citrix™

Citrix SD-WAN Data Sheet

Secure and optimize the workspace experience in the cloud

Solution overview

Citrix SD-WAN delivers the reliable, high-performance user experience to your distributed workforce needs to do their best work anywhere. With Citrix SD-WAN, you can simplify your hybrid multi-cloud initiatives by optimizing applications and automating connectivity. Easily deploy robust security capabilities where you need them. And choose from the broadest choice in security with a unified security service and integration with third-party best-of-breed firewalls.

A single cloud-based user interface makes it simple to manage your WAN, configure security policies, and monitor and prioritize applications. Citrix SD-WAN gives you the most flexibility with a range of physical and virtual form factors, you can deploy SD-WAN in public clouds, data centers, branches and home offices.

Citrix SD-WAN is a core capability of the Citrix unified approach to SASE (secure access service edge) along with zero-trust network access and cloud-delivered security for secure, reliable access to all applications anywhere from any device.

Citrix SD-WAN components

The Citrix SD-WAN solution consists of three main components:

- Cloud-hosted (or on-premises) orchestrator for centralized policy management and visibility
- Physical, virtual, branch, home and data center appliances
- Two software editions

SASE and Citrix SD-WAN overlay architecture
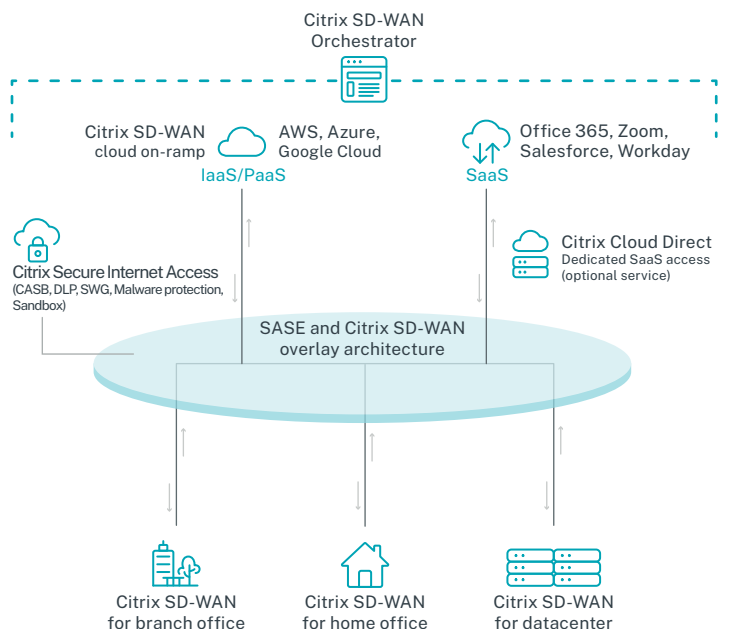
Citrix SD-WAN Orchestrator

Citrix SD-WAN Orchestrator is a cloud-hosted (or on-premises), multi-tenant management service available to Do-It-Yourself enterprises and Citrix partners. The Citrix SD-WAN Orchestrator Network dashboard (Figure 1) provides a bird's-eye view of an organization's SD-WAN network in terms of health and usage across all the sites. The dashboard captures a summary of the network-wide alerts, uptime of the overlay and underlay paths, highlights usage trends, and provides a global view of the network.

Application-centric policies: Application based traffic steering, Quality of Service (QoS), and Firewall policies, configurable globally or per site.

Physical and virtual form factors

The Citrix SD-WAN hardware appliances support the different Citrix SD-WAN editions, common hardware components, and virtual appliance information. The various Citrix SD-WAN hardware platforms offer a wide range of features, virtual paths, and throughput. Citrix SD-WAN software supports all Citrix SD-WAN hardware platforms.

Citrix SD-WAN VPX (virtual form factor) is available as a virtual instance in major cloud market places (Azure, AWS, GCP) and as BYOL.

