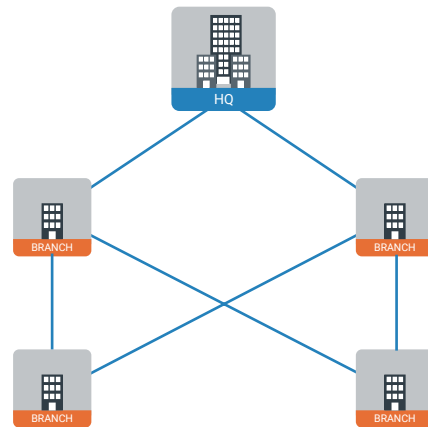
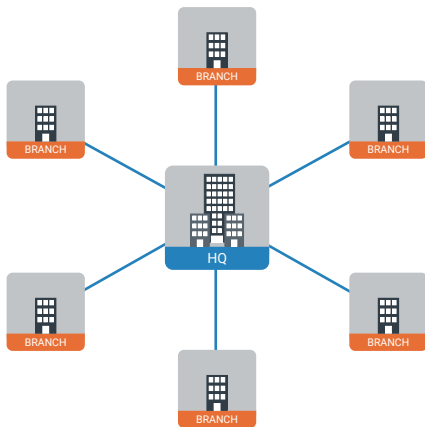
tion and firmware auto-upgrades. Generating a USB template configuration allows mass remote configuration of NGFW at branch sites via USB flash drives, triggered by a simple reboot. ZTP enables rapid provisioning of devices even in locations without skilled IT personnel.



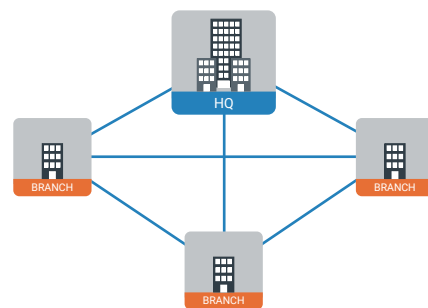
## Support for Diverse Topologies

Previous VPN topologies without SD-WAN capabilities were limited to simple site-to-site or hub-and-spoke (star network) configurations. The SD-WAN features support the same star configuration but allow for

improved resiliency through dual hubs. For enhanced flexibility, multiple overlapping star networks on different WAN interfaces can also be configured.



Furthermore, our SD-WAN controllers support full-mesh options, allowing multiple point-to-multipoint connections between devices (physical and virtual), and providing low-latency and high-bandwidth direct connections between devices in the mesh.





