

Secure Remote Access via SSL VPN from anywhere

Service Description

The Nova Datacom Juniper Secure Access SSL VPN implementation service provides specialized support by Certified Juniper Networks Security Engineers who have the skills and experience to help you deploy and configure a SSL VPN quickly, securely, and efficiently at your operations center. A Juniper Network Security manager can also be provided as an additional option.

The implementation service is intended for all Juniper Secure Access SSL VPNs and is delivered in five phases:

Phase 1: Pre-Qualification and Recommendations

Our certified Juniper engineer gathers the following information from your organization:

- Product requirements
- Existing physical and logical network topology review
- Deployment options: Standalone or Clustered for Redundancy /Load Balancing
- Centralized Management options
- Authentication Integration options: LDAP/Active Directory / PKI - Certificates, Smart Cards, DoD Common Access Card - CAC
- Access Method: Core, Java-SAM, Windows-SAM, Network Connect
- End point Security: Data Host check, Cache Cleaner
- Security Certification requirements: FIPS, Common Criteria

The engineer will then make recommendations about:

- Placement in network
- Access Method considerations
- Features to be used, licensing requirements and best practices recommendations
- Any special setup needed based on the applications and resources

Phase 2: Installation Planning

When you receive your customized Secure Access Juniper SSL VPN Plan, it addresses:

- Network placement and connection to surrounding network gear
- Cluster Architecture (if applicable)
- NSM (Network Security Manager) Design Architecture and integration (if applicable)
- Realm and Role design (Up to 5)
- Resource profiles and policy design (Up to 10)
- Split Tunnel configuration or Central Tunneling via Network Connect VPN tunnels to interoperable systems are completed after the initial migration.
- Endpoint Security
- Monitoring and administration (Syslog/SNMP)
- Recommendation for test plan

Phase 3: Installation

The engineer identifies the recommended Secure Access OS release for the device and begins the implementation. Activities include:

- System Configuration
- Application of License Keys

Cage: 4RLJ8
DUNS: 169242760
GSA: GS35F0322U Schedule 70

SBA-certified 8(a)
Minority Woman-Owned
SDB

- ❑ Installation of server certs and or configure Certificate Signing Request
- ❑ Importing the Trusted Certificate Authority
- ❑ Authentication Integration configuration
- ❑ Clustering configuration
- ❑ NSM Integration configuration
- ❑ Realm and Role design configuration (Up to 5)
- ❑ Configuration of Resource profiles and policy design (Up to 10)
- ❑ Java-SAM, Windows-SAM configuration
- ❑ Network Connect configuration
- ❑ Endpoint Security configuration
- ❑ Appliance monitoring and administration configuration
- ❑ Verification access and functionality
- ❑ Providing an 'As-built' configuration guide
- ❑ Providing a Flowchart of data flow
- ❑ Provide exported configuration in XML format
- ❑ The following steps may be initiated remotely and completed during the onsite visit:
 - Configure Smart Cards (FIPS model only)
 - Perform Initial Configuration (IP Addresses, DNS, Routing)
 - Load recommended Secure Access OS release onto the device
 - Assist in post-deployment monitoring while customer executes test plan

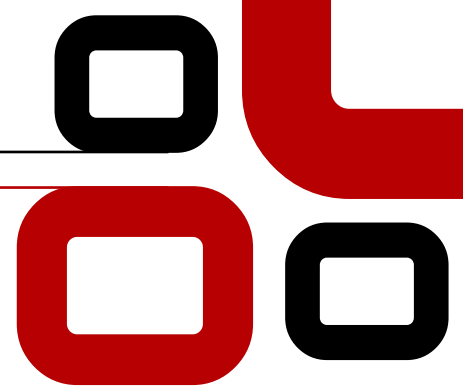
Phase 4: Knowledge Transfer

During the onsite phase, your engineer provides informal knowledge transfer and training to your technical staff. Topics covered during this information exchange may include:

- ❑ Review of Architecture and Device Configuration
- ❑ Basic troubleshooting
- ❑ Monitoring of event and access logs
- ❑ Centralized Management via NSM

Phase 5: Post-Installation Support

Once deployed, your organization receives support for 5 calendar days. During this phase, you can pose configuration-related questions to the implementation engineers by phone or e-mail. These engineers are available Monday through Friday, between 9 a.m. and 5 p.m. local time and have one business day to respond.



Nova Datacom responsibility

Provide a Certified Juniper Networks Security Engineer to:

- ❑ Help deploy and configure the SSL VPN at your Operation Center
- ❑ Provide Daily Status update
- ❑ Provide As-built configuration
- ❑ Be available for 5 days of remote post-installation support
- ❑ Be part of a designated team available for follow-up questions during normal business hours as agreed upon in SOW

Customer Responsibility

- ❑ Complete and submit pre-implementation questionnaire prior to the scheduling of Nova Datacom's onsite resource
- ❑ Provide a designated project manager or point-of-contact to interface with Nova Datacom for daily issues and coordination of resources
- ❑ Provide access to applications, databases, and in-house technical resources as required
- ❑ Provide all power and interface cabling to the equipment
- ❑ Provide network resources and connectivity
- ❑ Have a test plan for all critical applications



OPERATE
SERVICE SPECIALIST



IMPLEMENT
SERVICE SPECIALIST

Nova Datacom, LLC

4501 Singer Ct. Suite 350 Chantilly, VA 20151
www.novadatacom.com • info@novadatacom.com
Tel: 888.205.4062 • Fax: 703.234.9040

© 2011 Nova Datacom, LLC. All rights reserved. All other company and product names are trademarks of their respective owners.