SonicWall Remote Implementation Service – Secure Mobile Access 1000

The Remote Implementation Service for a SonicWall Secure Mobile Access (SMA) 1000 Series Appliance is a deployment service ("Activity") that deploys and integrates the SonicWall Secure Mobile Access (SMA) 1000 Series physical or virtual Appliance into a customer environment. This Activity is typically implemented within 20 business days after the SonicWall Advanced Services Partner receives the completed implementation planning document(s). The Activities will be limited to those stated herein.

Overview

SonicWall Remote Implementation Services are delivered by SonicWall's Advanced Services partners who have completed extensive training, certification and have demonstrated expertise in all aspects and products of SonicWall's solution platform. Upon the completion of purchase and processing, the Advanced Services partner will begin the coordination of the Remote Implementation Service within five (5) business days. Upon completion of the Remote Implementation Service, the Advanced Services partner will continue to support the configuration for thirty (30) calendar days.

Activities

The planned Activities include the following:

Pre-Deployment Steps

- Review existing network topology and configuration
- Create a valid design based on customer requirements
- Create network diagram based on proposed topology

Configuration

- Register unit and upgrade firmware
- Administrative Controls
- Cross Domain Single Sign-On (SSO)
- ActiveSync Authentication
- Secure HTTPS proxy access on the internal network
- Microsoft Outlook Web Access
- Windows SharePoint Services
- Lotus Domino Web Access
- Citrix Portal
- Two-Factor Authentication
- DNS
- Network Routes
- One Time Password for 5 devices
- End Point Control
- Domain Integration
- Network Interfaces
- System Time
- Network Objects
- Portal Settings (up to two)
- Custom Portal Logo
- URL-Based Aliasing Server Settings
- Remote Desktop Web Access Server Settings
- Security Settings
- Identity providers authentication method
- Services to be configured for each Services Objective
  1. Realm configured
  2. Communities configured
     - Employees
     - Partners
  3. Access Methods configured per Community
     - OnDemand
     - Web Proxy Agent
     - Translated Web
  4. Zones configured per Access Method
     - Trusted
     - Untrusted
     - Quarantined

Installation

- Work with customer over the phone to complete the physical or virtual installation
- Assist with client software on up to three (3) supported devices
- Configure the SMA 1000 Series Physical or Virtual Appliance
- Verify SSL-VPN remote connectivity is functioning properly
- Verify functionality of all configured features
- Configurations will be completed during normal business hours 0800 – 1700 hours Monday – Friday Local Standard Time
- Service Cutover may be after hours from 1700 – 1800 hours Monday – Friday Local Standard Time

SonicWall Remote Implementation Service – Secure Mobile Access 1000

Post-Implementation

- 30 days of post-implementation support is included should the customer need technical support for the specific implementation (the installation and configuration of the product only).
- The customer should contact SonicWall Support for product-related issues.
- Additional implementation support or management services (beyond 30 days) may be available for purchase (additional fees may apply).

Scope, Prerequisites and Other Terms

Scope

The following services are NOT included in the planned Activities for this service but, may be purchased separately (additional fees may apply):

- Troubleshooting client installation issues for SSL-VPN/ Mobile Connect
- Configuring any Appliance in the SRA or SMA 100 series
- Creation of additional portals
- Deploying a Distributed (Cluster) configuration
- Training/Consulting Services

Prerequisites

- The customer must ensure that the existing infrastructure, hardware and (if applicable) virtualized configuration is sufficient to support the environment
- The customer must commit a technical resource on a full-time basis to provide SonicWall or the partner with the assistance required
- When deploying the Virtual Appliance, the Customer is responsible for installing the virtual machine on their servers prior to the service engagement
- Customer will provide the group information required for Role-based Administration.
- Access Control lists will be provided by the customer prior to engagement of an authorized SonicWall provider.
- End Point Control Zones and Profiles for global, group, or user must be outlined prior to engagement of a SonicWall authorized provider.
- Network Interface IP addresses need to be assigned prior to engagement of an authorized SonicWall provider.
- Network Objects must be outlined prior to engagement of an authorized SonicWall provider.
- Workplace requires a browser that supports JavaScript and SSL
  - Translated Web access can be used as a method supported as an alternative method, but also requires JavaScript and SSL support in the browser
  - Mapping a backend resource either to a port on the EXSeries appliance, or to an external fully qualified domain name is another supported method
- Two RADIUS servers can be used for two-factor authentication, allowing users to be authenticated through the Web portal or with a Secure Mobile Access client.
- Microsoft Outlook Web Access is only supported based on the published versions in SonicWall Administration Guides and Data Sheets for the model and firmware version of the product being delivered
- Windows SharePoint Services are only supported based on the published versions in the SonicWall Administration Guides and Data Sheets for the model and firmware version of the product being delivered
- Lotus Domino Web Access is only supported based on the published versions in SonicWall Administration Guides and Data Sheets for the model and firmware version of the product being delivered
- Citrix Portal is only supported based on the published versions in SonicWall Administration Guides and Data Sheets for the model and firmware version of the product being delivered
- One Time Passwords requires SMS-capable phones. SMS-capable phones may have additional service provider fees that are not part of this SOW.
- Supported Authentication methods
  - LDAP with username/password or certificate
  - Quest Defender
  - SAML
  - Microsoft Active Directory with username/password, configured with either a single root domain, or one or more subordinate (child) domains
  - Public Key Infrastructure (PKI) with digital certificate SonicWall SMA Connect Tunnel 12.0 Deployment Planning Guide About SonicWall SMA Connect Tunnel 8
  - RSA Authentication Manager server authentication using token-based user credentials
  - Local users with username/password up to 5 accounts

SonicWall Remote Implementation Service – Secure Mobile Access 1000

Other Terms

- All activities will be performed remotely utilizing the phone and web conferencing
- It is the customer's responsibility to ensure it has the appropriate agreements with the provider of the Activities.
- The provision of the Activities does not include the development of any intellectual property. All right, title and interest arising from the performance of Activities shall vest in SonicWall.
- SonicWall and/or the provider of the Activities may require execution of additional documentation before performance of the Activities begin. This additional documentation may include (without limitation) dates for the work to begin. If the provider of the Activities can accommodate a change in schedule related to the Activities, the provider may require a two (2) week lead time (or more before Activities can be performed.
- If a customer makes any changes during or after the Activities begin, additional charges and/or schedule changes may apply.
- Only configured features publicly posted by SonicWall in the Datasheets may be configured.
- Not all Activities may need to be configured.
- The information provided herein is a general description of Activities. Any services delivered that are not explicitly outlined herein are not a part of this offer.
- The duration for the provision of Activities may vary based on many factors including, but not limited to, the complexity of the customer's environment.
- SonicWall is not responsible for ensuring Customer's compliance with data privacy, security and PCI requirements.
- Customer agrees that additional fees may be due and payable if Customer makes any such changes or otherwise fails to meet the prerequisites set forth herein.
- Only authorized SonicWall providers may provide the Activities described by this offer.

Purchase Information

SKU ID	DESCRIPTION
01-SSC-4357	SonicWall Remote Implementation SMA 1000 Series

About Us

Over a 27 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Blvd
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com