



























# SD-WAN Competitive Comparison Chart

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Networking</b>							
<b>Supports traditional routing and SD-WAN on the same platform</b>	 <p>Comprehensive traditional routing services. Smooth migration with features relevant to SD-WAN on the same platform. Unified image common across traditional routing and SD-WAN.</p>	 <p>No investment protection for smoother migration in relation to SD-WAN on same platform. Limited traditional routing feature set.</p>	 <p>Enabling SD-WAN does not require adding to, or changing, existing infrastructure.</p>	 <p>No investment protection for smoother migration in relation to SD-WAN on same platform. Limited traditional routing feature set.</p>	 <p>Requires adding new hardware to use SD-WAN.</p>	 <p>Enabling SD-WAN does not require adding to, or changing, existing infrastructure. Limited traditional routing feature set.</p>	 <p>Smooth migration to SD-WAN on the same platform. Complete traditional routing services available.</p>
<b>Core, edge, and cloud SD-WAN</b>	 <p>Appliances built to service core, edge, and cloud locations. Wide range of form factors with physical and virtual offerings.</p>	 <p>Appliances built to service core, edge, and cloud locations.</p>	 <p>Appliances built to service core, edge, and cloud locations.</p>	 <p>Appliances built to service core, edge, and cloud locations.</p>	 <p>Appliances built to service core, edge, and cloud locations.</p>	 <p>Appliances built to service core, edge, and cloud locations.</p>	 <p>Appliances built to service core, edge, and cloud locations.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Purpose-built SD-WAN Architecture</b>	 <p>Dedicated control, data, and management plane components for scalability and performance, offering an SDN-compliant architecture. Flexibility of matching architecture to business Intent. Cloud-hosted deployment managed by Cisco Cloud Ops team.</p>	 <p>Integrated control and data plane components limit flexibility.</p>	 <p>Legacy firewall-based architecture.</p>	 <p>Legacy combined control and data plane architecture.</p>	 <p>Dedicated control, data, and management plane components.</p>	 <p>Integrated control and data plane components limit flexibility.</p>	 <p>Integrated control and data plane components limit flexibility.</p>
<b>True zero-touch provisioning</b>	 <p>Mutually authenticated, multi-factor authentication with zero-touch provisioning for all components. One touch provisioning for air-gapped networks and MSPs.</p>	 <p><b>Limited</b> Requires additional authentication steps to provision.</p>	 <p>Multiple touch points to enable ZTP process. As it is based on Firewall enabling SD-WAN, it requires manual policy configurations.</p>	 <p><b>Limited</b> EdgeConnect devices are preconfigured, however requires additional authentication steps to provision.</p>	 <p>Multiple touch points.</p>	 <p>The ION devices are pre-configured to authenticate to the portal and support zero-touch provisioning and deployment.</p>	 <p><b>Limited</b> Requires additional authentication steps to provision.</p>






















