Nitel
Managed Secure Access Services Edge Service Description

The below Service Description applies to Nitel SASE services consisting of managed SD-WAN, Secure Remote Access, and Cloud Web Security services.

Software Defined Wide Area Networking (SD-WAN)

Nitel SD-WAN is a set of intelligent software services that connect users, devices, and branch office locations reliably and securely across a diverse set of WAN transport links. The Service enables use of multiple access connections at Customer locations to maximize availability and application performance during instances of connectivity degradation and/or loss of an individual connection. Deployment of multiple access connections at a location is required for SD-WAN to prioritize and route application traffic over the best performing connection. SD-WAN utilizes strong encryption to enable secure connections between Customer locations. SD-WAN consists of Edge devices deployed at customer locations, cloud orchestration/controllers and cloud gateways. All SD-WAN services require use of an Edge device (physical or virtual) and SD-WAN Orchestration to enable the service to function. Use of SD-WAN gateways is utilized in most SD-WAN scenarios to enable cloud-hosted application overlay traffic to be appropriately prioritized. Use of SD-WAN gateways is provided on a maximum per Megabit Per Second (Mb) basis for individual customer Edge locations. Where applicable, Nitel Solution Architects work with Customer to appropriately size the overlay traffic requirements.

Secure Remote Access (SRA)

SRA is a software agent-based solution installed on end-user devices to enable secure access to corporate applications. The SRA client integrates with Nitel's global cloud-based security platform to provide secure access to applications and resources on the customer's private network. SRA licenses are required for every named user with each license supporting up to five (5) unique user devices (e.g., laptop, tablet, phone). Nitel configures Customer administrators who are then responsible for setting up additional SRA accounts and distributing secure access software to end users. Nitel reserves the right to audit the number of licenses used and bill Customer if licenses exceed the contracted end-user license count.

Cloud Web Security (CWS)

CWS is a proxy-based solution that utilizes cloud security gateways available globally to apply security policies for Software as a Service (SaaS) and internet traffic. CWS provides protection from malicious websites, viruses and customer-defined prohibited content delivered via the web. The Service leverages continuously updated threat intelligence related to new virus signatures and updates to website categorizations to help reduce attack surfaces. For protection of fixed locations, Nitel provides licensing at the Edge device level to enable the service to interoperate with the Cloud platform. In this scenario CWS services pricing is based on expected bandwidth consumption on a per Megabit basis. For protection of remote users outside of an SD-WAN location, installation of a software client is required on end-user devices to enable secure, encrypted communication, with pricing based on individual named users.

Nitel SASE Management

Nitel provides life-cycle support for all SD-WAN, CWS, and SRA deployments.