Figure 1
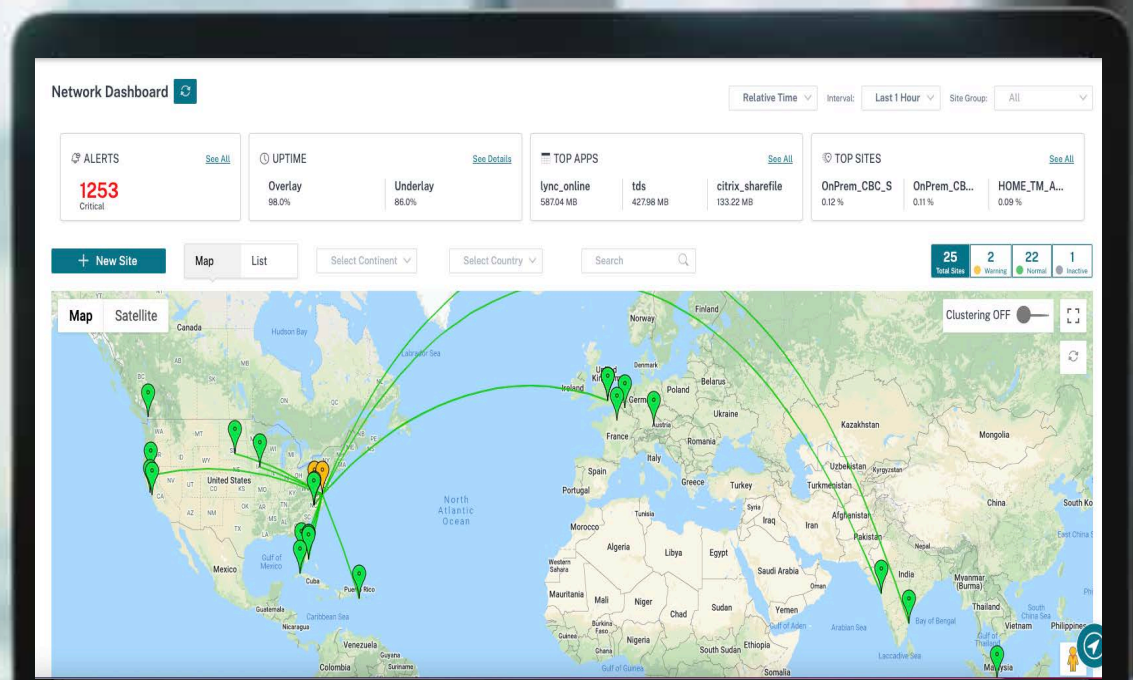
Software Editions

Citrix SD-WAN Software Editions	
Citrix SD-WAN Standard	Includes Standard Virtual WAN features only (refer to Feature table later in this document). Standard edition supports software-defined WAN capability to create a highly reliable network from multiple network links. It ensures that each application takes the best path to achieve the highest application performance.
Citrix SD-WAN Premium	Includes Standard Edition and WAN Optimization features. Premium Edition integrates WAN virtualization with WAN optimization capabilities to optimize branch and remote user experience and to achieve fully resilient applications regardless of network quality.
	Citrix Secure Internet Access and the Advanced Security add-on are additional cost.
	The Advanced Security add-on enables Edge Security features. It includes the following security capabilities: Web Filtering, Anti-Malware, Intrusion Prevention, SSL Inspection.

Citrix SD-WAN Portfolio

| 110 SE
110-WiFi SE
110-LTE-WiFi SE | 210
210-LTE | 1100 | 2100 | 4100 | 6100 |
| --- | --- | --- | --- | --- | --- |
| (20 to 200 Mbps) | (50 to 300 Mbps) | (200 to 500 Mbps) | (300 Mbps to 2 Gbps) | (2 Gbps to 3 Gbps) | (4 Gbps to 6 Gbps) |
| **Micro Branch / Home** | **Retail / Small Branch** | **Large Branch** | **Small/Medium DC** | **Data center** | **Large DC** |

Supported Virtual Appliance Platforms 20 Mbps - 1.5 Gbps (depending on platform)
ESXI | Citrix Hypervisor | Hyper-V | KVM

Azure   aws   Google Cloud

Licensing

Subscription*

Available for Standard and Premium Editions.

- Zero-capacity hardware
- Software subscription
- One or three-year terms
- Hardware maintenance
- Advanced Security add-on license
- Cloud Direct optional add-on license
- Orchestrator entitlement included and available for Standard, Advanced, and Premium editions
- CSS Select-level support included

Why Citrix SD-WAN

- Gartner #1 for Application Experience Optimization
  - Rock-Solid Experience for Citrix Apps and Desktops

- Comprehensive Security
  - All Gartner 'Core' & 'Recommended' SASE Capabilities

- Unified Cloud-Hosted Management
  - Cloud-hosted single-pane-of-glass networking & security

- Reliable, Resilient Connectivity
  - Over any type of connectivity to cloud, SaaS and virtual apps

- Consistent Hybrid Work Models
  - For execs, heavy-data users, call center reps, ad-hoc workspaces

Enhance workforce experience

Citrix SD-WAN helps connect a hybrid workforce to business applications. Home workers can leverage additional bandwidth and IT gains visibility into the entire network. Critical workers such as power users, execs and call center reps have redundancy and resiliency. Adding network redundancy greatly reduces the risk of outages as a single link, even with Service Level Agreements (SLAs), can still experience congestion and outages.

Improve real-time traffic performance for voice and video that is sensitive to congested networks, latency and jitter can stop robotic voice, audio dropouts, poor video and dropped calls. End-to-end network policy control, management and visibility reduces downtime.

Citrix SD-WAN ensures your hybrid workforce is always secure, connected, and engaged.

Simplify transition to multicloud

Citrix SD-WAN extends the network into IaaS/PaaS clouds where traditional WAN architectures were not designed for the cloud and assumed applications lived in the data center protected by a security perimeter.

Routing cloud-destined traffic through the data center's security stack increases latency and network hops and the requires more costly bandwidth to handle this additional traffic. Citrix SD-WAN provides consistent WAN administration across major clouds and speeds up site rollouts while lowering transport costs.

