System Release 7.17

ASTRO® 25

INTEGRATED VOICE AND DATA

Service Access Architecture

NOVEMBER 2016

MN003353A01-A

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003353A01-A	Original release of the *Service Access Architecture* manual	November 2016

This page intentionally left blank.

Contents

This page intentionally left blank.

List of Figures

This page intentionally left blank.

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About Service Access Architecture

Service Access Architecture is an optional security feature available for ASTRO® 25 systems.

This document describes the current technical solution for Service Access Architecture (SAA).

What Is Covered in This Manual?

The following information is covered in this document:

- Service Access Architecture Description on page 25, provides an overview of Service Access Architecture (SAA).
- Service Access Architecture Theory of Operation on page 29, provides a detailed overview of SAA and how it works internally and within the system.
- Service Access Architecture Installation on page 49, describes installation of SAA components.
- Service Access Architecture Configuration on page 51, describes configuration of SAA components required to get the feature programmed and functioning.
- Service Access Architecture Optimization on page 59, contains information related to ensuring optimal performance of SAA.
- Service Access Architecture Operation on page 61, provides operating information relating to SAA.
- Service Access Architecture Troubleshooting on page 67, describes troubleshooting procedures relating to SAA.
- Service Access Architecture Disaster Recovery on page 69, provides instructions for recovering the token functionality of a RNI-DMZ firewall, which has two-factor tokens provisioned.
- Service Access Architecture Maintenance on page 71, describes periodic maintenance procedures relating to SAA.
- Service Access Architecture Reference on page 73, contains reference information relating to SAA.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

See the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites (6881089E50)	Provides standards and guidelines to follow when setting up a Motorola Solutions communications site. Also known as the R56 manual. This manual may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).

Table continued…

Related Information	Purpose
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Authentication Services	Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems.
802.1x Service Ports on Switches	Provides information relating to the implementation and management of 802.1x standards to authenticate service users at designated Ethernet ports on HP switches and on the internal switch of GCP 8000 Site Controllers and GPB 8000 Reference Distribution Modules (RDMs), in ASTRO® 25 systems.
Backup and Restore Services	Provides information relating to the implementation and management of centralized backup and restore services for supported devices in ASTRO® 25 systems. This manual addresses server and client functions required for these services.
Fortinet Firewall	Provides information on the implementation and replacement of firewall appliances that Motorola Solutions provides, including a firewall in the DMZ between the ASTRO® 25 RNI and a CEN or the Motorola Solutions Support Centre, a firewall in the ISSI.1 Network Gateway between the ASTRO® 25 system and the ISSI.1 peer system, and a Telephony Firewall in the Enhanced Telephone Interconnect subsystem. These firewalls use Fortinet FortiGate models. See the "Zone Core Protection Infrastructure" manual for firewalls used for that feature.
Information Assurance Features Overview	Provides an overview of Information Assurance features for ASTRO® 25 systems, including a description of each feature and their impact on system implementation and management. Additionally, the manual contains details about Motorola Solutions services related to Information Assurance and physical security considerations for ASTRO® 25 systems.
KVL 4000 Radio Authentication User Guide	Provides information associated with the use of the KVL 4000 for Radio Authentication.
Radio Authentication	Provides information and procedures for an optional feature that prevents unwanted and potentially dangerous subscribers from accessing the network in ASTRO® 25 systems.
Securing Protocols with SSH	Provides information on the implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in ASTRO® 25 systems, including configuration sequences that

Table continued…

Related Information	Purpose
	minimize downtime when adding this feature to a system that is already in operation.
Terminal Servers LX Series	Covers installation, configuration, and management of the In-Reach® 8000 (LX-4000S) series Terminal Server which supports a network management connection to servers and network transport equipment in the zone.
Unified Network Configurator	Covers the use of Unified Network Configurator (UNC), a sophisticated network configuration tool that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers, and base radios, and is used to set up sites for ASTRO® 25 systems. UNC has two components: VoyenceControl and Unified Network Configurator Wizards (UNCWs).
Windows Supplemental Configuration Setup Guide	Provides additional procedures for Windows-based devices in ASTRO® 25 systems.
Virtual Management Server Software	Provides information for implementing, maintaining, and replacing common Hewlett-Packard hardware for servers in ASTRO® 25 systems.
Zone Core Protection Infrastructure	Provides information relating to the implementation and management of the Zone Core Protection (ZCP) feature available for ASTRO® 25 systems. ZCP is an optional configuration of hardware and software components for supporting network security atthe zone core (master site). ZCP-specific components covered in this manual include: ZCP firewalls, Mediation LAN switches, and an intrusion detection solution.

This page intentionally left blank.

Chapter 1

Service Access Architecture Description

This chapter provides a high-level description of Service Access Architecture.

1.1 Service Access Connection Using a Service Laptop

The Service Access Architecture (SAA) feature provides a secured communication path between the Radio Network Infrastructure (RNI) and a remote service user.

Fortinet firewalls in the ASTRO® 25 system provide Active Directory (AD) authentication and two-factor authentication.

The feature can be implemented in three access scenarios, in which a service laptop can be used to access the RNI:

Local

- A LAN switch connection at a remote site.

  See LAN Switch Connection at a Remote Site on page 29.

- A local VPN connection to the RNI-DMZ firewall via SAA, DMZ, or Internet ports on the firewall. Provided by Fortinet firewalls (via SAA, DMZ, or Internet ports).

  See Accessing Devices Using a Local VPN Connection from the RNI-DMZ Firewall or DMZ Switch on page 32.

- A local VPN connection to the RNI-DMZ firewall via SAA or DMZ VLAN ports on the DMZ switch. Provided by Fortinet firewalls (via SAA or DMZ ports).

  See Accessing Devices Using a Local VPN Connection from the RNI-DMZ Firewall or DMZ Switch on page 32.

Dial-up

A dial-up connection provided by a modem at a simulcast prime site.

See Dial-up Connection Through a Modem at a Simulcast Prime Site on page 33.

On-demand VPN

- A VPN connection to the RNI-DMZ firewall through the SAA modem and terminal server. Provided by Fortinet firewalls.

  See On-Demand VPN Connection to the RNI-DMZ Firewall Through the SAA Modem and Terminal Server on page 35.

- A VPN connection to the RNI-DMZ firewall from the CEN. Provided by Fortinet firewalls only.

  See On-Demand VPN Connection to the RNI-DMZ Firewall from the CEN on page 38.

- A VPN connection to the RNI-DMZ firewall from the Internet. Provided by Fortinet firewalls only.

  See On-Demand VPN Connection to the RNI-DMZ Firewall from the Internet on page 39.

These scenarios provide access to the following services for the remote service user:

- Remote control of devices
- Diagnostics

- File transfer
- Fault management

Secure remote access to these services reduces the amount of time spent maintaining the radio network, and reduces response time for issue resolution.

NOTICE: SAA is not intended to provide end-to-end secured access from the support user to any device regardless of its location in the system. It enables secured access to the trusted part of the radio network. If the device is outside the trusted part of the radio network (for example, at a remote site), other features such as link encryption and Secure Shell (SSH) are required to provide secured access to that device. End-to-end secured access may not be possible if the device does not support the required features.

1.1.1 Application Traffic Allowed from a Service Laptop to the RNI

The Firewall and Gateway Access Control Lists (ACLs) in an ASTRO® 25 system limit traffic from a remote technician laptop to several applications allowed to communicate with the Radio Network Infrastructure (RNI).

- Secure Shell (SSH) utilities, such as PuTTY
- Other applications that use SSH for secure communication
- Microsoft Windows Remote Desktop Connection
- VMware vSphere Client
- Software Download Manager (SWDL)
- SDM3000 Builder
- HTTPS
- Configuration/Service Software (CSS)

  NOTICE: You can use CSS on the laptop to access devices at a remote site where the service user computer resides. It can also be used to access devices at any remote site in the RNI, but only if you have dialed in to the zone core through the De-Militarized Zone (DMZ) (see Accessing Devices in the RNI Through Modem/Terminal Server in the DMZ and VPN on page 36). CSS can also be installed on the Network Management (NM) clients. This installation of CSS can be used to access devices throughout the RNI.
  Because NM Clients also provide other applications for accessing devices throughout the RNI, a general practice is to start by accessing the NM Client.

NM Clients can make an SSH connection to the following devices:

- HP Switches (except HP 2524)
- Terminal Server
- Motorola Solutions routers and gateways
- G-series RF Site equipment (GTR 8000, GCM 8000, GCP 8000, GPW 8000, or GPB 8000 devices)
- Voice Processor Module (VPM)-based products
- MOSCAD Network Fault Management (NFM) devices (SDM3000 Network Translator, SDM3000 Remote Terminal Unit (RTU)
- Console Telephony Media Gateway

NOTICE: SSH is a prerequisite for many forms of secure Service Access Architecture (SAA) in the system. For more information on SSH, including a list of devices supporting SSH, see *Securing Protocols with SSH* manual.

1.1.2

Service Laptop Connection

Access from the service laptop in an ASTRO® 25 system is restricted to the following locations that the laptop connects to.

Table 1: Service Laptop Location

ASTRO 25 Site Location Reference	Service Laptop Connecting Point
Master Site/Zone Core	Core LAN Switches On-demand VPN connection from the Internet to the RNI-DMZ firewall On-demand VPN connection from the Customer Enterprise Network (CEN) to the RNI-DMZ firewall PSTN dial-up connection to the terminal server and on-demand VPN connection through the terminal server to the RNI-DMZ firewall Local VPN connection to the RNI-DMZ firewall via SAA, DMZ, or Internet ports on the firewall Local VPN connection to the RNI-DMZ firewall via SAA or DMZ VLAN ports on the DMZ switch **NOTICE:** If the DMZ switch is present, local connections are done on the switch. If the DMZ switch is NOT present, local connections are done on the firewall.
Customer Enterprise Network (CEN)	Ethernet switch in CEN
Customer IP Telephony Network	Core LAN switches
NM/Dispatch Site	Ethernet switch at the NM/dispatch site
Inter-RF Subsystem Interface (ISSI) Gateway Site	External switch at the ISSI gateway site
Trunking Repeater Site	External HP switch or the switch port in the GTR 8000 Expandable Site Subsystem (ESS)
High Performance Data (HPD) Site	
SmartX Site	Ethernet switch at the SmartX site or at the zone core (if co-located)
Simulcast Prime Site	Ethernet switch at the simulcast prime site
Simulcast Remote Site	Ethernet switch at the simulcast prime site or local Ethernet switch in simulcast remote site
Zone X	Core LAN switches
K core	K core LAN switch K core DMZ firewall on-demand VPN connection from the Internet and CEN Local VPN connection to the DMZ firewall via DMZ or Internet ports on the firewall

Table continued…

ASTRO 25 Site Location Reference	Service Laptop Connecting Point
	Local VPN connection to the DMZ firewall via DMZ VLAN port on the DMZ switch
Conventional Site	If no Ethernet switch is available, connect via the serial interface to the site gateway
	If an Ethernet switch is available, connect to one of the ports on the Ethernet switch

1.2

Service Access Connection Using KVL

If the Radio Authentication feature is present in the system, a Key Variable Loader (KVL) 4000 device is used for loading the authentication key (K) to a Subscriber Unit (SU) for a corresponding Subscriber Unit Identity (SUID) in the SU, and uploading that information to the Authentication Center (AuC) server. The KVL operator connects the KVL device to the SU using an RS-232 serial interface. The SU then provides its SUID, and the KVL sends K to the SU to create a K-SUID pair in the KVL and SU. The KVL then can upload the K-SUID pair to the AuC server using local or remote access.