	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Active-active dual router SD-WAN topology</b>	<p>Allows for active-active networking to provide higher throughput and greater reliability. Capability to horizontally scale with easy-to-use features.</p>	<p>Does not support active-active connections.</p>	<p><b>Limited</b> Additional WAN switch required, which creates dependencies.</p>	<p><b>Limited</b> Allows for active-active networking but requires an additional switch, which creates dependencies.</p>	<p>Does not support active-active connections.</p>	<p>Does not support active-active connections.</p>	<p>Supports active-active connections.</p>
<b>Advanced routing protocols for brownfield integrations</b>	<p>Extends advanced routing intelligence, such as EIGRP, OSPF, RIP, and BGP, into cloud environments, allowing for faster, more reliable connectivity to cloud workloads. Supported with dual stack. Capability to also do underlay/overlay routing. Flexible policy and attribute support for easy routing manipulation.</p>	<p><b>Limited</b> Advanced routing protocols such as BGP, OSPF supported but does not provide the most efficient path selection.</p>	<p>Advanced routing protocols such as BGP, OSPF supported but does not provide the most efficient path selection.</p>	<p><b>Limited</b> Supports advanced routing protocols like BGP but lacks advanced routing support for protocols such as OSPF.</p>	<p>Supports advanced routing protocols, including BGP and OSPF.</p>	<p><b>Limited</b> Supports advanced routing protocols, such as BGP, but lacks support for protocols such as OSPF.</p>	<p>Supports advanced routing protocols, including BGP and OSPF, but does not provide the most efficient path selection.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Extensible Policy Framework</b>	<p>Dynamic path selection automatically steers critical applications around network problems. Microsegmentation and identity-based policy management drive consistent multidomain policy enforcement for a uniform user experience.</p>	<p><b>Limited</b> Policy could be passed in the form of per-device profiles but would be limited in terms of traffic engineering for data plane.</p>	<p>Policies for SD-WAN and firewall are managed separately, creating complexities in terms of traffic engineering and passing down centralized control and data plane policies.</p>	<p><b>Limited</b> Policies can be created and reused from business intent perspective, but limitations exist in microsegmentation and multidomain policy enforcement.</p>	<p><b>Limited</b> Has the ability to traffic-engineer based on application-aware policy, but limitations exist in multidomain policy enforcement.</p>	<p><b>Limited</b> Has the ability to traffic-engineer based on application-aware policy, but limitations exist in microsegmentation capabilities and multidomain policy enforcement.</p>	<p>Has the ability to traffic-engineer based on routing attributes, security policy, and application policy, but limitations exist in multidomain policy enforcement.</p>
<b>Complete SD-WAN/ SASE Integration</b>	<p>Automated registration and creation for IPsec tunnels to Umbrella Secure Internet Gateway (SIG) with guided workflows on vManage. Complete integration with Cisco AnyConnect, Cisco Duo, etc.</p>	<p><b>Limited</b> Workflows to SIG vendors with native SIG offering still a work in progress.</p>	<p>No guided workflows for SIG integrations.</p>	<p>No support for autoregistration or creation of IPsec tunnels for SASE, because they rely on third-party integrations.</p>	<p>Support for complete SASE integration.</p>	<p><b>Limited</b> Support for complete SASE integration with Prisma SD-WAN and Prisma Access. Complexities in API-based CloudBlades integration. No guided workflows for SIG integration.</p>	<p><b>Limited</b> Support for complete SASE integration with SD-WAN-enabled PAN-OS NGFW and Prisma Access. No guided workflows for SIG integration.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>WAN optimization</b>	<p>Provides WAN optimization services including TCP optimization, data redundancy elimination, FEC, and packet duplication.</p>	<p><b>Limited</b> Provides limited WAN optimization services, including FEC.</p>	<p><b>Limited</b> Provides limited WAN optimization services, including FEC.</p>	<p>Provides WAN optimization services including TCP optimization, data redundancy elimination, and FEC.</p>	<p><b>Limited</b> Provides limited WAN optimization services, including FEC.</p>	<p>Does not provide WAN optimization services.</p>	<p><b>Limited</b> Provides limited WAN optimization services, including TCP optimization, packet duplication, and FEC.</p>
<b>Security</b>							
<b>Remote Office Branch Office On-prem security services</b>	<p>Fully integrated UTM security capabilities in vManage, including enterprise firewall with application awareness, Snort IPS, URL filtering, AMP File Analysis, threat grid sandboxing, Cisco Umbrella DNS security, SSL and Talos threat intelligence.</p>	<p><b>Limited</b> Basic stateful firewall.</p>	<p>Integrated NGFW features with IPS/IDS/ ApplicationControl/ AMP capabilities.</p>	<p>Lacks security integrations in the SD-WAN console.</p>	<p>Integrated NGFW features with IPS/IDS/ ApplicationControl/ AMP capabilities.</p>	<p><b>Limited</b> Only offers basic zone-based firewall. No integrated security features such as IPS/IDS/AMP/URL filtering.</p>	<p>Integrated NGFW features with IPS/IDS/application control/AMP/ URL filtering/ DNS Security capabilities. Requires additional licensing.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Custom Silicon</b>	<p>Custom silicon root of trust in hardware provides embedded defense against foundational attacks and back doors. The Cisco vEdge Routers have a factory-installed Trusted Platform Module (TPM) chip with a signed certificate. This built-in security helps ensure automated, foolproof authentication of any new Cisco vEdge Routers joining the network and is a major advantage when deploying tens of thousands of endpoints.</p>	<p><b>Limited</b> Commercial off-the-shelf hardware with embedded defense unknown.</p>	<p><b>Limited</b> Custom silicon with embedded defense unknown.</p>	<p>Commercial off-the-shelf hardware with trustworthy solution unknown.</p>	<p>Commercial off-the-shelf hardware with trustworthy solution unknown.</p>	<p>Commercial off-the-shelf hardware with trustworthy solution unknown.</p>	<p>Commercial off-the-shelf hardware with trustworthy solution unknown.</p>
<b>Segmentation</b>	<p>Proven, scalable MPLS/VRF-like end-to-end segmentation with support for multi-segment topologies and multi-tenancy support.</p>	<p><b>Limited</b> VRF-based segmentation supported with no dynamic and flexible multi-segment topologies creation.</p>	<p><b>Limited</b> Limited segmentation capabilities with complex VDOMs configurations with no dynamic and flexible multi-segment topologies creation.</p>	<p><b>Limited</b> VRF-style segmentation, but with routing limitations in OSPF and Peer Priority.</p>	<p>Proven, scalable MPLS/VRF-like segmentation from Layer 2 to Layer 7.</p>	<p><b>Limited</b> Limited segmentation capabilities.</p>	<p><b>Limited</b> Provides scalable VRF-like segmentation but no flexible multi-segment topologies creation.</p>
