Accelerate journey to SASE

The shift to SaaS and cloud necessitates direct internet access as backhauling is inefficient and results in a degraded user experience. Network and security integration at the edge protects the user experience while preventing threats from entering through the network. Citrix SD-WAN along with Citrix Secure Internet Access secures direct internet access at the branch and remote user to threats from an increased attack surface. Citrix SD-WAN Orchestrator integrates management of Citrix SD-WAN and security as a cloud-delivered service allowing users to truly work from anywhere. The unified approach is built on a global cloud architecture.

Perpetual licensing also available upon request.

Feature	Standard Edition	Premium Edition
Application Identification	•	•
Citrix Protocol Support	•	•
Citrix Standard (DaaS) Integration and automation	•	•
Office 365 Optimization	•	•
WAN Optimization		•
Traffic Forwarding	•	•
Maximize Bandwidth Usage	•	•
Dual-ended QoS	•	•
Congestion management (Detection, avoidance, remediation)	•	•
Packet Loss Concealment	•	•
Latency Mitigation	•	•
Selective packet duplication for real-time applications	•	•
HDX Session Fairness	•	•
Link Failover	•	•
Fail-to-Wire*	•	•
SaaS-based Orchestration	•	•
Enterprise-grade private network support for Cloud Direct (SaaS/Cloud gateway)**	210,1100	•
Multi-cloud connectivity (Azure, AWS, GCP)	•	•
Integrated LTE***	110, 210	
Malware Prevention***	•	
Web Filtering***	•	
IDP/IDS***	•	
SSL Inspection***	•	
Next-Gen Firewall as VNF	1100	
Integration with Cloud Security	•	•
Integrated 802.1x WiFi	110	
Zero Touch Provisioning	•	•

*Not available on 110 platform
**Optional Cloud Direct add-on
***On Standard Edition with Advanced Security as an add-on for the 210 and 1100 appliances only

Software Features

Category	Features	Description
Enhance Workforce Experience		
Application Identification	Deep Packet Inspection (4,500 apps) App Classification Engine	Applications can be discovered and classified in real-time. The appliance analyzes an incoming packet and classifies it as belonging to a particular application or application family.
Citrix Protocol Extensions	AutoQoS for ICA Site, session, user-level HDX reporting	Granular visibility into HDX user sessions and the proprietary ICA protocol distinguishes different types of ICA traffic such as in-band audio, display remoting, multimedia redirection, and printing and can optimize such traffic using Quality of Service (QoS) controls. Auto-configures Citrix Virtual Apps and Desktops for optimal integration, whether on prem or in the cloud.
Citrix Standard (DaaS) Integration and automation	Automated workflow	Automated provisioning of SD-WAN on IaaS platform within Citrix Virtual Apps and Desktops Standard Edition/DaaS admin workflow.
Office 365 Optimization	API integration Beacon service	API integration and use of Office 365 connectivity principles to optimize how traffic is sent to Microsoft front doors. Office 365 optimization steers trusted SaaS traffic such as Office 365 Teams audio-video directly to the cloud, either to the Citrix Cloud Direct service for enhanced reliability and performance or directly to the closest Office 365 front door, while untrusted traffic can be steered to a data center security stack or cloud-based SW (Secure Web Gateway) for enforcement.
WAN Optimization	TCP Optimization Compression De-duplication and Caching	Improves the application experience while reducing bandwidth expenses. De-duplication and caching reduce traffic across the WAN. Compression reduces band width consumption and increases data throughput.TCP optimization reduces overhead.
Traffic Forwarding	Packet-based traffic forwarding	Data is delivered on a per packet basis. Packet-based forwarding reorders packets to mitigate changing WAN conditions in order to best steer traffic.
Maximize Bandwidth Usage	Virtual WAN	Maximize bandwidth usage (even for a single TCP session over 2 or more WAN links). To ensure high application performance for bandwidth intensive applications such as backups and large file transfers, multiple links are used simultaneously for a single session. If the bandwidth required for one session exceeds the available bandwidth on the best link, all the available bandwidth on the best link will be bonded with the second-best quality link.This lets high bandwidth applications have as much bandwidth as they need to perform optimally.
Dual-ended QoS	Dual-ended QoS	Dual-ended QoS measures latency, packet loss and jitter at both the sending end and destination. Administrators configure QoS globally from a single source and senders only send at the peers advertised receive rate. Unidirectional local measurements are shared with peer devices in the network. All sites get their fair share of bandwidth preventing oversubscription and wasted utilization.