For more information on the Radio Authentication feature, see the *Radio Authentication* manual.

For more information on the KVL 4000 device, see the *KVL 4000 Radio Authentication User Guide*.

Local Access Using KVL

The local access option involves connecting the KVL device to the available/allocated De-Militarized Zone (DMZ) switch or Radio Network Infrastructure (RNI)-DMZ firewall port using the USB-to-Ethernet adapter. In an M3 configuration with or without Zone Core Protection (ZCP), the KVL locally connects to the DMZ LAN switch and establishes a Virtual Private Network (VPN) connection with the RNI-DMZ firewall. In L core and M1/ M2 configurations with or without ZCP, the KVL locally connects to the RNI-DMZ firewall and establishes a VPN connection with it. The KVL then uploads the provisioning information to the AuC server. This information is encrypted using the KVL Unique Key Encryption Key (UKEK).

For more information on the firewall ports, see the *Fortinet Firewall*.

Remote Access Using KVL

The remote access option involves connecting the KVL device to the AuC server through the Internet using Cable/DSL connection and the USB-to-Ethernet adapter. The customer provides an internet connection to the firewall and the KVL establishes a VPN connection to the RNI-DMZ firewall, and then uploads the provisioning information to the AuC Server encrypted using the KVL UKEK.

Chapter 2

Service Access Architecture Theory of Operation

This chapter explains how Service Access Architecture (SAA) works in the context of your system.

It describes the following SAA paths and the prerequisites required for each path to operate:

Local

- A LAN switch connection at a remote site.

  See LAN Switch Connection at a Remote Site on page 29.

- A local VPN connection to the RNI-DMZ firewall via SAA, DMZ, or Internet ports on the firewall. Provided by Fortinet firewalls (via SAA, DMZ, or Internet ports).

  See Accessing Devices Using a Local VPN Connection from the RNI-DMZ Firewall or DMZ Switch on page 32.

- A local VPN connection to the RNI-DMZ firewall via SAA or DMZ VLAN ports on the DMZ switch. Provided by Fortinet firewalls (via SAA or DMZ ports).

  See Accessing Devices Using a Local VPN Connection from the RNI-DMZ Firewall or DMZ Switch on page 32.

Dial-up

A dial-up connection provided by a modem at a simulcast prime site.

See Dial-up Connection Through a Modem at a Simulcast Prime Site on page 33.

On-demand VPN

- A VPN connection to the RNI-DMZ firewall through the SAA modem and terminal server. Provided by Fortinet firewalls.

  See On-Demand VPN Connection to the RNI-DMZ Firewall Through the SAA Modem and Terminal Server on page 35.

- A VPN connection to the RNI-DMZ firewall from the CEN. Provided by Fortinet firewalls only.

  See On-Demand VPN Connection to the RNI-DMZ Firewall from the CEN on page 38.

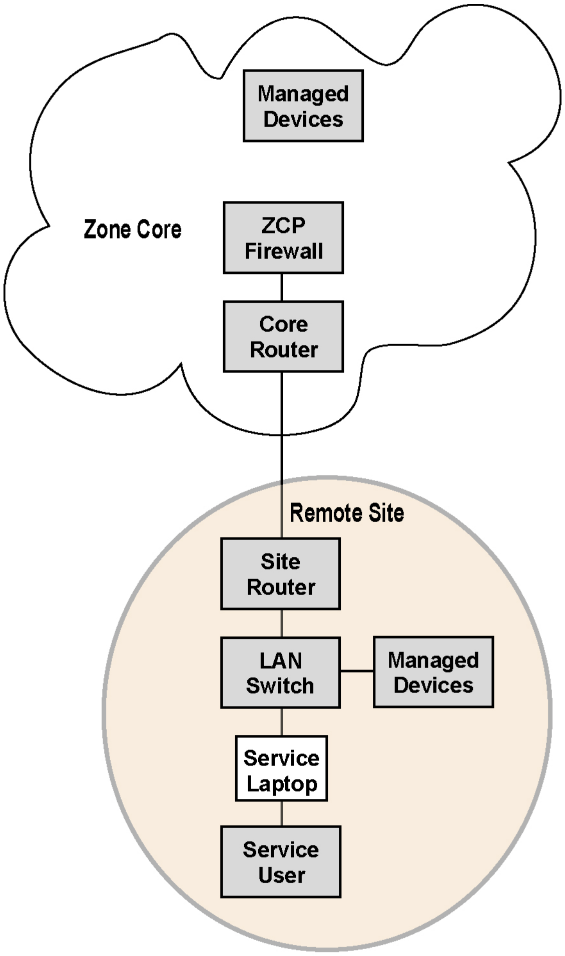
- A VPN connection to the RNI-DMZ firewall from the Internet. Provided by Fortinet firewalls only.

  See On-Demand VPN Connection to the RNI-DMZ Firewall from the Internet on page 39.

2.1 LAN Switch Connection at a Remote Site

The Service Access Architecture (SAA) connection through the LAN switch at a remote site provides the remote service user with access to the devices at the remote site, and to devices accessible from the zone core of the Radio Network Infrastructure (RNI).

Figure 1: SAA Connection Through LAN Switch at a Remote Site



SAA_LAN_switch_Remote_Site

Related Links

Service Access Connection Using a Service Laptop on page 25
Service Access Architecture Theory of Operation on page 29

2.1.1 Accessing Devices from a Remote Site LAN Switch

Follow this process to access devices using a direct connection to the LAN switch at a remote site.

Prerequisites: This Service Access Architecture (SAA) path requires components that may be present in the system to support other features including:

- MAC Port Lockdown/802.1x to support authenticated switch access
- Centralized Authentication to support MAC Port Lockdown/802.1x
- Zone Core Protection to restrict application traffic between the remote site and the zone core

NOTICE: To configure MAC Port Lockdown/802.1x for the service laptop, see the *Windows Supplemental Configuration Setup Guide* manual and the *802.1x Service Ports on Switches* manual for 802.1x software/configuration prerequisites.

Additional components that may be needed for this SAA path include:

- Microsoft Windows Remote Desktop Connection client software

- Secure Shell (SSH) client software utilities supporting SSH Version 2 such as PuTTY
- VMware vSphere Client software

This process requires that you have permission to access these devices (permissions are defined in Active Directory users/groups for devices that use Centralized Authentication).

Firewall rules and Gateway Access Control Lists (ACLs) restrict access to devices in the RNI. Active Directory group memberships also restrict access to devices that use Centralized Authentication. For information, contact your system administrator.

Process:

1. Connect the laptop to the Ethernet service port on the remote site LAN switch. Provide credentials to satisfy required 802.1x authentication.
2. Access devices at your site. For example:
   - To access Configuration/Service Software (CSS)-managed devices at your site, use CSS on the laptop. Restrictions on the devices that Motorola Solutions software can configure remotely are based on system security policies.
   - To access devices at your site, use Telnet or PuTTY on the laptop. If SSH is implemented, some devices may be configured for secure communications only.
   - To perform an SWDL of your site, use the computer-based Software Download Manager (SWDL) application on the laptop. Restrictions on the devices that Motorola Solutions software can configure remotely are based on system security policies.
   - To execute commands such as a ping, use the command prompt on the laptop.
   - To configure SDM3000 Network Translator (SNT) and SDM3000 Remote Terminal Unit (RTU) via Telnet/TFTP or SSH/SFTP (depending on your location and your administrative policies), use SDM3000 Builder on the laptop.
3. Connect to the Network Management (NM) client in the zone core using the Windows Remote Desktop Connection on the laptop.
4. From the NM client in the zone core, launch applications to access devices throughout the Radio Network Infrastructure (RNI). For example:
   - To establish secure sessions (SSH) or to transfer files securely (sftp), use PuTTY on the NM client. The NM client acts as the SSH client for devices configured as SSH servers in the RNI. (Other devices in the system configured as SSH clients can also be used to securely access devices configured as SSH servers.) See the ASTRO® 25 system *Securing Protocols with SSH* manual for instructions about using PuTTY for SSH sessions.
   - To access numerous devices throughout the RNI, launch the Unified Network Configurator from the browser on the NM Client. See the ASTRO® 25 system *Unified Network Configurator* manual.
   - To access CSS-managed devices at remote sites, use the Configuration/Service Software (CSS) on the NM client in the zone core. See *CSS Online Help*.

2.2 Local VPN Connection from the RNI-DMZ Firewall or DMZ Switch

The following local VPN connections are available:

- A local VPN connection to the RNI-DMZ firewall via SAA, DMZ, or Internet ports on the firewall
- A local VPN connection to the RNI-DMZ firewall via SAA or DMZ VLAN port on the DMZ switch

The local connections can be used if the service user is located at the zone core. Connecting locally can also be used to troubleshoot the remote connections via the same interfaces (SAA, DMZ, Internet). For example, if an Internet VPN cannot be established remotely, it may be a configuration problem with the RNI-DMZ firewall or the Customer Network Interface (CNI) specifically intermediate routers. If the local connection works, the RNI-DMZ firewall is configured correctly and the problem may be in the CNI (intermediate routers).

2.2.1 Accessing Devices Using a Local VPN Connection from the RNI-DMZ Firewall or DMZ Switch

Prerequisites: Ensure that the service laptop is configured with a static IP address. A static IP address is necessary to establish this type of local VPN connection.

Procedure:

1. Connect the service laptop to the RNI-DMZ firewall or DMZ switch via one of the following port types:
   - SAA
   - DMZ
   - Internet

   See “RNI-DMZ Firewall Port Connections” in the *Fortinet Firewall* manual.
2. Configure the VPN client (NCP Secure Entry Client) to connect to the RNI-DMZ firewall.
3. With the VPN client software installed on the laptop, establish a VPN connection to the trusted zone of the RNI, providing credentials to satisfy the required Active Directory (AD) authentication.
4. Connect to the managed devices in the RNI by using one of the following applications:
   - Microsoft Windows Remote Desktop Connection
   - Motorola Solutions Configuration/Service Software (CSS)
   - VMware vSphere Client
   - SDM3000 Builder

   Application traffic is restricted by firewall rules and by Access Control Lists (ACLs).
5. Connect to the Network Management (NM) client in the zone core by using the Windows Remote Desktop Connection on the laptop.
6. From the NM client in the zone core, launch applications to access devices throughout the RNI. For example:
   - To establish secure sessions (SSH) or to transfer files securely (SFTP), use PuTTY on the NM client. The NM client acts as the SSH client for devices configured as SSH servers in the RNI. Other devices in the system configured as SSH clients can also be used to securely access devices configured as SSH servers. See the *Securing Protocols with SSH* manual for instructions about using PuTTY for SSH sessions.
   - To access numerous devices throughout the RNI, launch the Unified Network Configurator (UNC) from the browser on the NM Client. *Unified Network Configurator* manual.
   - To access Configuration/Service Software (CSS)-managed devices at remote sites, use the CSS on the NM client in the zone core. See *CSS Online Help*.

