System Release 7.17.x
ASTRO® 25
INTEGRATED VOICE AND DATA

Fortinet Firewall
Feature Guide

SEPTEMBER 2019

MN003272A01-C

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 specific system, or may be dependent upon the characteristics of a specific 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.

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

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 or title of the section with the error
- A description of the error

Document History

Version	Description	Date
MN003272A01-A	Original release of the *Fortinet Firewall Feature Guide*	November 2016
MN003272A01-B	Consolidated for system releases 7.17, 7.17.2, 7.17.3. Includes information about Fortinet 101E: Firewalls Overview on page 12 and Firewalls Hardware Reference on page 48.	July 2019
MN003272A01-C	The following section was updated: Logging into the Firewall Web User Interface on page 43.	September 2019

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About Fortinet Firewall Feature Guide

This manual provides information relating to the implementation and replacement of firewall appliances that Motorola Solutions provides in ASTRO® 25 systems.

For information about managing firewalls in ASTRO® 25 systems, see the *Fortinet Firewall Manager User Guide*.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to www.motorolasolutions.com/training.

Related Information

Refer to the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual. This document may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
Fortinet Firewall Manager User Guide	Provides information on the implementation of server software and user interface supporting Fortinet firewall management in ASTRO® 25 systems.

Chapter 1

Firewalls Overview

A firewall is a network security device providing network boundary enforcement and attack detection. The firewall restricts traffic to known sources, destinations, and protocols, based on the hosts and services that are specified in the firewall configuration. All other traffic that is not defined is discarded.

Table 1: ASTRO® 25 Firewalls

		Fortinet FortiGate Firewall Model	
Firewall Type	**Location**	**101E**	**100D**
RNI-DMZ Firewall	In the De-Militarized Zone (DMZ), between the ASTRO® 25 Radio Network Infrastructure (RNI) and a Customer Enterprise Network (CEN). In ASTRO® 25 cores.	✓	✓
ISSI 8000 Firewall	Between the ASTRO® 25 RNI and other P25-compliant systems supported by the Intersystem Gateway (ISGW)	✓	✓
ISSI.1 Firewall	Between ISSI.1 Network Gateway sites.	✗	✓
Telephony Firewall	A component of the Enhanced Telephone Interconnect (ETI) feature. Used in configurations where the IP PBX Server is connected to an external IP network.	✓	✓
Control Room Firewall	At remote console sites, sub-tended console sites in trunking subsystems, hub sites in a conventional subsystem and hub sites in a K core system. Allows secured communications with outside networks.	✗	✓
Console Site Firewall	Console sites. Provides a secure interface to the zone core.	✗	✓
LMP Firewall	Between the WAVE 5000 network and ASTRO® 25. Provides a secure interface for conventional channels. The LMP Firewall is supported on system releases 7.17.2 and later.	✓	✓
K Core Firewall	K core hub site. Provides a secure interface to the Motorola Solutions Support Center (SSC) and the CEN.	✓	✓
ZCP Firewall	Between the zone core and sites or zone cores in a MultiZone or Dynamic System Resilient configuration. ZCP Firewalls are components of the Zone Core Protection feature.	✗	✓

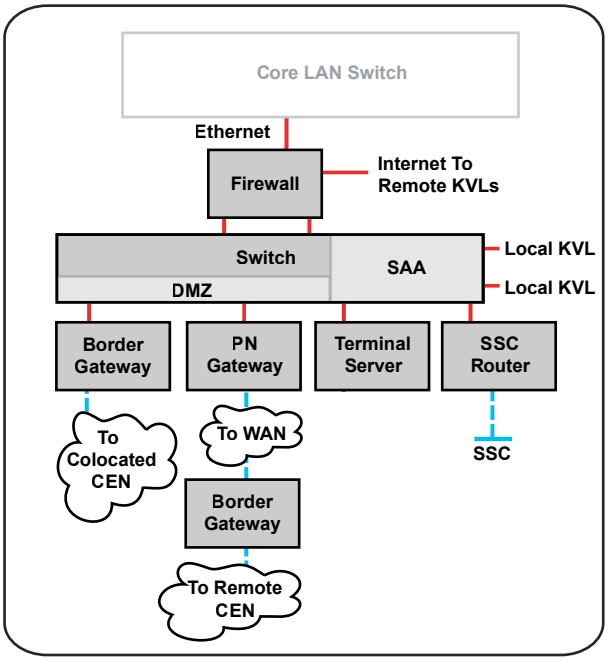
1.1
RNI-DMZ Firewalls

An RNI-DMZ firewall supports traffic flow for a variety of ASTRO® 25 features. This includes traffic that uses the following subnets:

- **DMZ subnet:** See RNI-DMZ Firewall Customer Network Data Traffic on page 14.
- **Service Access Architecture (SAA) subnet:** See RNI-DMZ Firewall Service and Radio Authentication Traffic on page 15.

The diagram below shows an RNI-DMZ firewall connected to a switch in an ASTRO® 25 system DMZ, and to a core LAN switch in the ASTRO® 25 system Radio Network Infrastructure.