Category	Features	Description
Congestion Management	QoS (Detection, avoidance, remediation)	A fourth measurement of QoS is congestion. Tunnels between appliances allow for proactive management of the traffic. The sending appliance tags each packet with information about the time sent and its order in the packet. The receiving appliance reads these tags and uses the data to measure transit time, congestion, jitter, packet loss, and other information about the performance and health of the path in each direction. The appliances share this information with the controller, which uses queuing theory and predictive behavioral statistical modeling to create a "map" of all of the paths in the WAN. The map is continuously updated with information from recent packets.
Software Features		
Packet Loss Concealment	QoS Packet Duplication TCP Optimization	Selective Acknowledgment (SACK) is a strategy which corrects this behavior in the face of multiple dropped segments. With selective acknowledgments, the data receiver can inform the sender about all segments that have arrived successfully, so the sender need retransmit only the segments that have actually been lost. Note: Can be applied to UDP flows/data.
Latency Mitigation	DPI DIA Intelligent path selection	Intelligent detection of the most optimal low-latency routes is achieved by creating a VPN overlay. Additionally, extending the network to the cloud with automated on-ramps and direct breakout removes the need to backhaul that traffic reducing the distance it has to travel.
Selective Packet Duplication	Packet Duplication	Packet duplication, or racing, ensures high application performance for real-time applications such as voice by duplicating a session's traffic across multiple paths. This means that no packets are lost and, as the first of the duplicate pair to arrive is used, each packet takes the lowest latency route. This allows for optimal application performance for just a small cost in bandwidth. It is ideal for improving media quality with softphones and Unified Communications apps. From an HDX perspective, a softphone/UC app can be "optimized" (the media engine runs on the user device, offloading the Citrix server) or "unoptimized" (media is processed on the Citrix server and delivered over ICA). Packet racing can be used in either case.
HDX Session Fairness	HDX Session Fairness	Session fairness ensures that no single HDX user consumes morethan a fair share of the available network bandwidth. Users continue to enjoy a responsive, interactive experience even when someone in the same office is transferring a huge file or printing a large graphics-intensive document.
Link Failover	Link Failover	SD-WAN will initially select the best path for each type of application based on an algorithm that takes in to account latency, loss, jitter, and congestion. If a network path starts to degrade or fail, traffic will be moved off of that path before it impacts the application and without the user noticing. The criteria for determining that a path is going bad is again an algorithm that takes in to account several factors in relation to all other possible paths. It's not using a fixed threshold for latency and loss.This technology means that you can create a reliable network from broadband links and wireless and satellite links, which can have variable performance and a higher risk of out age than a private network such as MPLS.

Category	Features	Description
Fail-to-Wire (FTW) Functionality	Fail-to-Wire (FTW)	Ethernet bypass for inline mode that allows traffic to bypass SD-WAN and flow directly across a pair of bridged interfaces in the event of appliance restart or failure.
Cellular	USB and dongle LTE	Gives networks fast performance and reliability. It's certified for operation on Verizon's, AT&T's and T-Mobile's 4G/LTE network along with a host of others.

Category	Features	Description
Simplify Transition to Multicloud		
SaaS-based Orchestration	SD-WAN Orchestrator	Centralized management and monitoring delivered as a SaaS solution as part of Citrix Cloud with visibility into users, permissions, applications, and WAN links across the entire network.
Automated Service/Connection Provisioning	API Integration with 3rd-party security vendors	API integration with 3rd-party security partners enables fast, simple cloud security setup. Through API automation, you can secure the connectivity (via IPsec) from the branch to the Palo Alto Prisma Cloud, Zscaler and Check Point Harmony. The benefits of automation become more significant as more branch sites are involved, directly translating into time savings and reduction in configuration errors. This is suited for organizations with a significant number of remote workers for which policy consistency between office and remote users is critical.
SaaS / Cloud gateway	Cloud Direct	Cloud-based gateways with close proximity to major SaaS, IaaS, and PaaS cloud locations. Customers generally connect their branches to such gateways for improved reliability, greater visibility, reduced latency, and improved performance for applications.
Enterprise-grade Private Network support (SaaS/ Cloud gateway)	Cloud Direct	Provides optimized high-performance connections from the local last mile networks to a network of geographically distributed PoPs that peer with SaaS clouds via dedicated paths.
Multicloud Connectivity	VPX	By deploying a VPX in an IaaS cloud with an SD-WAN appliance on-prem, customers get link bonding, packet-based real-time path selection, and resiliency in case of congestion, loss and link "brownouts" with no interruption of user experience. It improves application availability, modernizes the WAN for the cloud, provides real-time monitoring and insights, leveraging a massive global footprint and native access to a broad and deep set of traditional and emerging IT resources.
Mobility	802.1x WiFi	2X2 MIMO with embedded antenna Dual Band - Single Configure Active Band w/ 802.1X Authentication802.11 a/b/g/n/ac with max 4 SSIDs (typical 25 users/devices w/ guest support)
Configuration	Zero Touch Deployment	Citrix operated and managed cloud-based service which allows discovery of new appliances in the Citrix SD-WAN network, primarily focused on streamlining the deployment process for Citrix SD-WAN at branch or cloud service office locations.