Related Links

Service Access Connection Using a Service Laptop on page 25

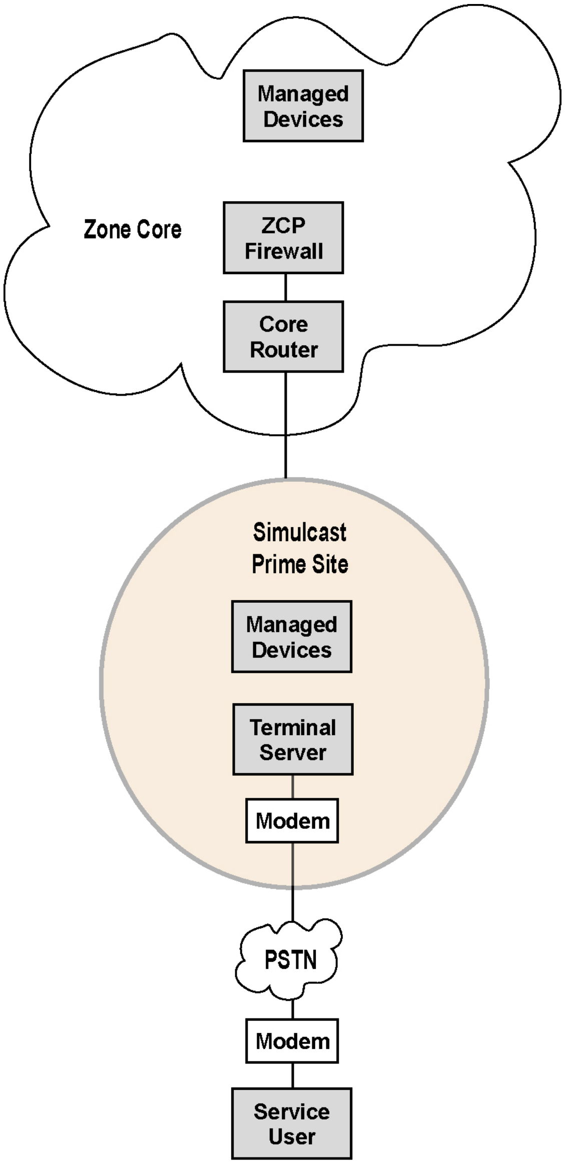
Service Access Architecture Theory of Operation on page 29

2.3 Dial-up Connection Through a Modem at a Simulcast Prime Site

This operation is recommended only if a Service Access Architecture (SAA) connection through the LAN switch at a remote site is not available, or access from the master site to the prime site is not available (prime site link down).

The Service Access Architecture (SAA) dial-up connection through a modem at a Simulcast Prime Site provides remote access to the devices at the simulcast prime site. It also provides access to the zone core, where the Network Management (NM) client can be used to access devices in the rest of the Radio Network Infrastructure (RNI).

Figure 2: SAA Dial-up Connection Through Modem/Terminal Server at Simulcast Prime Site



SAA_modem_Simul_Prime_SIte

Related Links

Service Access Connection Using a Service Laptop on page 25
Service Access Architecture Theory of Operation on page 29

2.3.1 Accessing Devices Using Dial-up to Simulcast Prime Site Modem/Terminal Server

Follow this process to access devices using a dialup connection to the modem and terminal server at a Simulcast Prime Site.

Prerequisites: Depending on your system configuration, additional components that may be needed for this Service Access Architecture (SAA) path include:

- MRV LX-4048 (48-port) Terminal Server with internal or external modem (replace the IR Series Terminal Server, if present)
- Microsoft Windows Remote Desktop Connection client software
- Secure Shell (SSH) client software utilities supporting SSH Version 2 such as PuTTY
- VMware vSphere Client software

This process requires that you have permission to access these devices (permissions are defined in Active Directory users/groups for devices that use Centralized Authentication).

Firewall rules and Gateway Access Control Lists (ACLs) restrict access to devices in the RNI. Access to devices is also restricted by your Active Directory group memberships for devices that use Centralized Authentication. For information, contact your system administrator.

Process:

1. Establish a dial-up connection to the modem at the Prime Site. This modem connects to the terminal server at the Prime Site. Provide Active Directory (AD) credentials to satisfy the required AD authentication.

   For information on the local authentication method used as a local fallback to AD authentication (if AD is unavailable), see the *Terminal Servers LX Series* manual.

2. Access devices at the Simulcast Prime Site in the following ways:
   - From the terminal server menu, connect to the console for devices in the Simulcast Prime Site connected to the serial ports on the terminal server.
   - To access Configuration/Service Software (CSS)-managed devices at the Simulcast Prime Site, use the CSS on the laptop. Restrictions on the devices that Motorola Solutions software can configure remotely are based on system security policies.
   - To configure SDM3000 Network Translator (SNT) and SDM3000 Remote Terminal Unit (RTU) via Telnet/TFTP or SSH/SFTP (depending on your location and your administrative policies), use SDM3000 Builder on the laptop.
3. Connect to the Network Management (NM) client in the zone core using the Windows Remote Desktop Connection on the laptop.
4. From the NM client in the zone core, launch applications to access devices throughout the Radio Network Infrastructure (RNI). For example:
   - To establish secure sessions (SSH) or to transfer files securely (SFTP), use PuTTY on the NM client. The NM client acts as the SSH client for devices configured as SSH servers in the RNI. (Other devices in the system configured as SSH clients can also be used to securely access devices configured as SSH servers.) See the ASTRO® 25 system *Securing Protocols with SSH* manual for instructions about using PuTTY for SSH sessions.

- To access numerous devices throughout the RNI, launch the Unified Network Configurator from the browser on the NM Client. See the ASTRO® 25 system *Unified Network Configurator* manual.
- To access CSS-managed devices at remote sites, use the Configuration/Service Software (CSS) on the NM client in the zone core. See *CSS Online Help*.

2.4 On-Demand VPN Connection to the RNI-DMZ Firewall Through the SAA Modem and Terminal Server

The Service Access Architecture (SAA) dial-up connection through a modem in the De-Militarized Zone (DMZ) provides a direct link between a remote service user and the Radio Network Infrastructure (RNI). A Virtual Private Network (VPN) tunnel connects the service user to the trusted side of the RNI-DMZ firewall (on the side of the RNI zone core). From there, you can access devices in the RNI.

This type of connection is not available in K core systems.

The SAA modem establishes a dial-up connection between the terminal server and the service user. Then the terminal server assigns a predefined IP address range to the service user so the RNI-DMZ firewall lets the service user access devices in the RNI when a VPN connection is established. The RNI-DMZ firewall authenticates VPN users via RADIUS to Active Directory and verifies two-factor tokens via built-in authentication server functionality. The terminal server is not used to connect to any devices in the DMZ, so its serial ports are not used.

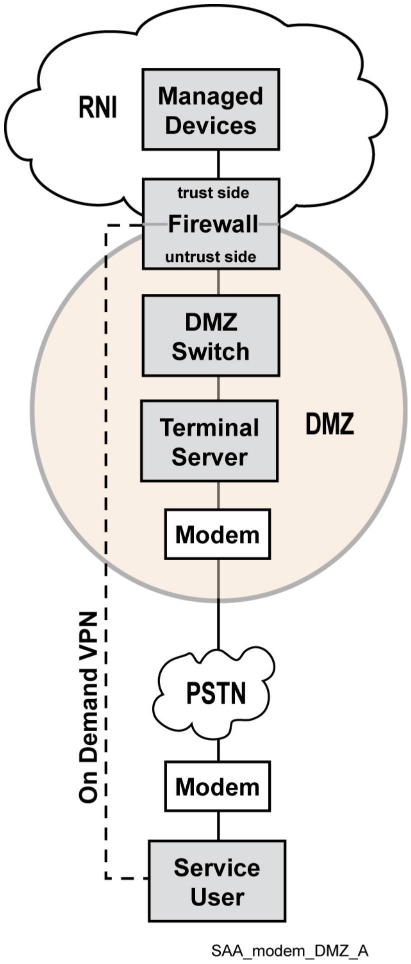
This type of connection is described by the following process:

1 The modem is used to establish a dial-up connection to the terminal server in the DMZ. Active Directory (AD) credentials are needed to establish this connection.

2 After the dial-up connection is established with the terminal server, a VPN connection can be established with the RNI-DMZ firewall. AD credentials are needed again to establish the VPN. (two-factor credentials are also necessary only if two-factor authentication is enabled for the user).

Figure 3: SAA Dial-up Connection Through SAA Modem/Terminal Server and VPN

This figure shows the dial-up connection through the modem and terminal server in the DMZ, and the VPN connection to the RNI-DMZ firewall.



Related Links

Service Access Connection Using a Service Laptop on page 25
Service Access Architecture Theory of Operation on page 29

2.4.1 Accessing Devices in the RNI Through Modem/Terminal Server in the DMZ and VPN

Follow this process to access managed devices in the Radio Network Infrastructure (RNI) using the terminal server in the De-Militarized Zone (DMZ) and Virtual Private Network (VPN).

Prerequisites:
Ensure the MRV LX-4008 (8-port) Terminal Server in the DMZ (with internal or external modem) is included for this Service Access Architecture (SAA) path.

Ensure that the NCP Secure Entry Client software is installed on the laptop.

Ensure that this path also includes the following components if they are required in the system to support other features:

- Active Directory Domain Controller for VPN authentication

- RNI-DMZ firewall: Fortinet FortiGate 100D firewall between the RNI and the DMZ, configured to allow SAA traffic (optionally, provides two-factor authentication)
- DMZ Ethernet switch

Depending on your system configuration, additional components that may be needed for this SAA path include:

- Microsoft Windows Remote Desktop Connection client software
- Secure Shell (SSH) client software utilities supporting SSH Version 2 such as PuTTY
- VMware vSphere Client software

Firewall rules and Gateway Access Control Lists (ACLs) restrict access to devices in the RNI. Active Directory group memberships also restrict access to devices that use Centralized Authentication. For information, contact your system administrator.

Process:

1. Establish a dial-up connection to the modem/terminal server in the DMZ. Provide Active Directory (AD) credentials to satisfy required authentication.

   NOTICE: For information on the local authentication method used as a fallback (if the Active Directory is unavailable), see the *Terminal Servers LX Series* manual.