## Streamlined User Interface (UI)

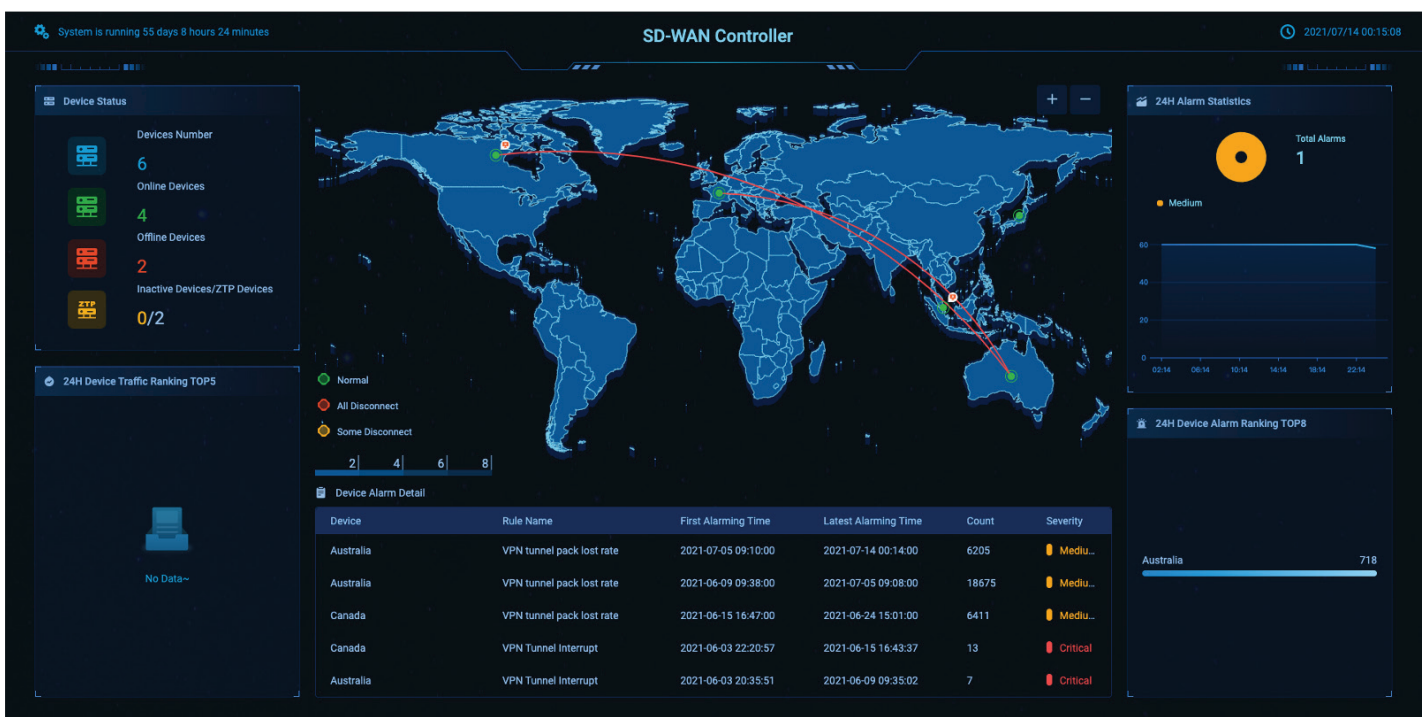
Legacy UIs impede rapid deployment and configuration. At Hillstone, we recognize the importance of simplicity in UIs and believe that eliminating complexity improves enterprise security. In that vein, we continue to work hard on streamlining our user interfaces. With the SD-WAN release,

we've revamped our UI, providing simple at-a-glance views of the devices in the network, their status, any alarms, and ongoing traffic flows. This streamlined UI simplifies operations for customers and supports large-scale deployments of SD-WANs.

## Unified Network Visibility

Our dashboards can display a global view of multiple branches, campuses, and data center locations, along with statuses of the devices deployed in those locations. Configurable alarm rules and triggers allow important events to be highlighted, and drill-down views that show the details behind every device. System information, software information, security, and malware signature database updates facilitate troubleshooting.