Category	Features	Description
Journey to SASE		
Built-in Layer 4 Stateful Firewall	Built-in Layer 4 Stateful Firewall	Integrated branch firewall that provides visibility and control of the traffic that is either going directly to the internet or getting backhauled to the head-end. The network is segmented into multiple firewall zones to control the traffic between them. It uses the deep packet inspection to identify the type of application and apply the configured firewall policy to its traffic. This integration of firewall on the branch appliance helps reduce the unnecessary traffic getting backhauled and wasting valuable WAN resources only to be blocked at the head-end.
Malware Prevention	Antivirus support on branch appliance (Integrated/Native)	It scans within archives such as zip, rar, tar, gzip, bzip2 (and more). Scans downloads using many technologies such as query thread intelligence database using metadata of file, local scans using Bitdefender's signature database.
Next-Gen Security	Web Filtering support on branch appliance (Integrated/Native)	Web Filtering helps administrators ensure web and content security across the branch network. Ensures users are not abusing network use policies providing the largest URL database of its kind across 79 categories, including high-risk categories. 750+ million domains and 32+ billion URLs classified across 45+ languages.
Next-Gen Security	IDS/IPS	Intrusion Prevention is an Intrusion Detection System (IDS) detecting malicious activity on network using 26,000+ signatures in the database.
Next-Gen Security	SSL inspection	Provides ability to analyze encrypted traffic, identify threats or handle policy violations. Performs man-in-the-middle decryption SSL traffic, analyze the data as it passes through such as to allow Web Filtering to block/lag sites, and re-encryption of SSL traffic.
Next-Gen Firewall	Next-gen Firewalls VNF	For customers who require a strong perimeter security and compliance with stringent healthcare or financial regulations, Citrix offers the SDN/ NFV ready platform capable of hosting several industry-leading next-generation virtual firewalls. As a start, the combination of SD- WAN 1100 with Palo Alto VM-Series and Check Point Quantum Edge have been optimized to deliver high performance of App-ID enabled firewall in a compact footprint.

Standard Edition Appliances

Model[8]	6100	4100	2100	1100	210	110	VPX	VPX-L
Total Encrypted Throughput[1] (License Term 1 or 3 Yr)	8 Gbps to 12 Gbps (4 Gbps to 6 Gbps)	4 Gbps to 6 Gbps (2 Gbps to 3 Gbps)	600 Mbps to 4 Gbps (300 Mbps to 2 Gbps)	400 Mbps to 1Gbps (200 Mbps to 500 Mbps)	100 Mbps to 600 Mbps (50 Mbps to 300 Mbps)	40 Mbps to 400 Mbps (20 Mbps to 200 Mbps)	40 Mbps to 3 Gbps (20 Mbps to 1.5 Gbps)	40 Mbps to 3 Gbps (20 Mbps to 1.5 Gbps)
Max Virtual Paths (Static/Dynamic)	1000/32	550/32	256/32	64/32	16/4	8/4	16 (8 for 20 Mbps License)	256
Third-party Firewall (VNF)[2]				Palo Alto Next Gen Firewall or Check Point Firewall				
Citrix Cloud Direct				100 Mbps	10 Mbps to 20 Mbps			

Advanced Security Capable Appliances - Branch Security (support is only for branches, not for MCN)

Model [8]	1100	410	210
Total Encrypted Throughput[1] (License Term 1 or 3 Yr)	400 Mbps or 600 Mbps or 1 Gbps (200 Mbps or 300 Mbps or 500 Mbps)	100 Mbps (Model: 410-050-AE) 200 Mbps (Model: 410-100-AE) 400 Mbps (Model: 410-200-AE) 600 Mbps (Model: 410-300-AE)	40 Mbps or 100 Mbps (20 Mbps or 50 Mbps)
Max Virtual Paths (Static/Dynamic)	64/32	24/8	16/4
Max Virtual Path Throughput with Edge Security	300Mbps (200 Mbps License) 400 Mbps (300 Mbps License) 600 Mbps (500 Mbps License)	150 Mbps	40 Mbps (20 Mbps License) 60 Mbps (50 Mbps License)
Edge Security[5] Throughput	50 Mbps (200 Mbps License) 100 Mbps (300 Mbps License) 200 Mbps (500 Mbps License)	50 Mbps	20 Mbps
IPS Throughput[6]	50 Mbps (200 Mbps License) 100 Mbps (300 Mbps License) 200 Mbps (500 Mbps License)	50 Mbps	20 Mbps
NGFW Throughput[7, 9]	50 Mbps (200 Mbps License) 100 Mbps (300 Mbps or 500 Mbps License)	50 Mbps	20 Mbps
Concurrent Sessions	30,000	7,100	4,400

Premium Edition Appliances

Model	6100	2100	1100
Total Encrypted Throughput[1] (License Term 1 or 3 Yr)	6 Gbps or 8 Gbps (3 Gbps or 4 Gbps)	600 Mbps or 1 Gbps or 2 Gbps (300 Mbps or 500 Mbps or 1 Gbps)	400 Mbps or 600 Mbps or 1 Gbps (200 Mbps or 300 Mbps or 500 Mbps)
Max Virtual Paths (Static/Dynamic)	1000/32	256/32	64/32
Optimized Application Capacity[10, 19]	500 Mbps	50 Mbps (300 Mbps License) 100 Mbps (Other Licenses)	10 Mbps (200 Mbps License) 20 MBps (300 Mbps License) 50 Mbps (500 Mbps License)
Max HDX CCUs[11]	750	300	100 (200 Mbps License) or 300 (Other Licenses)
Max Accelerated TCP Sessions[12]	60,000	20,000	10,000