1. Nitel Design Services: Nitel Solutions Architects (SA) work with Customer technical resources to identify Customer needs and develop a design. The output of the design phase includes development of a network diagram of the solution and technical specifics (e.g. routing, VLANs, overlay applications) required to deliver service.
2. Nitel Project Management Services: The Nitel Project Manager (PM) oversees the SD-WAN, CWS, and SRA deployments including development of a project plan and tracking and communicating status. The PM coordinates with Nitel service delivery resources to facilitate delivery of access connections, delivery of SD-WAN devices and/or virtual instances, professional installation of the service and testing of the solution prior to transitioning to production. To minimize impact, Nitel strongly recommends a phased rollout for deployment for CWS and SRA. The PM helps ensure dates are met and that the service is performing as expected prior to moving to full deployment.
3. Nitel Activations and Installation for SD-WAN: SD-WAN services may utilize fee-based on-site installation by Nitel Professional Installation technicians. Customers must have resources at the installation location available on the day of installation to provide access to the Nitel technician. As part of the activation process, Nitel's technician connects networks to the SD-WAN Edge device and performs testing to verify that the service is functioning properly. Once the service meets the predefined success criteria, the service is moved into production and billing commences. Inside wiring or other field services outside of the scope of the SD-WAN installation are not included. For Customers with on-site technical resources, self-installation is available, with the Customer fulfilling the role of the Nitel Professional Installation technician. For virtual instances, Customer is responsible for providing the virtual environment that meets the technical specification provided by Nitel. Once software installation in Customer's virtual environment is completed by Customer, Nitel will configure the software to meet the mutually agreed upon technical requirements. Any issues identified specific to Customer's virtual environment are the sole responsibility of Customer to troubleshoot and resolve.
4. Nitel Activations and Installation for CWS and SRA: To enable CWS for SD-WAN locations, Nitel applies licenses to SD-WAN Edge device(s) to enable the service to function. For Customer end-user protection outside of an SD-WAN location, Nitel will provide the link to Customer administrator with download instructions for the SRA client for distribution to its end-users. Installation of SRA and CWS clients on Customer end-user devices is the sole responsibility of Customer. Upon downloading the client, Customer will receive the appropriate level of service ordered from Nitel which is visible to the Customer Administrator via a Centralized Management platform.
5. Nitel Managed Services Center (MSC): Managed Services Engineers (MSE)s are engaged throughout the activation process of delivering service to customer locations. Once transitioned to production, SD-WAN, CWS, and SRA services are managed and supported by the MSC including the MSE involved in the activation.
    a. Proactive Monitoring includes automated alert and ticket generation when service(s) become unavailable. Proactive monitoring, ticketing and support includes SD-WAN Edge devices as well as all access connections under management by Nitel. After working with Customer to confirm power and cabling are in place for impacted location, Nitel works with underlying provider to resolve issues. For access connections not under Nitel management, an outage notification will be sent to Customer for troubleshooting with the underlying provider.
    b. 24x7 support: Tier 2 support is included in the service, with Customer responsible for Tier 1 support for its end-users. Customer Administrator must open any tickets related to

end-user issues and perform the first level of triage to ensure that the problem is not related to end user device issues. Nitel may then communicate directly with the end-user if necessary to resolve issues.

   c. Software/firmware updates: Nitel manages the SD-WAN infrastructure including firmware updates to Edge devices to ensure all elements are on current Nitel supported code versions.

6. Customer Change Requests:
   a. Configuration Change Request (CCR): The process for Customer to initiate a CCR is defined as follows:
      i. Customer authorized contact opens a Nitel Ticket with a detailed written description of the desired configuration change(s)
      ii. Nitel will begin the MSC and Engineering Review (defined below) on the Customer's submitted CCR within one (1) business day.
   b. Managed Services Center and Engineering Review (ER)**:** Nitel will conduct an ER of all CCR's to ensure the following:
      i. Hardware/software meets all prerequisites.
      ii. Backups of previous version/configuration are refreshed and can support a roll-back if needed.
      iii. Change is consistent with best practices.
      iv. Change is relevant to Customer's environment.
      v. Change can be implemented in allotted timeframe.
      vi. Concerns are communicated to Customer through a previously approved channel for final authorization.
   c. Approval and Scheduling of CCRs**:** Nitel will work with Customer to address any concerns from the ER. Nitel will then determine, in coordination with the customer, the best way to implement the CCR. After scope definition, the service Intervals below will apply:
      i. Device Configuration Change (DCC) **–** consists of a CCR by Customer to make a configuration change. Our objective is to complete a DCC within 24 business hours after approval of the request.
      ii. Emergency Device Configuration Change (EDCC) **–** consists of a CCR by Customer to facilitate urgent, corrective action related to a production impacting issue or security request. Our objective is to complete an EDCC within 4 business hours after approval of the request.
      iii. Project-Oriented Request (POR) **–** consists of a CCR by Customer to make changes that are of inordinate complexity or "out of scope" and often require additional resources or sufficient time to coordinate, plan, and implement. If Customer initiates such a Project, Customer agrees to work in good faith with Nitel to develop a scope of work and implementation plan which will be documented in a Nitel Service Order Form describing the scope of the work to be performed by Nitel and the related costs.
      iv. Nitel reserves the right to bill Customer for an excessive amount of change requests at standard Nitel Professional Services hourly rates.

7. Customer Visibility and Reporting: Nitel provides Customer with access to the Orchestrator for viewing real-time and historical metrics. Customer can view performance and bandwidth consumption of network connections and applications to enable adjustments for optimizing

performance. Customer Administrator Training on the visibility and reporting platform is included in the service.

