Remote Implementation of a SonicWall Secure Mobile Access (SMA) 1000 Series and Secure Remote Access (SRA) EX Appliances

Overview

Remote Implementation of a SonicWall-branded SMA 1000 Series Appliance service ("Activity") typically consists of 20 days to assist the customer with the remote installation and configuration of the SonicWall Internet Security Appliance. The Activities will be limited to those stated herein.

Activities

The planned Activities include:

Pre-Deployment Steps

- Review existing network topology and configuration
- Create a valid design based on customer requirementss

Configuration

- Configurations will be completed remotely
- Create network diagram based on proposed topology
- 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
- Web Application Firewall
- Domain Integration
- Network Interfaces
- System Time
- External FTP/TFTP Server
- 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
- NetExtender Settings
- 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
  - 3 Zones configured per Access Method
    - Trusted
    - Untrusted
    - Quarantined
- Will provide configuration for an All-in-one configuration

Implementation

- Work with customer over the phone to complete the physical installation
- Assist with client software on up to three (3) 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

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.

Remote Implementation of a SonicWall Secure Mobile Access (SMA) 1000 Series and Secure Remote Access (SRA) EX Appliances

Scope, prerequisites, dependencies 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/ NetExtender/Mobile Connect
- Configuring any Appliance in the SMA or SRA 100 series
- Creation of additional portals
- Deploying a Distributed (Cluster) configuration
- Training/Consulting Services

Prerequisites

- The customer must ensure that the existing infrastructure and hardware 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

Other terms

- 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.
- 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 such as NetExtender or Secure Virtual Assist.
  - SSO in SMA/SRA appliances do not support two-factor authentication
- 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 supports LDAP Certificate
  - Dell Defender
  - SAML CA SiteMinder
  - RADIUS PhoneFactor with username/password or token-based authentication such as SecurID or SoftID
  - 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
  - RSA ClearTrust with credentials
  - Local users with username/password
    - Up to 5 accounts

Remote Implementation of a SonicWall Secure Mobile Access (SMA) 1000 Series and Secure Remote Access (SRA) EX Appliances

- Customer provides SSL certificates to be used for the SSL connection, two certificates are required for:
  - The appliance services use a certificate to secure user traffic.
    - A Commercial Certificate Authority (CA) is recommended
    - A self-signed certificate can be used. The customer is required to deploy the Root CA to each client prior to deployment, if the customer does not want the end user to accept a self-signed certificate each time they connect.
  - The Appliance Management Console (AMC) uses a certificate to secure management traffic
    - Requires a self-signed certificate
  - SonicWall will provide a Certificate Signing Request if directed by customer
    - How the certificate and who the certificate are signed by is a responsibility of the customer
- Customer will provide the group information required for Role-based Administration
- 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 EX-Series appliance, or to an external fully qualified domain name is another supported method
- Access Control lists will be provided by the customer prior to SonicWall partner's engagement. The list can be either provided by a pre-existing Client Access VPN solution or a newly developed security policy
- End Point Control Zones and Profiles for global, group, or user must be outlined prior to SonicWall partner engagement. The outline can come from either a pre-existing Client Access VPN solution or a newly developed security policy
- Network Interface IP's need to be assigned prior to SonicWall partner engagement.
- External FTP/TFTP Server IP's need to be assigned prior to SonicWall partner engagement.
- Network Objects must be outlined prior to SonicWall partner engagement. The outline can come from either a pre-existing Client Access VPN solution or a newly developed security policy
- Only configured features publicly posted by SonicWall in the Datasheets may be configured.
- Not all Activities may need to be configured.
- All Activities will be performed remotely utilizing the phone and web conferencing.
- 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 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.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®