VPX WANOP Appliances
(Citrix Hypervisor 5.5-6.5, Microsoft Hyper-V 2012 R2 or higher, ESX/ESXi 4.1-6.5)

Model [1,10] Optimized WAN Capacity	VPX 2-WO 2 Mbps	VPX 6-WO 6 Mbps	VPX 10-WO 10 Mbps	VPX 20-WO 20 Mbps	VPX 50-WO 50 Mbps	VPX 100-WO 100 Mbps	VPX 200-WO 200 Mbps
QoS/Unaccelerate Throughput Limit	15 Mbps	50 Mbps	75 Mbps	150 Mbps	250 Mbps		300 Mbps
Max HDX CCUs[11] (Concurrent SD-WAN Client Plug-Ins)	20	60	100				
Max Accelerated TCP Sessions[12]	5,000			10,000		20,000	30,000
Video Caching and Networking Cloud Connector[13]	-	-	-	-	-	-	-
Memory Hard Drive[15]	6 GB 100 GB			6 GB 250 GB		8 GB 500 GB	16 GB 500 GB
Virtual CPU	1X Citrix Hypervisor & 2X VMware vSphere (> 2.33 GHz)			2-4X Citrix Hypervisor, Microsoft Hyper-V & VMware vSphere (> 2.33 GHz)			2-4X Citrix Hypervisor, Microsfot Hyper-V & VMware vSphere (~3.0 GHz)

Standard Edition Virtual and Cloud Appliances
(Citrix Hypervisor 6.5 SP1, Microsoft Hyper-V 2012 R2 or higher, ESX/ESXi 5.5, 6.0, 6.5, 6.7, Linux KVM Ubuntu 16.04)

Model	VPX-20 / VPX-L-20	VPX-50 / VPX-L-50	VPX-100 / VPX-L-100	VPX-200 / VPX-L-200	VPX-500 / VPX-L-500	VPX-1000 / VPX-L-1000	VPX-1500 / VPX-L-1500
Total Encrypted Throughput[1] (License Term 1 or 3 Yr)	40 Mbps (20 Mbps)	100 Mbps (50 Mbps)	200 Mbps (100 Mbps)	400 Mbps (200 Mbps)	1 Gbps (500 Mbps)	2 Gbps (1 Gbps)	3 Gbps (1.5 Gbps) (on Azure)
Max Virtual Paths Static / Dynamic VPX	16 / 4	16 / 4	16 / 4	16 / 4	16 / 4	16 / 4	16 / 4
Max Virtual Paths Static / Dynamic VPX-L	256 / 32	256 / 32	256 / 32	256 / 32	256 / 32	256 / 32	256 / 32
Hypervisor Support							
Processor		Dual Core Intel VTx2 for VPX				Quad Core Intel VTx2 for VPX	
Virtual CPU		2vCPU @ 2.7 GHz / 16vCPU @ 2.7 GHz		4vCPU @ 2.7 GHz / 16vCPU @ 2.7 GHz		8vCPU @ 3.0 GHz / 16vCPU @ 2.7 GHz	8vCPU @ 2.7 GHz 16vCPU @ 2.7 GHz
Memory VPX	4 GB	4 GB	4 GB	8 GB			
Memory VPX-L	16 GB	16 GB	16 GB	16 GB			
Cloud Support[3]							
AWS — VPX		c3.xlarge				-	-
AWS — VPX-L		m4.4xlarge					
Azure[4] — VPX		D3_v2 / F16					
Azure[4] — VPX-L		F8					
GCP — VPX		N1-standard-4			-	-	-
GCP — VPX-L		N1-standard-16					

Storage		
	MCN/RCN	Branch
Virtual Path Count <128 paths	120 GB	40 GB
Virtual Path Count >128 paths	240 GB	120 GB