2. With the NCP Secure Entry Client software installed on the laptop, establish a VPN connection to the RNI-DMZ firewall, providing credentials to satisfy required Active Directory (AD) authentication and two-factor authentication (if enabled).
3. Application traffic is restricted by firewall rules and by Access Control Lists (ACLs). Connect to managed devices in the RNI using one of the following applications:
   - Microsoft Windows Remote Desktop Connection
   - Motorola Solutions Configuration/Service Software (CSS)
   - VMware vSphere Client
   - SDM3000 Builder
4. Connect to the Network Management (NM) client in the zone core using the Windows Remote Desktop Connection on the laptop.
5. From the NM client in the zone core, launch applications to access devices throughout the Radio Network Infrastructure (RNI). For example:
   - To establish secure sessions (SSH) or to transfer files securely (sftp), use PuTTY on the NM client. The NM client acts as the SSH client for devices configured as SSH servers in the RNI. (Other devices in the system configured as SSH clients can also be used to securely access devices configured as SSH servers.) See the ASTRO® 25 system *Securing Protocols with SSH* manual for instructions about using PuTTY for SSH sessions.
   - To access numerous devices throughout the RNI, launch the Unified Network Configurator from the browser on the NM Client. See the ASTRO® 25 system *Unified Network Configurator* manual.
   - To access Configuration/Service Software (CSS)-managed devices at remote sites, use the CSS on the NM client in the zone core. See *CSS Online Help*.

Related Links

Application Traffic Allowed from a Service Laptop to the RNI on page 26

2.5 On-Demand VPN Connection to the RNI-DMZ Firewall from the CEN

This type of Service Access Architecture (SAA) connection provides the service user access to the devices in the Radio Network Infrastructure (RNI) from the Customer Enterprise Network (CEN) through a Virtual Private Network (VPN). An on-demand VPN connection is established between the CEN and the RNI-DMZ (De-Militarized Zone) firewall.

A DMZ (CEN) on-demand VPN connection is only available for IPv4 systems when the RNI-DMZ firewall is present. For DMZ on-demand VPN, the following changes can be required:

RNI-DMZ firewall changes for on-demand VPN

Verify the specific route to the DMZ (CEN) VPN client IP address. If no route exists, add a static route to the DMZ (CEN) VPN client IP address.

Backhaul/next hop router changes for on-demand VPN

Verify the specific route to the DMZ (CEN) VPN client and DMZ firewall IP address. If no route exists, add a static route to the DMZ (CEN) VPN client and RNI-DMZ firewall IP address.

CEN router changes for on-demand VPN

Verify the specific route to the RNI-DMZ firewall IP address. If no route exists, add a static route to the RNI-DMZ firewall IP address.

Related Links

Service Access Connection Using a Service Laptop on page 25

Service Access Architecture Theory of Operation on page 29

Troubleshooting VPN Connections from the CEN or Internet on page 67

2.5.1 Accessing Devices from the CEN Through a VPN

Perform this process to establish a Virtual Private Network (VPN) connection to the RNI-DMZ (Radio Network Infrastructure-De-Militarized Zone) firewall from the Customer Enterprise Network (CEN). This connection provides secure service access to the devices throughout the RNI.

Procedure:

1. Configure VPN client to connect to the RNI-DMZ firewall.

   NOTICE: The RNI-DMZ firewall permits VPN connections to originate from the CEN, but it is up to the user to configure the network to reach the RNI-DMZ firewall. This may require additional manual configuration depending on how existing CEN connections are configured.

2. With the NCP Secure Entry Client software installed on the laptop, establish a VPN connection to the trusted zone of the RNI, providing credentials to satisfy the required Active Directory (AD) authentication.

3. Connect to the managed devices in the RNI by using one of the following applications:

   - Microsoft Windows Remote Desktop Connection
   - Motorola Solutions Configuration/Service Software (CSS)
   - VMware vSphere Client
   - SDM3000 Builder

   Application traffic is restricted by firewall rules and by Access Control Lists (ACLs).

4. Connect to the Network Management (NM) client in the zone core by using the Windows Remote Desktop Connection on the laptop.

5. From the NM client in the zone core, launch applications to access devices throughout the RNI. For example:
   - To establish secure sessions (SSH) or to transfer files securely (SFTP), use PuTTY on the NM client. The NM client acts as the SSH client for devices configured as SSH servers in the RNI. Other devices in the system configured as SSH clients can also be used to securely access devices configured as SSH servers. See the *Securing Protocols with SSH* manual for instructions about using PuTTY for SSH sessions.
   - To access numerous devices throughout the RNI, launch the Unified Network Configurator (UNC) from the browser on the NM Client. *Unified Network Configurator* manual.
   - To access Configuration/Service Software (CSS)-managed devices at remote sites, use the CSS on the NM client in the zone core. See *CSS Online Help*.

Related Links

Troubleshooting VPN Connections from the CEN or Internet on page 67

2.6 On-Demand VPN Connection to the RNI-DMZ Firewall from the Internet

This type of Service Access Architecture (SAA) connection provides the service user access to the devices in the Radio Network Infrastructure (RNI) from the Internet through a Virtual Private Network (VPN). An on-demand VPN connection is established between the Internet and the RNI-DMZ (De-Militarized Zone) firewall.

Related Links

Service Access Connection Using a Service Laptop on page 25
Service Access Architecture Theory of Operation on page 29
Troubleshooting VPN Connections from the CEN or Internet on page 67

2.6.1 Accessing Devices Through Internet VPNs

Virtual Private Network (VPN) connections to the RNI-DMZ (Radio Network Infrastructure-De-Militarized Zone) firewall from the Internet provide secure service access to the devices throughout the RNI.

Procedure:

1. On a laptop with the NCP Secure Entry Client software installed, configure the VPN client to connect to the RNI-DMZ firewall.

   NOTICE: The RNI-DMZ firewall permits VPN connections to originate from the Internet. To start using VPN connections from the Internet, configure the network to reach the RNI-DMZ firewall. Depending on the properties of the existing Internet connections, the network may require additional manual configuration.
2. Establish a VPN connection to the trusted zone of the RNI, providing credentials to satisfy the required Active Directory (AD) authentication.
3. Connect to the managed devices in the RNI by using one of the following applications:
   - Microsoft Windows Remote Desktop Connection
   - Motorola Solutions Configuration/Service Software (CSS)
   - VMware vSphere Client

- SDM3000 Builder

Firewall rules and Access Control Lists (ACLs) restricts application traffic.

4. Connect to a Network Management (NM) client in the zone core by using the Windows Remote Desktop Connection on the laptop.
5. From the NM client in the zone core, launch applications to access devices throughout the RNI.

   Step example:

   - To establish secure sessions (SSH) or to transfer files securely (SFTP), use PuTTY on the NM client. The NM client acts as an SSH client for devices configured as SSH servers in the RNI. You can also use other devices in the system configured as SSH clients to securely access devices configured as SSH servers. For instructions about using PuTTY for SSH sessions, see the *Securing Protocols with SSH* manual.
   - To access numerous devices throughout the RNI, launch the Unified Network Configurator (UNC) from a browser on the NM Client. See the *Unified Network Configurator* manual.
   - To access CSS-managed devices at remote sites, use CSS on the NM client in the zone core. See *CSS Online Help*.

Related Links

Troubleshooting VPN Connections from the CEN or Internet on page 67

2.7

Configuring FortiTokens in the ASTRO 25 System

The following process explains how hard and mobile FortiTokens are configured in the RNI-DMZ firewall for one time password authentication. The procedures are performed on the Fortinet firewall by using the web-based manager.

Prerequisites:
Ensure that the admin and vpnadmin accounts are enabled in Active Directory (AD).

Obtain the credentials for the admin and vpnadmin accounts.

NOTICE: For systems that previously had RSA installed, add the RSA service user IDs to the Fortinet RNI-DMZ firewall in order to enable VPN access and two-factor authentication. During the expansion to the FortiToken solution, a report containing the RSA user IDs may be available from the Upgrade Operations team.

Process:

1. Before you make any configuration changes, read the information in the following sections:
   - Default Firewall Configuration for Users and User Groups on page 41
   - UNC Backup of FortiToken Data on page 42
2. Set the time and time zone on the RNI-DMZ firewall.

   NOTICE: Perform this procedure if your system does not have an NTP server or if the time and/or time zone on the firewall is inaccurate.

   See Setting the Time and Time Zone on the RNI-DMZ Firewall on page 42.
3. Configure DNS server settings in the RNI-DMZ firewall.

   See Configuring DNS Server Settings in the RNI-DMZ Firewall on page 43.
4. Register the RNI-DMZ firewall.

   See Registering the RNI-DMZ Firewall on page 43.
5. **Soft tokens:** Configure the e-mail server settings in the RNI-DMZ firewall.

See Configuring E-Mail Server Settings in the RNI-DMZ Firewall on page 43.

NOTICE: This step is only required if you want to use soft tokens.

6. **Soft tokens:** Configure the SMS server settings in the RNI-DMZ firewall.

   See Configuring an SMS Service in the RNI-DMZ Firewall on page 44.

   NOTICE: This step is only required if you want to use soft tokens and you want to send authentication codes to users via SMS.

7. Add FortiTokens in the RNI-DMZ firewall.

   a Add hard tokens in the RNI-DMZ firewall.

   See Adding Hard Tokens in the RNI-DMZ Firewall on page 45.

   b Add mobile tokens in the RNI-DMZ firewall.

   See Adding Mobile Tokens in the RNI-DMZ Firewall on page 45.

8. Assign FortiTokens to existing users in the RNI-DMZ firewall.

   a Assign hard tokens to existing VPN users.

   See Assigning Hard Tokens to VPN Users on page 46.

   b Assign mobile tokens to existing VPN users.

   See Assigning Mobile Tokens to VPN Users on page 46.

9. Configure new VPN users.

   See Creating New VPN Users in the RNI-DMZ Firewall on page 51.
   This procedure consists of creating new users, enabling the e-mail or sms service for the new users (optional), and adding them to the vpnusers group.

Postrequisites:
After making any configuration changes in the RNI-DMZ firewall, pull the RNI-DMZ firewall configuration from the Unified Network Configurator (UNC) to ensure that the configuration can be retrieved in disaster scenarios. For more information, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

2.7.1 Default Firewall Configuration for Users and User Groups

The default RNI-DMZ (Radio Network Infrastructure-De-Militarized Zone) firewall configuration for users and user groups includes the following TNCT configured values:

- A default Virtual Private Network (VPN) user “serviceuser” is created in the TNCT RNI-DMZ firewall configuration for all systems which have one of the following VPNs: SAA or DMZ or Internet VPN.
  - A local user account is created for K core systems only.

    The password for the local “serviceuser” VPN account: to be provided later
  - A RADIUS user account is created for L core and M core systems.