	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Encrypted traffic analysis</b>	<p>Can detect malware by matching encrypted SHA patterns without decryption.</p>	<p>Cannot detect encrypted malware.</p>	<p><b>Limited</b> Not a robust ETA solution across network infrastructure/ devices.</p>	<p>Cannot detect encrypted malware.</p>	<p>Provides TLS/SSL traffic encryption.</p>	<p>Cannot detect encrypted malware.</p>	<p>Can detect malware by decrypting, inspecting, and controlling inbound and outbound SSL and SSH connections.</p>
<b>Threat intelligence</b>	<p>Globally recognized threat intelligence (TALOS) with the ability to deploy incident response services.</p>	<p>No threat intelligence.</p>	<p>Provides threat intelligence capabilities.</p>	<p>No threat intelligence.</p>	<p>Provides threat intelligence and monitoring.</p>	<p>No threat intelligence.</p>	<p>Provides threat intelligence capabilities as an add-on.</p>
<b>Cloud</b>							
<b>SaaS Connectivity</b>	<p>Transport independence provides intelligent path selection to leading SaaS applications based on performance metrics and best path selection, such as Office 365, SIG, load-balancing, Cisco Webex, etc.</p>	<p><b>Limited</b> SaaS optimization based on manual application rule creation through DIA broadband paths to colocations.</p>	<p><b>Limited</b> Basic SaaS optimization with manual SLA creation for every application.</p>	<p>Transport independence provides intelligent path selection to leading SaaS applications based on performance metrics and best path selection.</p>	<p><b>Limited</b> Basic SaaS optimization with manual SLA creation for every application.</p>	<p><b>Limited</b> Basic SaaS optimization with manual application rule creation for every application.</p>	<p><b>Limited</b> Basic SaaS optimization with manual SLA creation for every application. Needs additional SaaS security platform for advanced SaaS optimization.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>IaaS Connectivity</b>	 <p>Guided workflows for automated deployment of Cisco SD-WAN Cloud OnRamp for IaaS connectivity.</p>	 <p><b>Limited</b> Either manual gateways or shared resources. Automation only with Microsoft Azure vWAN.</p>	 <p>Manual gateway configuration.</p>	 <p><b>Limited</b> Either manual gateways or shared resources.</p>	 <p><b>Limited</b> Either manual gateways or shared resources.</p>	 <p><b>Limited</b> Manual gateways, shared resources, or complex API integration through CloudBlades.</p>	 <p><b>Limited</b> Either manual gateways or shared resources.</p>
<b>Colocation-cloud gateways</b>	 <p>Simplified network management with traffic aggregation through colocation hubs to cloud workloads, with guided workflows for automated deployment.</p>	 <p><b>Limited</b> Limited collocated aggregation.</p>	 <p><b>Limited</b> Limited collocated aggregation.</p>	 <p><b>Limited</b> Limited collocated aggregation.</p>	 <p><b>Limited</b> Limited collocated aggregation.</p>	 <p><b>Limited</b> Limited collocated aggregation.</p>	 <p><b>Limited</b> Limited collocated aggregation.</p>
<b>Multi-Cloud connectivity</b>	 <p>Guided workflows for automated deployment across various Cloud Service Providers (CSPs), such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).</p>	 <p><b>Limited</b> Partnership with Microsoft Azure vWAN. Guided workflows.</p>	 <p>Limited workflows for multicloud connectivity.</p>	 <p><b>Limited</b> Manual deployment across various CSPs.</p>	 <p><b>Limited</b> Manual deployment across various CSPs.</p>	 <p><b>Limited</b> Manual deployment across various CSPs or through complex CloudBlades API integration.</p>	 <p><b>Limited</b> Manual deployment across various CSPs.</p>