Hardware Specifications

Model	6100 SE/PE	4100 SE	2100 SE/PE	1100 SE/PE	210 SE	210 LTE SE (R1/R2/RC)	110 SE	110 Wi-Fi SE	110 LTE Wi-Fi SE
Total Disk Space[16]	480 GB (SSD)	2 TB (SSD)	720 GB (SSD)	480 GB (SSD)	64 GB (mSATA)		64 GB (mSATA)	32 GB (mSATA)	
Compression History (SSD)	SE: NA PE: 960 GB	SE: NA PE: 2.8 TB	SE: NA PE: 480 GB	SE: NA PE: 148GB	NA	NA	NA	NA	NA
RAM	256 GB	128 GB	32 GB	24GB	4 GB				
Network Interfaces									
Fail-to-wire	4X10 GbE-SR 4X1 GbE-TX	2X10 GbE-SR 4X1 GbE-TX	4X 1 GbE-TX	4X 10/100/1000-TX	1X 10/100/1000-TX		NA	NA	NA
Non Fail-to-wire	4X 10 GbE SFP+		4X 1 GbE-SFP	2X 10/100/1000-TX 2X Flexible Combo Ports (SFP or 10/100/1000-TX 2X POE)	1X 10/100/1000-TX 2X Flexible Combo Ports (SFP or 10/100/1000-TX)			3X 10/100/1000-TX	
Management	2X 1 GbE-TX		1X 1 GbE-TX		1X 10/100/1000-TX				
WAN Interface[18]									
Integrated LTE	NA	NA	NA	NA		Integrated CAT6 LTE Advanced (Dual CA) Modem (300 Mbps DL / 50 Mbps UL) - 3 Region Variants (include antennae)	NA	NA	Integrated CAT4 LTE Global Modem (150 Mbps DL / 50 Mbps UL) (include antennae)
LTE SIM Management	NA	NA	NA	NA		Single SIM (Primary with auto or manual APN)	NA	NA	Dual SIM (Primary and failover with auto or manual APN)

Model	6100 SE/PE	4100 SE	2100 SE/PE	1100 SE/PE	210 SE	210 LTE SE (R1/R2/RC)	110 SE	110 Wi-Fi SE	110 LTE Wi-Fi SE
WLAN Interface[17]									
Integrated Wi-Fi	NA	NA	NA	NA	NA	NA	NA	2X2 MIMO with embedded antenna Dual Band Single Configure Active Band	
Wi-Fi Standards	NA	NA	NA	NA	NA	NA	NA	802.11 a/b/g/n/ac	
Frequency Range	NA	NA	NA	NA	NA	NA	NA	2.4GHz: 2.412 ~ 2.472 GHz 5GHz: 5.180 ~ 5.825 GHz	
Max Simultaneous SSIDs	NA	NA	NA	NA	NA	NA	NA	4	
Geography Region Domain	NA	NA	NA	NA	NA	NA	NA	US or Canada / Rest of World (ROW)	
Max Output Power	NA	NA	NA	NA	NA	NA	NA	20 dBm	
Mechanical									
Rack Units	2RU (3.5in/ 8.9cm)	2RU (3.5in/ 8.9cm)				1RU (1.75 in/ 4.45 cm)			
Rack Options					EIA 310-D, IEC 60297, DIN 41494 SC48D rack width with mounting brackets			Shelf	
System Depth	28 in/72 cm	28 in/72 cm	24 in/ 63.5 cm	9.9 in/ 25 cm	6.9 in/ 17.53 cm	6.9 in/ 17.53 cm	8.5" L X 6.25" W X 1.5" H 2.16 X 15.88 X 3.81 cm	8.5" L X 6.25" W X 1.5" H 2.16 X 15.88 X 3.81 cm	8.5" L X 6.25" W X 1.5" H 2.16 X 15.88 X 3.81 cm
System Weight	60 lbs/ 27.2 kg		26 lbs/ 11.8 kg	4.5 lbs/ 2.04 kg	2.9 lbs/ 1.35 kg	2.9 lbs/ 1.35 kg	1.37lbs/ 0.62 kg	1.45lbs/ 0.69 kg	1.6lbs/ 0.78 kg
Shipping Dimensions	36.5" X 24.5" X 11"		32" X 23.5" X 7.5" (81.5 x 59.7 X 19.1 cm)	13.66" X 12.75" X 7.48" (34.69 X 32.38 X 18.99 cm)	17.5" X 12" X 2.75" (44.5 X 30.5 X 7.0 cm)	17.5" X 12" X 2.75" (44.5 X 30.5 X 7.0 cm)		15.16" L X 10" W X 3.55" H (38.51 X 25.4 X 9.02 cm)	
Shipping Weight	69 lbs/ 31.3 kg		40 lbs/ 18.1 kg	7.5 lbs/ 3.4 kg	4.6 lbs/ 2.09 kg	5.0 lbs/ 2.27 kg	2 lbs/ .91 kg	2.2 lbs/ .95 kg	2.5 lbs/ .98 kg