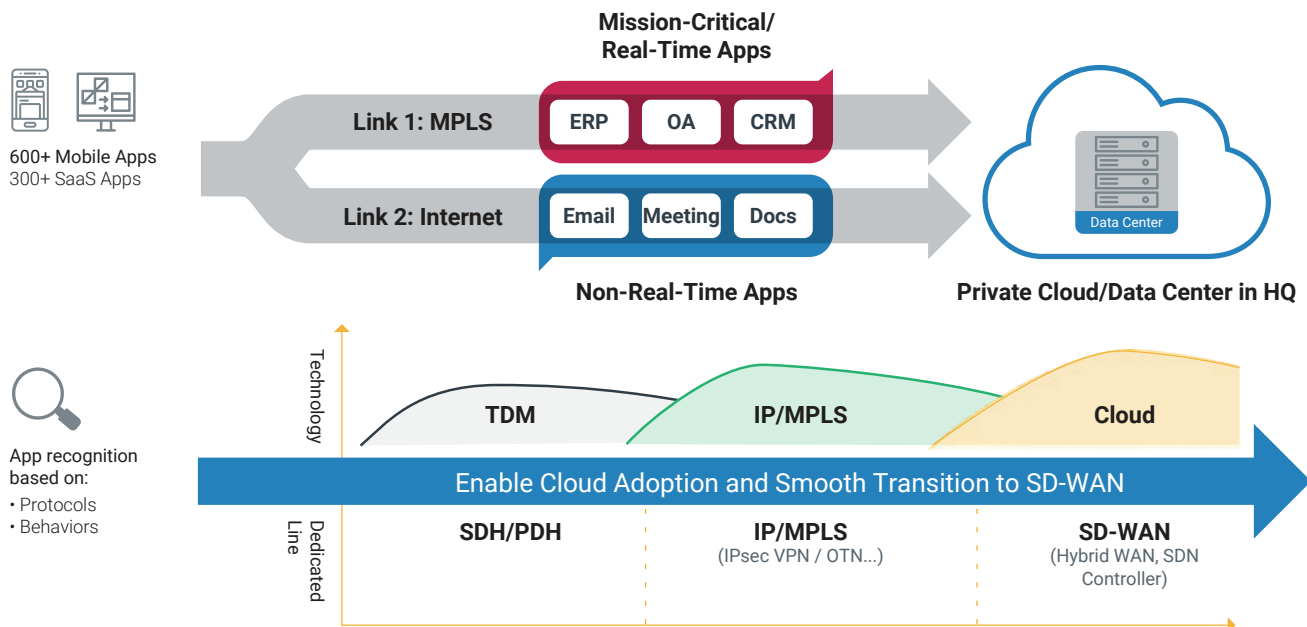
The SD-WAN controller software on HSM facilitates under-the-hood troubleshooting and configuration updates via a WebUI or CLI proxy, depending on what is needed. Centralizing all configuration and management functions through the controller reduces the operational overhead for IT staff and mitigates the need for remote site visits.



## Application and Context-Aware Routing

Hillstone's SD-WAN benefits from our NGFW's traffic categorization capabilities, providing support for matching source and destination addresses, service details, and even application types. By leveraging this service matching, enterprise IT can implement sophisticated rules that WAN physical and virtual interfaces use for different traffic types. In addition, multi-link resiliency is enhanced through fine-grained load-balancing and routing rules (active-active with load balancing, primary-backup, custom rule-driven), providing the utmost flexibility.

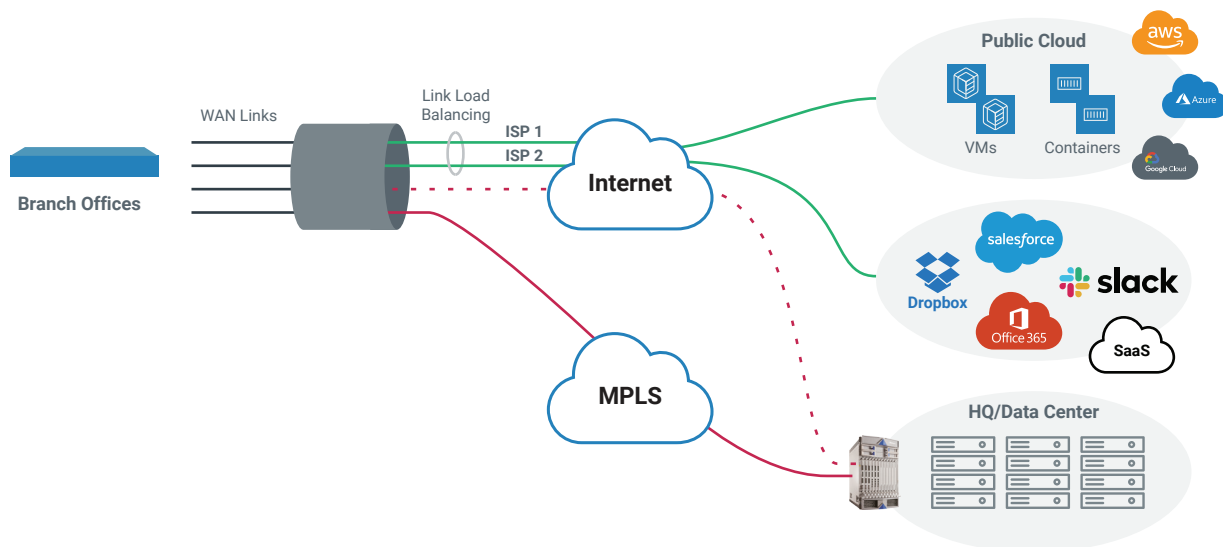
The same capabilities can be used to direct different classes of traffic over various links. For instance, routing latency-sensitive collaboration and communications traffic over more expensive MPLS private links between corporate sites while using cheaper IPsec tunnels over business broadband for bulk file transfers.