	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Edge</b>							
<b>Storage</b>	<p>Provides IoT/OT automation with integrated branch storage and compute. Supported by Cisco Catalyst 8200 Series.</p>	<p><b>Limited</b> VNFs can be deployed on VMware SD-WAN Edge appliances.</p>	<p>No edge VNF hosting capabilities.</p>	<p>No edge VNF hosting capabilities.</p>	<p><b>Limited</b> VNFs can be deployed on Versa SD-WAN Edge appliances.</p>	<p>No edge application-hosting capabilities.</p>	<p>No edge application-hosting capabilities.</p>
<b>Multi-Cloud Visibility</b>	<p>Visibility across the internet, the cloud, and SaaS with the native integration of Cisco ThousandEyes on compatible Cisco Catalyst 8200 Series and Cisco Catalyst 8300 Series Edge Platforms.</p>	<p><b>Limited</b> No edge application-hosting capabilities. VNFs can be deployed on VMware SD-WAN Edge appliances.</p>	<p>No edge application-hosting capabilities.</p>	<p>No edge application-hosting capabilities.</p>	<p><b>Limited</b> No edge application-hosting capabilities. VNFs can be deployed on Versa SD-WAN Edge appliances.</p>	<p>Visibility across the internet, the cloud, and SaaS with the native integration of Prisma Access ADEM.</p>	<p><b>Limited</b> Needs integration with Prisma Access for visibility across the internet, the cloud, and SaaS through ADEM, which makes integration highly complex.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Voice integration</b>	<p>Cisco Catalyst 8000 Edge Platforms offer rich voice services in SD-WAN and traditional IOS XE software feature stacks. Cisco is the only SD-WAN vendor to natively integrate analog/digital IP directly into single CPE. In SD-WAN mode, the Cisco Catalyst 8300 Series also prevents internal and external outages using SRST. The series also continues to support a long list of traditional IOS XE voice use cases.</p>	<p><b>Limited</b> No edge application-hosting capabilities. VNFs can be deployed on VMware SD-WAN Edge appliances.</p>	<p>No edge application-hosting capabilities.</p>	<p>No native voice integration.</p>	<p>No native voice integration.</p>	<p>No native voice integration.</p>	<p>No native voice integration.</p>
<b>Advanced LTE Solutions</b>	<p>Advanced cellular capabilities as a transport link supported with deployment flexibility of built-in module, card or external gateway on Cisco Catalyst 8000 Series.</p>	<p>Cellular capabilities as a transport link.</p>	<p>Cellular capabilities as a transport link.</p>	<p>No significant cellular support.</p>	<p><b>Limited</b> No significant cellular support. Cellular support on limited model (CSG1000).</p>	<p><b>Limited</b> Cellular support on limited model (one ION 1200 model).</p>	<p>Supports cellular capabilities in 5G-based NGFW.</p>

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Industrial SD-WAN</b>	 Ruggedized SD-WAN options, for adverse and industrial environments.	 No ruggedized SD-WAN options.	 Ruggedized SD-WAN options.	 No ruggedized SD-WAN options.	 No ruggedized SD-WAN options.	 No ruggedized SD-WAN options.	 Ruggedized SD-WAN options.
<b>Wi-Fi/5G-ready</b>	 Uses advanced wireless frequency and protocol technology.	 Uses advanced wireless frequency and protocol technology.	 Uses advanced wireless frequency and protocol technology.	 No advanced wireless capabilities.	 Uses advanced wireless frequency and protocol technology.	 No advanced wireless capabilities. Dependence on third parties to enable features.	 No advanced wireless capabilities. Dependence on third parties to enable features. Does have 5G-ready NGFW hardware.
<b>Data center integration (Common policies across domains)</b>	 Cross-domain integrations, common QoS policies between Cisco ACI and SD-WAN. Extend TrustSec Security Group Tags (SGTs)/ metadata from WAN to campus to data center.	 Unifies data center policies with edge needs.	 No data center integration.	 No data center integration.	 No data center integration.	 No cross-domain integration.	 No cross-domain integration.

	Cisco	VMware	Fortinet	Silver Peak	Versa	Palo Alto Networks (Prisma SD-WAN)	Palo Alto Networks (PAN-OS NGFW)
<b>Microsegmentation</b>	 <p>Supports microsegmentation and policy enforcement through scalable group tags for user groups.</p>	 <p><b>Limited</b> Minimal Layer 2 microsegmentation and policy enforcement.</p>	 <p><b>Limited</b> Minimal Layer 2 microsegmentation and policy enforcement.</p>	 <p>Supports microsegmentation and policy enforcement through scalable zones.</p>	 <p>Supports microsegmentation and policy enforcement through scalable zones.</p>	 <p>No microsegmentation and policy enforcement.</p>	 <p>Supports microsegmentation and policy enforcement through scalable zones.</p>