Model	6100 SE/PE	4100 SE	2100 SE/PE	1100 SE/PE	210 SE	210 LTE SE (R1/R2/RC)	110 SE	110 Wi-Fi SE	110 LTE Wi-Fi SE
Power, Environmental, and Regulatory									
Power Supplies	Dual Redundant, Hot Swappable		Single (Optional Dual Redundant)		Single				
Wattage (Max)	1000W	1000W	450W	96.8W	45W	45W	24W	24W	24W
Input Voltages, Frequency Ranges	100-240 VAC, 47-63 Hz	100-240 VAC, 47-63 Hz	3.4-1.7A	2A	100-240 VAC, 47-63 Hz	100-240 VAC, 47-63 Hz	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz
Input Current	5.5- 2.8 A	7.0- 3.5 A	5.5- 2.8 A	9.0- 4.5 A	4.0-2.1A	4.0-2.1A	2.0A	2.0A	2.0A
Operating Temperature	32-114°F (0-45°C)	32-104°F (0-40°C)							
Operating Altitude				0-16,000 ft (0-5,000 M)					
Storage Temperature	14-140°F (-10-60°C)	14-140°F (-10-60°C)	14-140°F (-10-60°C)	-4-140°F (-20-60°C)	14-140°F (-10-60°C)	14-140°F (-10-60°C)	14-140°F (-10-60°C)	14-140°F (-10-60°C)	14-140°F (-10-60°C)
Allowed Relative Humidity	5%-95%, Non-condensing	20%-80%, Non-condensing	20%-80%, Non-condensing	5%-95%, Non-condensing	5%-90%, Non-condensing				
Safety Certifications	CSA				UL		NA	NA	NA
Electromagnetic Emissions, Safety, and Environmental	FCC (Part 15 Class A), CCC, KCC, NOM, CITC, EAC, MoC, CE, VCCI, RCM, Anatel, BSMI, NTRA		FCC (Part 15 Class A), CCC, KCC, FCC (Part 15, Class B)	FCC (Part 15 Class A), CCC, KCC, FCC (Part 15, Class B), NOM, CITC, EAC, MoC, CE, VCCI, RCM	FCC (Part 15 Class B), CE, Anatel, BIS, BSMI, CCC, CITC, EAC, ICASA, KCC, RCM, VCCI	FCC (Part 15 Class A), CE, Anatel, BIS, BSMI, CCC, CITC, EAC, ICASA, KCC, RCM, VCCI, NAL, SSRC24	NA	NA	NA
Environmental Compliance	ROHS, WEEE				ROHS, WEEE, Reach				NA
Industry Certifications	NA	NA	NA	NA	NA	NA	NA	Wi-Fi CertifiedTM 25	GCF, PTCRB, Wi-Fi CertifiedTM 25
Regulatory Certifications	NA	NA	NA	NA	NA	Anatel, CE, CCC, ENACOM, FCC, ICASA, ISED, RCM, UL	Anatel, BTK, CE RED, CCC, ENACOM, FCC, ICASA, IFT, ISED, RCM, SRRC, UL, WPC		
Citrix Compliance Regulatory Model	2U1P1A	2U1P1B	1U1P1A	SDW-1100	SDW-210	SDW-210-LTE-R1, SDW-210-LTE-R2, and SDW-210-LTE-RC	NA	NA	NA

Footnotes

1. Total encrypted throughput refers to full duplex total amount of bandwidth that the appliance model is licensed for, both upstream and downstream, and is based on AES-128 encryption.

2. Palo Alto Networks and Check Point Next Generation Firewall (NGFW) can be hosted as VNF on Citrix SD-WAN 1100 SE.

3. Cloud server types are the minimum recommended server size to support the listed performance numbers for each model.

4. With a Citrix SD-WAN subscription and a Citrix Virtual Apps & Desktops (CVAD) Standard for Azure subscription, customers are entitled to use Citrix SD-WAN VPX in the Azure subscription hosting the CVAD workloads with no additional licensing fee if the Azure subscription is Citrix-managed.

5. Edge security throughput refers to total amount of NGFW bandwidth that the appliance model can be licensed for.

6. Total throughput measured with IPS enabled.

7. Total NGFW throughput measured with Firewall, IPS URL-Filtering, and Anti-malware enabled.

8. Advanced Security is not supported in MCN mode. Advanced Security can be availed through Advanced Edition add-ons on top of Citrix SD-WAN SE devices, on AE supported platforms (including 410 SE which is already End of Sale).

9. SSL Inspection is a compute intense operation. Enabling SSL Inspection will lead to performance degradation and latency.

10. Some protocols (ICA, for example) can limit the processing capacity of the appliance before the licensed bandwidth is reached.

11. User count is based upon a medium-level workload as defined by Login VSI and Virtual Desktops/Apps advanced encryption security. User count is limited by link bandwidth and TCP session counts. No user count is enforced. Published numbers are for guidance purposes only.

12. TCP session count will be reduced by active HDX sessions. No session count is enforced. Published numbers are for guidance purposes.

13. For Citrix SD-WAN appliances, the Citrix Networking Cloud Connector is delivered as a separate software appliance.

14. The VPX images are qualified to run on both Intel and AMD processors.

15. For best performance, use solid state drives or high IOPs storage devices.

16. Models using HDD (Hard Disk Drive) and SSD (Solid State Drive) are indicated accordingly.

17. Wi-Fi Signal strength will be impaired and Wi-Fi connection to the appliance may not even be possible. Installation onto a shelf in a metal rack is not recommended.

18. Extender cables required to remotely locate the LTE Antennas.

19. Only outbound WAN traffic is counted against the licensed bandwidth. Inbound QoS and/or unaccelerated traffic does not count against the licensed bandwidth. Total inbound optimizable traffic should not exceed this threshold.