8. Co-management Capabilities: services, Nitel will provide write-access privileges to qualified Customer Administrators. Nitel will provide Customer with documentation and training on in scope service elements. Customer Administrators can make an unlimited number of policy changes. In the event a change made by Customer results in a service interruption, Customer agrees to pay Nitel for all hours incurred completing service restoration at an amount of $250 per hour.
9. Hardware Warranty and Replacement:
    a. Purchased Hardware -- Hardware purchased from Nitel includes a warranty which is the lessor of one-year or the manufacturer's published warranty at time of purchase. This warranty excludes abuse and/or force majeure events. During the warranty period, Nitel, at its sole discretion, will reasonably determine if purchased hardware is defective, requiring replacement. If Nitel determines hardware is defective within the warranty period, Nitel will ship replacement hardware as soon as reasonably possible at Customer's expense. Nitel will provide Customer with a Return Merchandise Authorization (RMA) number and return address included in the shipment of the replacement hardware. Customer shall return defective hardware within fifteen (15) business days, with RMA number being clearly visible on the outside of the packaging, to the address identified by Nitel. If Nitel does not receive returned hardware within fifteen (15) business days, Customer will be charged the then current list price for the replacement hardware. For devices that fail outside of the warranty period, Customer much purchase a replacement device from Nitel. If the exact model of equipment is not available, Nitel will provide options to Customer for selection of an equivalent device to replace the failed device.
    b. Rented Hardware -- Rented hardware is not available for locations outside of the United States and its Territories. For the duration of the service term, Nitel provides faulty hardware replacement at no cost to the customer. Nitel reserves the right to replace faulty hardware with an equivalent device which may or may not be the exact model number of the failed device. For instances where device failure is determined by Nitel, replacement equipment will be shipped Next Business Day, where available, provided failure diagnosis is completed prior to noon Central Time Zone (U.S.). Customer must return defective equipment to Nitel within fifteen (15) business days from the date of replacement hardware receipt by Customer. Customer may be billed for the then current list price for equipment not received within the fifteen (15) business days referenced above. Upon service termination, Customer must return all rented equipment to Nitel within fifteen (15) business days of the last date of service. If Nitel does not receive returned hardware within fifteen (15) business days, Customer will be charged the then current list price for the replacement hardware.
    c. Hardware Replacement within the Continental United States (Excludes Alaska, Hawaii and U.S Territories). During the contract term, Nitel will replace failed equipment during normal business hours (Monday to Friday 9 a.m. CST to 5 p.m. CST). Replacement hardware is shipped Next Business Day at no additional charge if failure diagnosis by Nitel happens by 2 pm CST.
    d. Hardware Replacement outside the Continental United States (Includes Alaska, Hawaii and U.S Territories). During the contract term, Nitel will replace failed equipment during

normal business hours (Monday to Friday 9 a.m. CST to 5 p.m. CST). Replacement hardware is shipped Next Business Day, where available, at no additional charge if failure diagnosis by Nitel happens by 11 a.m. CST. International shipments may experience delays due to customs requirements for devices. Typical replacement times will range from three (3) to five (5) business days. For this reason, High Availability Designs or Cold Spares are strongly recommended for international deployments.

e. Activations of Replacement Hardware:

   i. Customers that purchase Cold Spare equipment can contact Nitel for remote assistance in activating replacement devices 24x7x365.

   ii. Remote installation assistance is standard for replacement of faulty devices and is provided on a 24x7x365 basis. Optional on-site technician installation is available for purchase with next Business Day dispatches selected when available.

Export Restrictions

SD-WAN services may be subject to export laws and regulations, primarily around the use of encryption technologies. Customer shall not permit any end-user to access the SD-WAN service in a country subject to U.S. embargo. Customer is required to adhere to U.S. export laws and/or regulations and agrees to ensure that SD-WAN services will not be exported, directly or indirectly to any prohibited countries or use for any purposes explicitly prohibited by U.S. export laws and/or regulations.