    The password for the RADIUS “serviceuser” VPN account is defined in the RADIUS server.
- A default user group “vpnusers” is created in the RNI-DMZ firewall configuration for all systems which have one of the following VPNs: SAA or DMZ or Internet VPN.
  - The “serviceuser” VPN user account is by default added to the default VPN user group “vpnusers”.
- Newly created users need to be assigned to the VPN user group “vpnusers”.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40

2.7.2
UNC Backup of FortiToken Data

After configuration changes are made (such as adding and editing VPN users, or modifying token-to-user mapping), from the UNC, pull the individual RNI-DMZ firewall configurations. This ensures that the configurations can be retrieved in disaster scenarios. For more information, see “Device Management” in the *Unified Network Configurator* manual.

⚠ **CAUTION:** The use of the Unified Network Configurator (UNC) rollback functionality with the RNI-DMZ firewall may lead to data inconsistency in the firewall. When applying a rollback configuration to the RNI-DMZ firewall, configuration changes local to the firewall may or may not be preserved. To address the unintended configuration changes during rollback, use the UNC to compare the rollback configuration to the current configuration on the firewall (after the rollback has been applied). Take note of the differences and apply the necessary changes manually on the firewall. On the UNC, pull the fixed firewall configuration to establish a new baseline.

IMPORTANT: If an RNI-DMZ firewall is being recovered and has mobile tokens provisioned, you need to perform an additional step to regain their functionality. Contact Fortinet Support and provide the following information:

- Failed Fortinet firewall serial number
- Replacement Fortinet firewall serial number
- FortiToken Mobile redemption certificate with serial number

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40

2.7.3
Setting the Time and Time Zone on the RNI-DMZ Firewall

The clock on the Fortinet RNI-DMZ firewall must be accurate to work properly with the FortiToken devices. Before you activate the FortiToken devices, check if the time and time zone on your system is accurate, and set them to correct values if necessary.

In systems with the Network Time Protocol (NTP) server, the firewall is configured by default to retrieve the time from the NTP server. In such systems, setting the time on the firewall manually is not required. However, you need to set the time zone. In K core systems, an NTP server is optional. If your system does not have an NTP server or the time and/or time zone on your system is inaccurate, set the time and time zone on the firewall manually by performing this procedure.

IMPORTANT: Ensure that you check and set the time and time zone on the firewall before entering the activation code from the FortiToken Mobile Redemption Certificate and/or importing the hard token seed file from the Activation CD. Adjusting the time on the firewall after the tokens have been activated prevents VPN connections from being established.

Procedure:

1. In the Fortinet web-based manager, select **Dashboard** → **Status**.
2. In the **System Information** area, in the **System Time** field, click **Change**.
3. In the **Time Settings** window, perform the following actions:
   a. From the **Time Zone** drop-down list, select your time zone.

   b Click the **Set Time** option. Enter the current time as accurately as possible and the current date.

4. Click **OK** to save the changes.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40

2.7.4

Configuring DNS Server Settings in the RNI-DMZ Firewall

Perform this procedure by using the Fortinet web-based manager. The admin account is required to make these changes.

Procedure:

1. Select **System** → **Network** → **DNS**.
2. In the **DNS Settings** area, perform one of the following actions:
   - To use the FortiGuard Servers (default setting), leave **Use FortiGuard Servers** selected.
   - To use different DNS servers, select **Specify**, and add the **Primary** and **Secondary** DNS servers.
3. Click **Apply**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Adding Mobile Tokens in the RNI-DMZ Firewall on page 45

2.7.5

Registering the RNI-DMZ Firewall

Prerequisites: Connect the RNI-DMZ firewall to the Internet.

Procedure:

1. Select **System** → **Config** → **FortiGuard**.
2. In the **Support Contract** area, click the green flag for **Registration**.
3. Perform one of the following actions:
   - If you have a FortiCare account, enter login information, and click **OK**.
   - If you do not have a FortiCare account, create a new account, enter login information, and click **OK**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Recovering Mobile Tokens in the RNI-DMZ Firewall on page 69

2.7.6

Configuring E-Mail Server Settings in the RNI-DMZ Firewall

The FortiToken e-mail option sends a token activation code to the configured email address. The activation code can then be redeemed within the Fortinet iOS or Android application for a mobile token. The mobile token works just like a hard token; the only difference is that it is contained within the mobile application.

NOTICE: The activation code is sent along with an expiration time. After the expiration time has passed, the token can no longer be activated and needs to be re-provisioned.

You need to configure the e-mail services based on the VPN users' e-mail providers.

The admin account is required to make these changes.

Perform this procedure on the Fortinet firewall by using the web-based manager.

Procedure:

1. Select **System** → **Config** → **Advanced** → **Email Service**.
2. Enter the **SMTP Server** and **Default Reply To** address.
3. If applicable, enable **Authentication** and enter the **SMTP User** and **Password** to use.

   The **SMTP User** must be a full e-mail address.
4. Click **Apply**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Assigning Mobile Tokens to VPN Users on page 46

2.7.7

Configuring an SMS Service in the RNI-DMZ Firewall

The FortiToken SMS option sends a token activation code to the configured SMS number. The activation code can then be redeemed within the Fortinet iOS or Android app for a mobile token. The mobile token works just like a hard token; the only difference is that it is contained within the mobile application.

NOTICE: The activation code is sent along with an expiration time. After the expiration time has passed, the token can no longer be activated and will need to be re-provisioned.

If you do not use the FortiGuard Messaging Service, you need to configure the SMS services based on the VPN users' wireless providers.

The admin account is required to make the following changes.

Perform this procedure on the Fortinet firewall by using the web-based manager.

Procedure:

1. Select **System** → **Config** → **Advanced** → **SMS Service**.
2. In the **SMS Service** area, click **Create New**.
3. Perform the following actions:
   a. In the **Name** column, enter a name for the SMS service.
   b. In the **Address** column, enter the service address (domain name).
   c. Click **OK**.
4. Click **Apply**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Assigning Mobile Tokens to VPN Users on page 46

2.7.8 Adding Hard Tokens in the RNI-DMZ Firewall

Before you can successfully use the FortiToken 200CD token, it must first be installed and activated on the Fortinet firewall, which serves as a token validation server.

The vpnadmin account is needed to add tokens.

Procedure:

1. Log on to the web-based manager of your Fortinet unit from your computer.
2. Insert the CD labeled *FortiToken 200 Activation File*.
3. In the web-based manager, select **User & Device** → **FortiTokens**, and click **Create New**.
4. For the **Type**, select **Hard Token**, and click **Import**.
5. Select **Seed File**, browse to the **.**FTK file on the CD, and click **OK**.

   The loaded serial numbers appear in the list. You can cancel the import if desired.

Each FortiToken 200 is installed and activated, and shown as **Available** in the FortiToken UI

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40

2.7.9 Adding Mobile Tokens in the RNI-DMZ Firewall

To deploy FortiToken Mobile tokens for One Time Password use, you must first install the tokens on the Fortinet RNI-DMZ firewall running FortiOS 5.0 or greater. After installing the tokens, you can assign them to users.

For each FortiToken Mobile purchase, you receive a redemption certificate for the number of tokens purchased. The activation code is 20 digits, revealed by scratching off the designated area of the certificate.

The vpnadmin account is needed to add tokens.

Prerequisites:
Obtain a FortiToken Mobile Redemption Certificate (activation code).

Ensure that the RNI-DMZ firewall has Internet connectivity.

Configure DNS server settings in the RNI-DMZ firewall. See Configuring DNS Server Settings in the RNI-DMZ Firewall on page 43.

Procedure:

1. Locate the 20-digit activation code on the redemption certificate.
2. Log on to the Fortinet web-based manager.
3. Select **User & Device** → **FortiTokens**.
4. Select **Create New**.
5. Select **Mobile Token**.
6. In the **Activation Code** field, enter the 20-digit certificate code.
7. Click **OK**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40

2.7.10 Assigning Hard Tokens to VPN Users

The vpnadmin account is needed to assign tokens.

Perform this procedure by using the Fortinet web-based manager.

Procedure:

1. In the web-based manager, select **User & Device** → **User** → **User Definition**.
2. Select the check box for the user account that you want to configure. On the toolbar, click **Edit User**.
3. In the **Edit User** dialog box, select the **Enable Two-factor Authentication** option.
4. From the **Token** drop-down list, select the FortiToken serial number you want to assign to the selected user account.
5. If this user does not belong to the vpnusers group, perform the following actions:
   - a. Select the **Add this user to groups** check box.
   - b. From the drop-down list, select **vpnusers**.
6. Click **OK**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Creating New VPN Users in the RNI-DMZ Firewall on page 51

2.7.11 Assigning Mobile Tokens to VPN Users

The vpnadmin account is needed to assign tokens.

Perform this procedure by using the Fortinet web-based manager.

Prerequisites: Ensure that the SMS or e-mail server settings are configured in the RNI-DMZ firewall. See Configuring an SMS Service in the RNI-DMZ Firewall on page 44 and Configuring E-Mail Server Settings in the RNI-DMZ Firewall on page 43.

Procedure:

1. In the web-based manager, select **User & Device** → **User** → **User Definition**.
2. Select the check box for the user account that you want to configure. On the toolbar, click **Edit User**.
3. **If the user does not already have the Contact Info configured:** In the **Edit User** window, in the **Contact Info** area, select either the e-mail address or phone number for SMS messages.

   If a phone number is used, the full phone number must be entered. For US numbers, the initial `1` must be included.
4. Select the **Enable Two-factor Authentication** option.
5. From the **Token** drop-down list, select the FortiToken serial number that you want to assign to the selected user account.
6. Click **Send Activation Code**.

   In the Fortinet web-based manager, the tokens are marked as `Pending` until the user activates their code. When the code is activated, the tokens change their status to `Assigned`.

   An activation code is sent to the user’s e-mail address or SMS number.

7 If this user does not belong to the vpnusers group, perform the following actions:

   a Select the **Add this user to groups** check box.

   b From the drop-down list, select **vpnusers**.

8 Click **OK**.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Creating New VPN Users in the RNI-DMZ Firewall on page 51
Recovering Mobile Tokens in the RNI-DMZ Firewall on page 69

This page intentionally left blank.

Chapter 3

Service Access Architecture Installation

This chapter provides information on the software and hardware required for installation of the Service Access Architecture.

3.1 Service Access Architecture Required Software and Hardware

The following table lists sources of information about installing, configuring, and operating the software and hardware elements used for the Service Access Architecture (SAA) service paths.

Table 2: Required Software and Hardware for SAA

The SAA feature introduces no new hardware elements to the system.