## Smart Workflow Orchestration

Beyond putting in place service-based or application-based rules, our SD-WAN solution provides business-oriented workflow rules. This feature offers intelligent and convenient control over access and routing capabilities, differentiating between internal corporate applications and public SaaS. Security policies, routing rules, and even NAT configurations can be applied automatically based on the context of access and type of application.










For instance, a business may want to allow access to certain internal applications and resources at a HQ from all branch locations. By defining a business workflow once, Hillstone's SD-WAN controller can push the same policy across all remote locations to enable these controls. Any new branch coming online would be subject to the same policy without further configuration.



## Superior Security Capabilities

The foundation for Hillstone products is an industry-leading NGFW with all the capabilities you would expect from a product suite that's made the Gartner Magic Quadrant for network firewalls for seven consecutive years. Both our E-Series and new A-Series NGFWs provide an uncompromising and rich feature set that rivals all major NGFW

incumbents in the market. Hillstone NGFW supports advanced policies, advanced threat and malware protection, including TLS decryption, command and control site blocking, IP reputation, and cloud sandboxing.

<b>Application Control</b> <b>4000+</b> Application identification 	<b>Intrusion Prevention</b> <b>8000+</b> IPS signatures 	<b>Antivirus</b> <b>Real-time Updated</b> Virus and malware detection 
<b>Network Attack Defense</b> <b>Attack Defense</b> Anti-DDoS/DDoS, protocol anomaly 	<b>User Control</b> <b>Authentication</b> Combined with AD authentication account 	<b>IP Reputation</b> <b>Block risky IPs</b> from accessing servers 
<b>URL Filtering</b> <b>140+ Million</b> Dynamic URL filtering 	<b>Botnet C&amp;C</b> <b>Post breach protection</b> blocks the control channel and catches intranet bots 	<b>Sandbox</b> <b>Multiple protocols &amp; file types</b> Complete behavior analysis 
<b>Firewall</b>		

