SonicWall Remote Implementation Service - Firewall Appliances

The Remote Implementation Service for a SonicWall Firewall appliance is a deployment service ("Activity") that deploys and integrates the SonicWall Firewall physical or virtual appliance into a customer environment. This Activity is typically implemented within 10 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
- Review firewall intended use and compliance requirements
- Review of underlying virtual infrastructure for appropriate sizing (if applicable)

Configuration

- Register unit and upgrade firmware
- Pre-configuration of the unit remotely
  - Convert all NAT and Firewall rules from existing security appliance(s)
  - Configure General Settings (e.g. System Time, DHCP, etc.)
  - Configure Network Interfaces and VLAN
  - Define Address Objects and Groups
  - Define Service Objects and Groups
  - Define Access Control Rules
  - Define NAT policies
  - Configure advanced authentication (Local, LDAP, TACACS or RADIUS)
  - Configure Global VPN Client and/or SSL-VPN
  - Configure Global VPN Client and/or SSL-VPN
  - Configuration of appropriate remote access client on up to three supported devices
  - Configure Site-to-Site VPN Tunnels (up to 10) with other firewalls (if applicable – need access to remote firewalls)
  - Configure High Availability unit in Active/Passive Mode (if applicable – requires additional HA appliance)
  - Configure Security Services to recommended settings:
  - Gateway Anti-Virus
  - Intrusion Protection Service
  - Anti-Spyware
  - Geo-IP
  - Botnet
  - Content Filter Service (No more than two policies)
  - Application Visualization (if requested)
  - Application Control (Best practice standard configuration)
  - Capture ATP
  - Configure integrated wireless (if applicable) with a up to two SSIDs

Installation

- Work with customer over the phone to complete the physical or virtual installation
- Verify NAT and Firewall rules are working as expected
- Verify Site-to-Site VPN(s) are passing data
- Verify Global Client VPN and/or SSL-VPN users are able to connect
- High Availability Failover testing (if applicable)
- WAN Failover testing
- Content Filter Service testing
- Application Visualization testing
- After testing is complete, provide customer with a backup of all settings
- 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 - Firewall Appliances

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):

- Configuration of SonicPoint or SonicWave Wireless Access Points
- Configuration of Software Defined WAN (SDWAN) components
- Integration with management platforms
- Physical or Virtual Switch configuration
- Configuration of more than 5 local users for authentication
- Enforced Anti-Virus implementation
- Configuration of Comprehensive Anti-Spam Service
- Configuration of WAN Acceleration
- Configuration of additional VPN Tunnels
- Virtual Assist configuration
- Client software deployment
- GMS installation/configuration
- Training/Consulting Services
- Provide configuration after hours
- Provide Landing page or Automated certificate enrollment method

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
- Customer is required to present DPI-SSL certificate to the installation technician
- Customer is required to perform self-enrollment of DPI-SSL Certificate
- Customer is required to have a healthy Active Directory and will make all Microsoft configurations.

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.

SonicWall Remote Implementation Service - Firewall Appliances

Purchase Information

SKU ID	DESCRIPTION
01-SSC-8525	SONICWALL REMOTE IMPLEMENTATION SOHO APPLIANCE
01-SSC-8526	SONICWALL REMOTE IMPLEMENTATION TZ 3X0/4X0 APPLIANCE
01-SSC-8527	SONICWALL REMOTE IMPLEMENTATION TZ5X0/TZ6X0 APPLIANCE
01-SSC-8528	SONICWALL REMOTE IMPLEMENTATION NSA26X0/36X0/46X0 APPLIANCE
01-SSC-8530	SONICWALL REMOTE IMPLEMENTATION NSA56X0/66X0 APPLIANCE
01-SSC-3051	SONICWALL REMOTE IMPLEMENTATION SM/NSA 9X00
02-SSC-0318	SONICWALL REMOTE IMPLEMENTATION NSV 10/25/50/100 SERIES
02-SSC-0319	SONICWALL REMOTE IMPLEMENTATION NSV 200/300/400 SERIES
02-SSC-0320	SONICWALL REMOTE IMPLEMENTATION NSV 800/1600 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