Required Software/Hardware	Reference Information
NCP Secure Entry Client (systems with Fortinet RNI-DMZ firewalls)	See Configuring the NCP Secure Entry VPN Client for the Fortinet RNI-DMZ Firewall on page 54.
Network and Security Manager – firewall management software	*Firewall Manager* manual
Fortinet FortiManager – firewall management software, optionally used for logging	*Fortinet Firewall Manager* manual
Windows Remote Desktop Connection client software	See the *Help* available in the tools and Standard Utilities to Access an ASTRO 25 System on page 61.
PuTTY client for Secure Shell (SSH) and SFTP, and general configuration of secure and clear protocols in the radio network infrastructure	*Securing Protocols with SSH* manual
VMware vSphere Client software	*Virtual Management Server Software* manual
SDM3000 Builder software	*SDM3000 Builder User Guide* and the *MOSCAD NFM* manual
MRV LX-4008 Terminal Server **NOTICE:** The serial ports on the LX-4008 Terminal Server are not connected to console ports of any devices in the De-Militarized Zone (DMZ).	*Terminal Servers LX Series* manual
Fortinet firewall	*Fortinet Firewall* manual
DMZ Switch	*System LAN Switches* manual
MAC Port Lockdown/802.1x	*802.1x Service Ports on Switches* and *MAC Port Lockdown* manuals

Table continued…

Required Software/Hardware	Reference Information
Zone Core Protection	*Zone Core Protection Infrastructure* manual
Authentication Servers and Domain Controllers	*Authentication Services* manual
Other Information Assurance features	*Information Assurance Features Overview* manual
Master Site	*Master Site Infrastructure Reference Guide*
Network Management (NM) Client	*Private Network Management Client* manual
Simulcast Subsystems and other remote sites	ASTRO® 25 documentation about each type of site.
MOSCAD Network Fault Management (NFM) devices	*MOSCAD Network Fault Management Feature Guide*

Chapter 4

Service Access Architecture Configuration

This chapter provides configuration information and procedures relating to Service Access Architecture.

4.1 Service User Accounts Configuration

For the following Service Access Architecture (SAA) paths to the zone core of the Radio Network Infrastructure (RNI), configure service user accounts in the Fortinet web-based manager.

- Dial-up connection to the modem and terminal server in the De-Militarized Zone (DMZ)
- Dial-up connection to the modem and terminal server in a Simulcast Prime Site
- Virtual Private Network (VPN) connection to the RNI-DMZ Firewall from the Customer Enterprise Network (CEN)
- Virtual Private Network (VPN) connection to the RNI-DMZ Firewall from the Internet

For using the 802.1x service port on a switch, and for accessing devices that use Centralized Authentication, configure the service user accounts in the Active Directory on the authentication servers. For more information, see the *Authentication Services* manual.

Related Links

Connecting to the System with NCP Secure Entry Client on page 61

4.2 Creating New VPN Users in the RNI-DMZ Firewall

Before configuring any authentication, except dynamic profiles, you must create VPN users. Create VPN users by using the Fortinet web-based manager. VPN accounts can use one-factor or two-factor authentication.

When creating new users, there are two differences between local and remote users:

- Local users require a password to be configured.
- Remote users do not require a password, but do require a remote authentication server to be configured.

NOTICE: Remote users must be added both to the RNI-DMZ firewall and the remote authentication server.

Prerequisites:
Ensure that the vpnadmin account is created so that you can add users and change their group information.

Ensure that the serviceuser and vpnadmin accounts are enabled in the Active Directory (AD) so that you can administer users on the firewall. For information on enabling accounts, see the *Authentication Services* manual.

NOTICE: For systems that previously had RSA installed, add the RSA service user IDs to the Fortinet RNI-DMZ firewall in order to enable VPN access and two-factor authentication. During the expansion to the FortiToken solution, a report containing the RSA user IDs may be available from the Upgrade Operations team.

Procedure:

1 Select **User & Device** → **User** → **User Definition**.

2 Select **Create New**.

3 In the **Choose User Type** window, select one of the following user types:

- **Local User**
- **Remote RADIUS User**

4 Click **Next**.

5 In the **Specify Login Credential** window, perform the following actions:

If…	Then…
If the user is a local user,	perform the following actions: **a** In the **User Name** field, enter the username. **b** In the **Password** field, enter a password. It is recommended to use passwords that are at least six characters long.
If the user is a remote RADIUS user,	perform the following actions: **a** In the **User Name** field, enter the username. **b** Select **Match user on RADIUS server**, and select the RADIUS server from the drop-down menu.

6 Click **Next**.

7 Optional: In the **Provide Contact Info** window, provide an e-mail and/or SMS number for mobile token activation code delivery:

If…	Then…
If you want the mobile token activation code to be sent to this user by e-mail,	in the **Email Address** field, enter the user's e-mail address to e-mail them the token code.
If you want the mobile token activation code to be sent to this user in a text message,	perform the following actions: **a** select the **SMS** option **b** In the **Phone Number** field, enter the user's mobile phone number to receive the token code in a text message. The form adds the country code for the selected country or region automatically. **c** From the **Service Type** drop-down list, select the user's mobile provider. **d** Click **Next**.

If both an e-mail and SMS number are provided for a user, the interface will ask you which method of delivery should be used when a mobile token is assigned.

8. Optional: To use two-factor authentication with this user, in the **Provide Extra Info** window, perform the following actions:
   a. Select the **Enable** option.
   b. Select the **Two-factor Authentication** option.
   c. From the **Token** drop-down list, select the FortiToken serial number to associate with this user.
9. In the **Provide Extra Info** window, select the **User Group** option. From the drop-down list, select **vpnusers**.
10. Click **Create**.

Postrequisites:
After making any configuration changes in the RNI-DMZ firewall, pull the RNI-DMZ firewall configuration from the Unified Network Configurator (UNC) to ensure that the configuration can be retrieved in disaster scenarios. For more information, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

Related Links

Configuring FortiTokens in the ASTRO 25 System on page 40
Assigning Hard Tokens to VPN Users on page 46
Assigning Mobile Tokens to VPN Users on page 46

4.3
Modifying the Password for a Local vpnadmin Account

A full admin account is needed to modify the password for a local vpnadmin account. This procedure is for K core systems that do not have the Unified Network Configurator (UNC). Perform this procedure by using the Fortinet web-based manager.

Procedure:

1. In the web-based manager, log on using a full admin account.

   For example, admin.
2. Select **System** → **Admin** → **Administrators**.
3. Select the local vpnadmin account. On the toolbar, click **Edit**.
4. Click **Change Password**.
5. In the **Edit new password** window, in the **New Password** field, enter the new password.
6. In the **Confirm Password** field, re-enter the new password. Click **OK**.
7. Click **OK**.

Postrequisites:
After making any configuration changes in the RNI-DMZ firewall, pull the RNI-DMZ firewall configuration from the Unified Network Configurator (UNC) to ensure that the configuration can be retrieved in disaster scenarios. For more information, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

4.4
Modifying the Password for a Local VPN User Account

The vpnadmin account is needed to modify the password for a local VPN user, for example, serviceuser. This procedure is for K core systems that do not have the Unified Network Configurator (UNC). Perform this procedure by using the Fortinet web-based manager.

Procedure:

1. In the web-based manager, select **User & Device** → **User** → **User Definition**.
2. Select the user account. On the toolbar, click **Edit User**.
3. In the **Password** field, remove the existing password, and enter the new password.
4. Click **OK**.

Postrequisites:
After making any configuration changes in the RNI-DMZ firewall, pull the RNI-DMZ firewall configuration from the Unified Network Configurator (UNC) to ensure that the configuration can be retrieved in disaster scenarios. For more information, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

4.5 NCP Secure Entry Client

NCP Secure Entry Client is a third-party Virtual Private Network (VPN) client that can be used to remotely connect to an ASTRO® 25 system. Configure the VPN client to match the firewall settings.

4.6 Configuring the NCP Secure Entry VPN Client for the Fortinet RNI-DMZ Firewall

After installing the NCP Secure Entry Client on your laptop, configure the client.

Use this procedure only with the Fortinet RNI-DMZ firewall to configure the following Virtual Private Network (VPN) connections:

- Service Access Architecture (SAA) VPN (dial-up connection to the modem and terminal server in the DMZ)
- Internet VPN
- De-Militarized Zone (DMZ) (Customer Enterprise Network – CEN) VPN

For each of these connections, a different gateway IP address (RNI-DMZ firewall IP address) is used in the VPN client.

Prerequisites:
Install the NCP Secure Entry Client on the laptop.

Obtain access to the rules configured on the firewall between the De-Militarized Zone (DMZ) and the Radio Network Infrastructure (RNI), including the following information:

- Pre-Shared Key
- IP addresses

To obtain the firewall rules, use the Fortinet web-based manager or contact your system administrator.

Procedure:

1. From the **Start** menu, select **Programs** → **NCP Secure Client** → **NCP Secure Entry Client Monitor**.
2. In the **NCP Secure Entry Client** window, select **Configuration** → **Profiles** to create a new profile.
3. In the **Profiles** window, click **Add / Import**.
4. In the **New Profile Wizard – Connection Type** window, select **Link to Corporate Network Using IPsec**. Click **Next**.

5 In the **New Profile Wizard – Profile Name** window, enter the profile name of the connection. Click **Next**.

6 In the **New Profile Wizard – Communication Medium** window, select **LAN (over IP)**. Click **Next**.

7 In the **New Profile Wizard – VPN Gateway Parameters** window, perform the following actions:

   a In the **Gateway (Tunnel Endpoint)** field, enter the IP address of the RNI-DMZ firewall to use as the VPN gateway.

      - For an SAA VPN connection, enter the IP address of the RNI-DMZ firewall in the following format: `XXX.`***`<zone_id>`***`.XXX.XXX` where ***`<zone_id>`*** is the number of the zone where the firewall is located.
      - For a DMZ VPN connection, enter the DMZ IP address of the RNI-DMZ firewall.
      - For an Internet VPN connection, enter the address is the Internet IP address of the RNI-DMZ firewall.

   b Select the **Extended Authentication (XAUTH)** check box.

   c Click **Next**.

8 In the **New Profile Wizard – IPsec Configuration** window, perform the following actions:

   a From the **Exchange Mode** drop-down list, select **main mode (IKEv1)**.

   b From the **PFS Group** drop-down list, select **DH-Group 14 (2048 Bit)**.

   c Click **Next**.

9 In the **New Profile Wizard – Pre-shared Key** window, perform the following actions:

   a In the **Shared Secret** field, enter the shared secret.

   b In the **Confirm Secret** field, re-enter the shared secret.

   c Click **Next**.

10 In the **New Profile Wizard – IPsec Configuration - IP Addresses** window, perform the following actions:

   a From the **IP Address Assignment** drop-down list, select **Local IP Address**.

   b Click **Next**.

11 In the **New Profile Wizard – Firewall Settings** window, perform the following actions:

   a From the **Stateful Inspection** drop-down list, select **when connected**.

   b Select the **NetBIOS over IP** check box.

   c Click **Finish**.

12 In the **Profiles** window, select the newly created profile from the list. Click **Edit**.

13 On the left side of the **Profile Settings** window, select **Basic Settings**, and select the **Default Profile after System Reboot** check box.

14 On the left side of the **Profile Settings** window, select **Line Management**, and perform the following actions:

   a From the **Connection Mode** drop-down list, select **manual**.

   b In the **Inactivity Timeout (sec)** field, enter `100`.