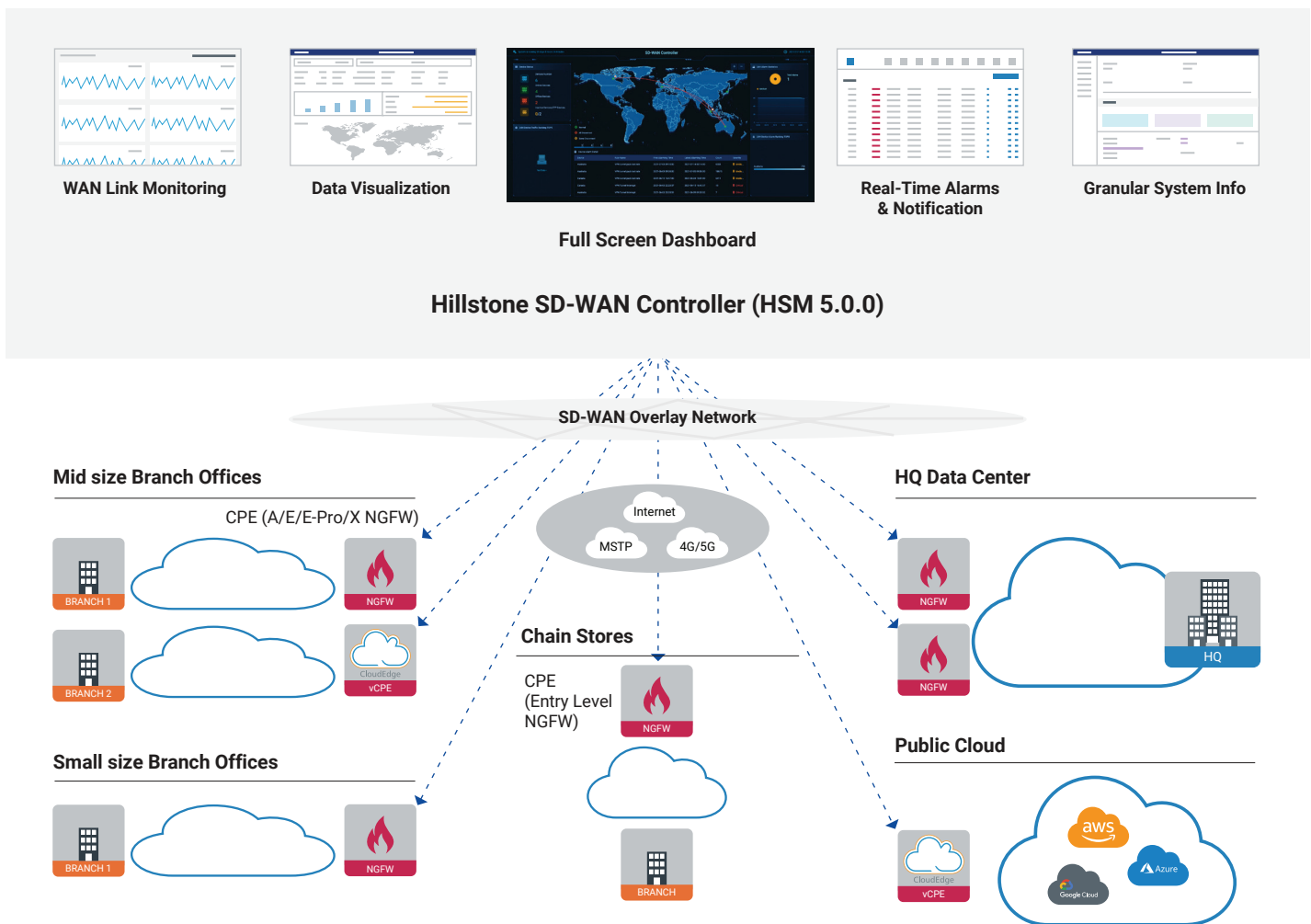
While many classes of SD-WAN solutions support multi-link connectivity and flexible routing, our SD-WAN product is built on a foundation of enterprise and carrier-grade security. Enterprise customers all over the world have identified security as a critical priority for their WAN modern-

ization. Only a security-focused SD-WAN like Hillstone's can address WAN challenges while continuing to defend against the increasing number and growing sophistication of security attacks faced by enterprises today.

## Hillstone SD-WAN Architecture

Hillstone's SD-WAN solution is made up of the following components:

- SD-WAN controller running on the HSM platform that orchestrates and manages the different SD-WAN end-points
- Hillstone virtual NGFW (CloudEdge) installed in virtual machines on private or public clouds
- Hillstone NGFW (A series, E/E-Pro/X series) at corporate HQ and branch locations



In the diagram above, the dedicated SD-WAN controller running as part of the HSM provides vital functionality for managing the multiple SD-WAN end-points across the network. Whether these SD-WAN nodes are Hillstone NGFW acting as CPE, or virtual NGFW (CloudEdge) playing the role of the virtual CPE in a public or private cloud, the Hillstone SD-WAN controller can configure, manage and monitor all these nodes globally.