SD-WAN Technologies – VMware

Nitel offers VMware SD-WAN technologies to deliver services. Nitel offers the following service packages available globally which are specified on Nitel Service Order Forms:

1. Nitel SD-WAN (VMware) Premium is suitable for organizations of all sizes that require optimization of SaaS applications that are not hosted within the customer’s environment.
2. Nitel SD-WAN (VMware) Enterprise is suitable for organizations of all sizes that require optimization of applications hosted locally within the customer environment, without any need for prioritization of SaaS applications.
3. Nitel SD-WAN (VMware) Standard is suitable for organizations of all sizes that do not require optimization of applications, use of multicast or full-mesh VPNs.
4. Supported Features by Service Package

FEATURE	NITEL SERVICE LEVELS		
	STANDARD	ENTERPRISE	PREMIUM
VMware SD-WAN Orchestrator Central management tool provides simplified configuration, provisioning, monitoring, fault management, logging, and reporting.	x	x	x

Diverse Multipath Priority Optimization (DMPO) Multiple WAN connections are used simultaneously in order to maximize bandwidth while ensuring application performance.	x	x	x
Direct Tunnel from Branch to Cloud Security Service	x	x	x
Dynamic Full Mesh VPN Support		x	x
Advanced Routing Open Shortest Path First (OSPF) Border Gateway Protocol (BGP)	x	x	x
Advanced Routing Multicast		x	x
Virtual Services Orchestration For next generation firewall deployments on VMware SD-WAN Edges	x	x	x
Application Optimization - Locally Hosted Services		x	x
Application Optimization - Cloud Hosted Services			x
Use of Gateways as Cloud VPN Hub			x
Upgradeable to higher edition	x	x	
Mixed Editions - ability to have more than one software subscription type within a single customer	x	x	x

<u>**CWS Technologies – VMware**</u>

Nitel offers the following service packages available globally which are specified on Nitel Service Order Forms:

a. Nitel CWS Standard includes URL filtering anti-malware and cloud usage.
b. Nitel CWS Advanced includes standard features plus data protection.
c. Supported Features by Service Package

FEATURE	**NITEL SERVICE LEVEL**	
	STANDARD	**ADVANCED**
SSL Inspection decrypts and reviews SSL-encrypted Internet communication between the client and the server to inspect payload for prohibited content, including malicious code**.**	x	x
URL Filtering restricts access to specific categories of websites and controls employee web browsing to protect users against web sites spreading malware, stealing information, or hosting inappropriate content**.**	x	x
Geographic region-based filtering allows or denies internet traffic based on the country of origin**.**	x	x
Content Filtering restricts the type of content that can be downloaded by users. Rules are application specific and can be applied to executables, files, documents, and archives.	x	x

Content Inspection (Anti-virus/malware) protection helps protect users and infrastructure from known virus and zero-day malware attacks	x	x
Basic Sandbox is an isolated environment where file behavior is inspected to help protect against Day Zero attacks contained in scripts, executable, archives and compressed packages.	x	x
Advanced Sandbox is an isolated environment where file behavior is inspected to help protect against Day Zero attacks contained in scripts, executable, archives, compressed packages, office applications, multimedia and calendar.		x
Cloud Access Security Broker (CASB) Visibility provides a view of all applications in use by the enterprise**.**	x	x
Cloud Access Security Broker (CASB) Control provides a view of all applications in use by the enterprise and provides the ability to restrict applications users access and activities they can perform within specified applications**.**		x
Data Loss Prevention (DLP) Visibility and Control inspects file uploads and text submitted to Web pages for predefined sensitive data to help prevent the transmitting of sensitive data outside of the customer perimeter.		x
SaaS Tenant Restriction identifies the list of tenants that are restricted from user access. For example, allow access to the Office 365 corporate accounts but restrict access to personal accounts.	x	x

VMware Specific Terms and Conditions

For Nitel SASE (VMware), all use of Nitel's SASE service requires acknowledgement and acceptance of the then-current underlying terms and conditions set forth in the VMware End-User License Agreement (EULA) found at https://www.vmware.com/download/eula.html.