15 If you have not configured the IKE and IPsec policies yet, on the left side of the window, select **IPsec General Settings**, click **Policy Editor**, and perform the following actions:

   a In the **IPsec Configuration** window, select **IKE Policy**. Click **Add**.

   b In the **Name** field, enter: `pre-aes256–sha256` c From the **Authentication** drop-down list, select **Pre-shared Key**.

d From the **Encryption** drop-down list, select **AES 256 Bit**.

e From the **Hash** drop-down list, select **SHA 256 Bit**.

f Click **OK**.

g In the **IPsec Configuration** window, select **IPsec Policy**. Click **Add**.

h In the **Name** field, enter: `esp-aes256-sha256`

i From the **Encryption** drop-down list, select **AES 256 Bit**.

j From the **Authentication** drop-down list, select **SHA 256 Bit**.

k Click **OK**.

l Click **Close**.

16 In the **Policies** area, perform the following actions:

a From the **IKE Policy** drop-down list, select **pre-aes256-sha256**.

b From the **IKE DH Group** drop-down list, select **DH-Group 14 (2048 Bit)**.

c From the **IPsec Policy** drop-down list, select **esp-aes256-sha256**.

17 On the left side of the **Profile Settings** window, select **Advanced IPsec Options**, and perform the following actions:

a In the **Interval** field, enter `20` seconds.

b In the **Number of retries** field, enter 8

c Select the **Anti-replay Protection** check box.

d Select the **Standard IPsec** check box.

18 On the left side of the **Profile Settings** window, select **Certificate Check**, and ensure that the available fields are empty.

19 Click **OK** to save the configuration and close the **Profile Settings** window.

20 Click **OK** to close the **Profiles** window.

21 After configuring the NCP Secure Entry Client, click the red button to establish the connection. Make the IKE Virtual Private Network (VPN) negotiate by sending traffic through the VPN.

a In the **User ID** field, enter the RADIUS user name (for all systems except K) or local user name (K system).

b In the **Password** field, enter the RADIUS user password (for all systems except K) or local user password (K system).

Postrequisites:
After you configure the NCP Secure Entry Client on your laptop, access the ASTRO® 25 system using the VPN tunnel. See Connecting to the System with NCP Secure Entry Client on page 61.

Related Links

Service Access Architecture Required Software and Hardware on page 49

4.7 Service Access Architecture Equipment Configuration

This section describes the configuration of components required for Service Access Architecture.

DMZ Ethernet Switch

Required configuration changes to the De-Militarized Zone (DMZ) Ethernet switch include provisioning and connection of a new physical Ethernet port to the DMZ terminal server. For information about viewing the configuration of a device, see the *Unified Network Configurator* manual.

Firewall

Motorola Solutions enters the firewall rules for your ASTRO® 25 system. You can view firewall rules by using the Web-based manager (GUI), and contact the Motorola Solutions Support Center (SSC) or your system administrator.

Zone Core Protection

For information on Zone Core Protection (ZCP), see the *Zone Core Protection Infrastructure* manual.

Terminal Servers

The following sections provide summaries of terminal server configurations for the Service Access Architecture. For more information, see the *Terminal Servers LX Series* manual.

DMZ Terminal Server (MRV LX-4008)

The DMZ terminal server, by default, authenticates users on the Active Directory (AD) to establish dial-up connections. After a dial-up connection is established, a Virtual Private Network (VPN) connection must be established with the RNI-DMZ firewall.

The DMZ terminal server is also configured to provide local fallback authentication for AD authentication (if the AD is unavailable due to failure).

NOTICE: The serial ports on the LX-4008 terminal server are not connected to console ports of any devices in the DMZ.

Simulcast Prime Site Terminal Server

The Simulcast Prime Site terminal server, by default, authenticates users on the Active Directory (AD) to establish dial-up connections.

The Simulcast Prime Site terminal server is also configured to provide local fallback authentication for AD authentication (if the AD is unavailable due to failure).

Modem Disconnection from Master Site Terminal Servers (if Present)

Any modems (internal or external) connected to Master Site terminal servers must have the Plain Old Telephone Service (POTS) line disconnected. This disconnection is required to prevent direct access to the Radio Network Infrastructure (RNI).

This page intentionally left blank.

Chapter 5

Service Access Architecture Optimization

No optimization procedures are required for the Service Access Architecture feature.

This page intentionally left blank.

Chapter 6

Service Access Architecture Operation

To take full advantage of the Service Access Architecture (SAA) feature, review the information related to the operation of this feature.

- Applications used to establish service connections to the devices in the system
- Access Control Lists (ACLs) for controlling service traffic
- Service operations that can be performed when service access originates from on-demand VPN connections or remote sites

For additional information about operating the software and hardware used for the Service Access Architecture (SAA) service paths, see the relevant documentation for each device.

Related Links

Service Access Architecture Required Software and Hardware on page 49

6.1 Connecting to the System with NCP Secure Entry Client

After you configure the NCP Secure Entry Client on your laptop, use the Virtual Private Network (VPN) tunnel to access the ASTRO® 25 system in the following ways.

Use this procedure only in a system with the Fortinet RNI-DMZ firewall.

Procedure:

1 Right-click on the NCP Secure Entry Client icon in the system tray, select **Connect**. Select the connection that you configured.

   See Service User Accounts Configuration on page 51.

2 Send commands through the VPN.

   Step example: Open a command prompt, and ping a device on the trusted side of the firewall, in the ASTRO® 25 system zone core.
   For more examples, see Available Service Traffic when SAA is Implemented on page 63

Related Links

Configuring the NCP Secure Entry VPN Client for the Fortinet RNI-DMZ Firewall on page 54

6.2 Standard Utilities to Access an ASTRO 25 System

Authorized service personnel can use the following standard utilities to access devices in an ASTRO® 25 system:

Microsoft Windows Remote Desktop Connection
This utility provides remote control of a Windows-based computer (the equivalent to logging in locally to that computer).

VMware vSphere Client

Use this application to share a session on any ESXi-based virtual machine (it can be any virtual machine using Windows Server 2012, such as DC and AuC, or Windows Server 2008 – GMC) with others using the vSphere console. The user and the technician can both launch the VMware vSphere Client, connect to the same virtual machine, and share the session from the vSphere console. For information on how to install and operate the application, see the *Virtual Management Server Software* manual.

PuTTY and PuTTY Key Generator

If required by your administrative policies, you may need to use SFTP instead of FTP, and SSH terminal sessions instead of Telnet. PuTTY is the tool certified for use as an SFTP and SSH client in an ASTRO® 25 system. PuTTY is part of the standard installation on the Network Management (NM) Client, and is available for installation from the ASTRO® 25 system *Windows Supplemental* media. For additional information about using PuTTY tools in an ASTRO® 25 system, see the *Securing Protocols with SSH* manual.

Related Links

Service Access Architecture Required Software and Hardware on page 49

6.3

Access Control Lists Overview

Pre-configured Access Control Lists (ACLs) allow only the traffic on the lists to pass through gateways in the ASTRO® 25 Radio Network Infrastructure (RNI). The ACLs are the same for all ASTRO® 25 system configurations.

Security Rules Enforced by ACLs

The following examples of security rules are enforced by ACLs:

- Traceroute is not permitted in the radio network infrastructure.
- Ping is allowed only between the following sites, only in the following direction:
  - From the zone core to remote sites
  - From dispatch sites to the zone core
  - From one zone core to another zone core
  - From the LAN switch at a Simulcast Prime Site to the Simulcast Remote Subsite
  - In systems with distributed conventional subsystems, from a conduit hub or hub with a conventional site controller to any other hub or base radio site in the same subsystem
  - In systems with Distributed Conventional Hub Sites, from any Hub Site to Conventional Base Radio Sites and trunked RF sites directly connected by ESL tunnels
- Configuration of an RF site device can be performed from outside that site using Motorola Solutions software accessed from a Network Management (NM) Client (or, in K cores, Motorola Solutions software on a service laptop). However, there are restrictions on the devices that Motorola Solutions software can configure remotely, based on system security policies.
- Traffic between two remote sites (RF sites or NM/dispatch sites) is blocked, except in cases where NM/dispatch sites are configured into Trust groups in the ACLs.
- If the sites are not running applications between sites over the InterZone Links (such as logging/ playback stations or MOSCAD Network Fault Management), traffic between sites in different zones can all be blocked or can all be allowed. It is not possible to block selective sites. Blocking traffic between sites in different zones is recommended, .

- Telnet and Secure Shell (SSH) to routers and gateways must originate from NM Clients on a Zone Network Management (ZNM) or User Configuration Server (UCS) subnet. The configuration file enforces this restriction.

ACL Considerations

No configuration of ACLs is required. However, the following considerations are related to ACLs:

- Before you attempt to remotely access a device in the RNI, use the information provided in this section, or contact your system administrator, to determine the network paths available to the device.
- Make a plan for a file transfer that may be required for service, for disaster recovery (restore), or for administrative purposes. If in your system, use the centralized Backup and Restore (BAR) service as a central SFTP server file collection point. From there, the files can be accessed by the Solution Support Center (SSC), or can be downloaded using an SFTP client (PuTTY is available on the NM Client and other Windows-based devices in the ASTRO® 25 system). If there is no BAR Server, set up an SFTP server where files can be collected. Contact the SSC regarding other possibilities for FTP/SFTP servers for file collection. The account name to use for transferring files to the BAR Server is `ftp_user`.

  NOTICE: The password for this account is set up during installation of the BAR Server. For information, see the ASTRO® 25 system *Backup and Restore Services* manual.

6.3.1 Service Access Architecture ACLs for Conventional Subsystems

Traffic originating in one conventional subsystem and destined for another conventional subsystem must go through the zone core, except where trusted group relationships are created between hubs, Access Control Lists (ACLs) block all traffic (except for voice traffic).

Within a conventional subsystem:

- Secure protocols (including Secure Software Download Manager (SWDL), Secure Shell (SSH), SFTP, HTTPS) are allowed:
  - On the hub LAN and Base Radio (BR) site LAN
  - From hubs to BR sites within the conventional subsystem
- Clear protocols (including clear SWDL, Telnet, SNMP, FTP, TFTP, HTTP) are allowed:
  - On the hub LAN and BR site LAN
  - Between any hubs within the conventional subsystem
  - From any hub to its directly tunneled BR sites

6.4 Available Service Traffic when SAA is Implemented

Service Access Architecture (SAA) supports the following origination points for service traffic:

- De-Militarized Zone (DMZ) dial-up
- Remote sites
- Customer Enterprise Network (CEN) through a VPN
- Internet through a VPN

NOTICE: Firewall rules and router Access Control Lists (ACLs) restrict access to devices in the Radio Network Infrastructure (RNI). Active Directory group memberships restrict access to devices that use Centralized Authentication. For information, contact your system administrator.