As depicted, Hillstone's SD-WAN solution supports multiple link types, from dedicated MPLS links to direct internet access via broadband to 4G/5G fixed wireless connections. Each SD-WAN node can simultaneously manage across multiple underlay connections, applying sophisticated content and application-aware policies. Likewise, flexible topologies are supported by Hillstone's SD-WAN controller.

Hillstone's SD-WAN is a strong contender in the space, built on our superior security foundations. As we revisit the essential market requirements for SD-WAN, it's clear that Hillstone's solutions more than meet the criteria:

- **Centralized management with automated provisioning**— Our ZTP capabilities and HSM provide a unified global view across the thousands of devices in the network, with automated provisioning that bundles in a software update and licensing for the fastest hassle-free onboarding.
- **Encrypted overlay tunnels over different physical links**— As IPsec and TLS experts, we've leveraged our expertise to build secure, high-performance tunnels supporting multiple topologies, from hub-and-spoke (star) to double-hub for resiliency to full-mesh for extreme connectivity and flexibility. We've supported numerous connection types historically, and with our SD-WAN solution, we provide even greater visibility with our dedicated line monitoring and visualization.
- **Multi-link handling and intelligent routing**— Our SD-WAN smart routing and business workflow orchestration capabilities provide service and application-aware routing capabilities, including enabling load-balancing across multiple links, primary-backup setups, and combinations in between. Differentiating between internal and external applications and applying different routing and security policies to various traffic classes is easily achieved with the Hillstone solution.
- **Converged security and connectivity**— Providing more than just converged security and connectivity, Hillstone's SD-WAN has built intelligent and flexible connectivity on a bedrock of superior protection. Having an industry-leading NGFW as a foundation lends our solution substantial credibility, especially with today's enterprises reeling from the onslaught of ransomware attacks and data breaches.

## Getting Started with Hillstone SD-WAN

Hillstone Networks SD-WAN is available with the release of HSM v5.0.0. Our new revamped UI provides the full range of SD-WAN capabilities in a simple-to-use dashboard. Supporting up to 3,000 devices in its initial release, even large global enterprises with thousands of sites can benefit from Hillstone's security-focused SD-WAN solution.

For existing customers with our CloudEdge NGFW solution, migration to the new SD-WAN feature set is seamless, and you continue to benefit from our market-leading security protection while gaining unparalleled ease-of-management, improved reliability, and agile WAN routing. Not to mention, you'll enjoy improved cost-savings from being able to use

cheaper broadband connections in your WAN connectivity mix while retaining control over quality-of-service for sensitive corporate applications.

For new customers contemplating WAN upgrades, Hillstone provides the best value in the security space, with features and capabilities rivaling the largest incumbents in the enterprise security market, but at an affordable price. And with our feature-rich SD-WAN capabilities, Hillstone is a natural choice for your WAN modernization projects.



## Why Hillstone?

Hillstone Networks was founded by security industry veterans from NetScreen, Cisco, and Juniper. With our security heritage and innovative solutions, Hillstone has built a comprehensive suite of products that protect enterprises worldwide.

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 multilayer, multi-stage 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 SD-WAN, NGFW, ZTNA, breach detection, 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.

## Learn More

Engage with us to learn more about Hillstone's SD-WAN solutions by contacting your local authorized Hillstone Networks reseller.

[www.Hillstonenet.com/solutions/secure-sd-wan/](http://www.Hillstonenet.com/solutions/secure-sd-wan/)



Visit [www.hillstonenet.com](http://www.hillstonenet.com) to learn more  
or contact Hillstone at [inquiry@hillstonenet.com](mailto:inquiry@hillstonenet.com)