Related Links

Connecting to the System with NCP Secure Entry Client on page 61

6.4.1 Service Traffic Originating from On-Demand VPN

These service functions can be performed when the service access originates from on-demand VPN connections: dial-up to the SAA modem and terminal server, Customer Enterprise Network (CEN), and Internet.

Table 3: Service Traffic Originating from On-Demand VPN

Service Function	Available Service with SAA
Transfer files from devices in the Radio Network Infrastructure (RNI)	• FTP • SFTP (If Secure Shell (SSH) is implemented in the system, the PuTTY command-line utility on the technician computer or Network Management (NM) client can be used to execute SFTP commands to any devices in the RNI configured as SSH servers. See the ASTRO® 25 system *Securing Protocols with SSH* manual.)
Remote access to devices in the RNI that are configured as SSH servers	Establish an SSH session directly from PuTTY on your laptop or PuTTY on the NM client.
Remote access to the console devices operator position for data collection	Use Windows Remote Desktop Connection on the laptop, or on the NM client.
Ping directly to devices in the RNI	Execute the ping command from the laptop.

6.4.2 Service Traffic Originating from Remote Sites

Table 4: Service Traffic Originating from Remote Sites

These service functions can be performed when the service access originates at Remote Sites.

Service Function	Available Service with SAA
Software Download Manager (SWDL) from a remote site to a remote site	Use the Windows Remote Desktop Connection on the laptop to log in to the Network Management (NM) client and launch the SWDL from the NM client. **NOTICE:** This function is not allowed from an NM client outside the zone core. Use this function to load from a simulcast prime site to subsites.
	Use this function in conventional subsystems between hubs and Base Radio (BR) Sites as described in the Access Control List (ACL) section of this manual.
Configure a remote site where the technician is not located	Use the Windows Remote Desktop Connection on the laptop to connect to the NM client. From the NM client, launch applications to access devices throughout the Radio Network

Table continued…

Service Function	Available Service with SAA
	Infrastructure (RNI), including Configuration/Service Software (CSS) and the Unified Network Configurator. However, restrictions are on the devices that Motorola Solutions software can configure remotely, based on system security policies.
	NOTICE: This function is not allowed from an NM Client outside the zone core.
Telnet and ping	Use the Windows Remote Desktop Connection on the laptop to log on to the NM client. Using a ping from these NM clients to remote sites is allowed, but not from a remote site to a remote site. Direct site to site traffic is not allowed.
	Use telnet from the NM client in the zone core to other devices in the zone core that allow telnet.
Secure Shell (SSH) access (SSH and SFTP) from a remote site to devices configured as SSH servers in the zone core	Establish an SSH session directly from PuTTY on the laptop, or from PuTTY on the NM Client.
Check alarms from the MOSCAD Network Fault Management (NFM) system	Use the Windows Remote Desktop Connection on the laptop to log in to the Graphical WorkStation (GWS).
Use ZoneWatch	Use the Windows Remote Desktop Connection on the laptop to log in to the NM client in the zone core. Launch ZoneWatch from the NM client.
Private Network Management (PNM) functions	Use the Windows Remote Desktop Connection on the laptop to log in to the NM client in the zone core. Perform PNM functions from the NM client.
Access the VoyenceControl client component of Unified Network Configurator **NOTICE:** The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.	Use the Windows Remote Desktop Connection on the laptop to log in to the NM client in the zone core. VoyenceControl can be launched from the browser on the NM client.

This page intentionally left blank.

Chapter 7

Service Access Architecture Troubleshooting

This chapter describes troubleshooting procedures relating to Service Access Architecture.

7.1 Troubleshooting VPN Connections from the CEN or Internet

If a VPN cannot be successfully established when originating from the Customer Enterprise Network (CEN) or Internet, ensure that the local ports on the RNI-DMZ firewall or DMZ switch are working. In other words, connect the service laptop directly to the DMZ VLAN or Internet port on the RNI-DMZ firewall or DMZ switch, and attempt to establish the VPN again. If the VPN can be successfully established, the problem most likely lies in the network configuration outside of the RNI. The configuration of the devices external to the RNI (on the CEN or Internet paths) should be verified. If the VPN cannot be established while locally connected, the initial TNCT configuration of the RNI-DMZ firewall could be the issue.

For more information on port connections, see “RNI-DMZ Firewall Port Connections” in the *Fortinet Firewall* manual.

Related Links

On-Demand VPN Connection to the RNI-DMZ Firewall from the CEN on page 38
On-Demand VPN Connection to the RNI-DMZ Firewall from the Internet on page 39
Accessing Devices from the CEN Through a VPN on page 38
Accessing Devices Through Internet VPNs on page 39

This page intentionally left blank.

Chapter 8

Service Access Architecture Disaster Recovery

If the RNI-DMZ firewall is being recovered and has two-factor tokens provisioned, additional steps need to be performed to regain the functionality of the tokens.

8.1

Recovering Hard Tokens in the RNI-DMZ Firewall

The vpnadmin account is needed to add tokens.

Procedure:

1. Log on to the web-based manager of your Fortinet unit from your computer.
2. Insert the CD labeled *FortiToken 200 Activation File*.
3. In the web-based manager, select **User & Device** → **FortiTokens**, and click **Create New**.
4. For the **Type**, select **Hard Token**, and click **Import**.
5. Select **Seed File**, browse to the **.**FTK file on the CD, and click **OK**.

Any hard tokens that were previously assigned appear as **Assigned** in the FortiToken UI. You do not need to reassign the tokens to users.

Postrequisites:
After making any configuration changes in the RNI-DMZ firewall, pull the RNI-DMZ firewall configuration from the Unified Network Configurator (UNC) to ensure that the configuration can be retrieved in disaster scenarios. For more information, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

8.2

Recovering Mobile Tokens in the RNI-DMZ Firewall

Prerequisites: Ensure that the new firewall is registered. See Registering the RNI-DMZ Firewall on page 43.

Procedure:

1. Submit a Technical Support ticket to the Fortinet support website: https://support.fortinet.com/ to transfer the tokens to the new firewall. In the ticket, include the following information:
   - The FTM License Numbers for each set of mobile tokens. The FTM License Number is the number starting with **FTM** at the bottom of the FortiToken Mobile Redemption Certificate.
   - The serial number of the old firewall equipment
   - The serial number of the new firewall equipment
2. Optional: Verify that the tokens have been transferred to the new firewall:
   a. Ensure that you are connected to the Internet.
   b. On the Fortinet support website, go to **Asset** → **Manage/View Products**.
   c. Select the new firewall serial number.

   d Click **License and Key**.

3 When the new firewall picks up the new registration, perform the following actions:

If…	Then…
If the mobile tokens were previously unassigned,	assign and provision the tokens. See Assigning Mobile Tokens to VPN Users on page 46.
If the mobile tokens were previously assigned,	re-provision the tokens by re-sending the activation codes for users to input into their mobile device. See Assigning Mobile Tokens to VPN Users on page 46. **NOTICE:** In the **Contact Info** area, you do not have to provide any information if the fields are already filled out from the previous provisioning.

Postrequisites:
After making any configuration changes in the RNI-DMZ firewall, pull the RNI-DMZ firewall configuration from the Unified Network Configurator (UNC) to ensure that the configuration can be retrieved in disaster scenarios. For more information, see “Pulling the Configuration for a Single Device” in the *Unified Network Configurator* manual.

Chapter 9

Service Access Architecture Maintenance

This chapter describes periodic maintenance procedures relating to Service Access Architecture.

9.1 Maintenance with a Technician Laptop

The technician is responsible for updating the following software on the laptop:

Microsoft Windows operating system
Install the latest patches and updates

Antivirus software
Maintaining updated virus definitions

The technician is responsible for backing up secure configuration information and secure data according to the policies of the organization.

This page intentionally left blank.

Chapter 10

Service Access Architecture Reference

This chapter contains reference information relating to Service Access Architecture.

10.1 Service Laptop

The Service Laptop or a laptop computer is a valuable tool for most troubleshooting. Use it to obtain information about the functioning of system components and the transport architecture between sites.

Primary uses of Service Laptop include:

- Quick checking of component status, configuration, and reconsideration
- Saving hard and soft copies of all configuration information for a system
- Configuring and servicing base radios with the Configuration/Service Software (CSS) application
- Using Customer Programming Software (CPS) to program subscriber radios

Depending on system configuration, other possible uses include:

- Local configuration and troubleshooting of SDM3000 Network Translator (SNT) and SDM3000 Remote Terminal Unit (RTU) devices using the SDM3000 Builder application.

A Service Laptop may be used to directly troubleshoot, configure, and read local alarm logs for devices in the radio network. The Service Laptop can be used to check the local status of a device, program radios and base stations, and save a backup of device configurations.

10.1.1 Service Laptop Recommended Hardware

The Service Laptop requires the following minimum specifications:

Processor: 1 GHz or higher Pentium grade

Memory:

- 1 GB RAM recommended for Windows 10 32-bit
- 2 GB RAM recommended for Windows 10 64-bit

Hard Disk Space:

- 300 MB minimum free space (for a Typical Installation, including Help Text and Software Download)
- 150 MB minimum free space (for a Compact Installation)

Peripherals:

- Microsoft Windows-supported mouse or trackball
- Microsoft Windows-supported serial port for product communication
- Microsoft Windows-supported Ethernet port for product communication
- Microsoft Windows-supported Printer port for report printing
- Media for software installation

NOTICE: For computers not equipped with a serial port, radio communications may be possible with the use of an off-the-shelf USB-to-RS232 converter.

Service Monitor: Aeroflex 3900 Series service monitor with P25 options installed.

10.1.2 Service Laptop Recommended Software

Install the following software applications on the Service Laptop for site equipment configuration, maintenance, and troubleshooting.

CSS
To configure and troubleshoot the base radios and site controller.

SWDL
To download firmware to the base radios and site controller.

CPS
To program subscriber radios.

Load the Service Laptop with the following software:

- Configuration/Service Software (CSS)
- Customer Programming Software (CPS)
- NCP Secure Entry Client (for systems with Fortinet RNI-DMZ firewalls)
- PuTTY
- Software Download Manager (SWDL)
- Third-party Telnet client
- Windows Remote Desktop

The following operating system is recommended:

- Windows 10 32-bit
- Windows 10 64-bit

The following browser is recommended:

- Microsoft Internet Explorer 11

  NOTICE: While other browsers may suffice (Netscape Navigator version 4.8 or above, Firefox version 2.0 or above, or other), it is best to employ the recommended browser on the service laptop to achieve best performance.

Install the following optional software applications on the Service Laptop:

- SDM3000 Builder - for local configuration and troubleshooting of SDM3000 Network Translator (SNT) and SDM3000 Remote Terminal Unit (RTU) devices.

Install the following software applications if the Service Laptop is connected to a system where 802.1 x authentication is enforced:

- OpenSSL Toolkit - a general-purpose cryptography library used by Certificate Generation and Deployment (CGD) tool for deploying certificates.

Follow the instructions on the installation CDs for each software.