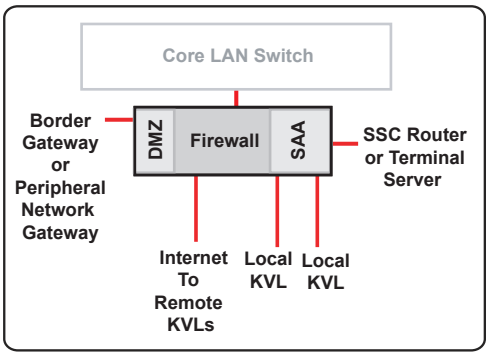
Figure 1: Firewall Connected to a DMZ/SAA Switch



L_M_Core_Firewall_Options_with_Switch_A

The diagram below shows an RNI-DMZ firewall with no DMZ/SAA switch. The firewall connects to a core LAN switch in the ASTRO® 25 system Radio Network Infrastructure.

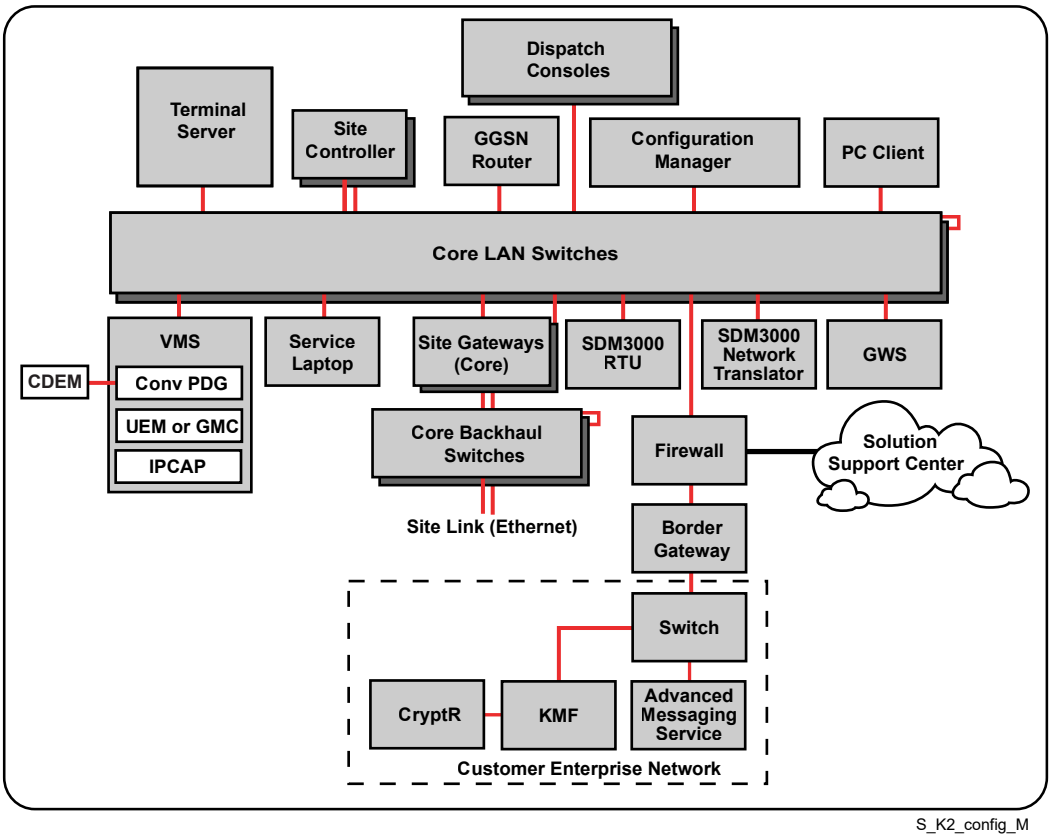
Figure 2: Firewall With No DMZ/SAA Switch



S_Firewall_Option_No_Switch_B

The diagram below shows the RNI-DMZ firewall in an ASTRO® 25 system, connected to a K2 core LAN switches in the Radio Network Infrastructure.

Figure 3: Firewall in ASTRO 25 System K2 Core



1.1.1
RNI-DMZ Firewall Customer Network Data Traffic

One of the subnets of the ASTRO® 25 DMZ is used for traffic between the Radio Network Infrastructure and your organization's Customer Enterprise Network (CEN). Depending on the number of CENs and their location, this may be implemented using one or both of the following tools:

- Border gateway linking directly to a CEN that is co-located with the ASTRO® 25 DMZ
- Peripheral Network (PN) gateway linking through a WAN to a border gateway to a remote CEN (not applicable to firewalls in ASTRO® 25 K core systems)

The firewall in the ASTRO® 25 DMZ allows or denies access to the system network based on the source of the data traffic, the destination, the direction of the traffic flow, and the type of data service. Some of the types of traffic that the firewall allows are:

- Management software to management software (for example, ASTRO® 25 system network fault management application to a manager in your organization's network)
- Packet Data
- Air Traffic Information Access (ATIA)
- Over-the-Ethernet-Keying (OTEK)

NOTICE: Over-the-Ethernet-Keying (OTEK) provides key management for consoles through the Key Management Facility (KMF) which is installed on an external Customer Enterprise Network (CEN). For more information on the OTEK feature, see the *Key Management Facility User Guide*.
Devices that use the KMF and OTEK feature include consoles, Archiving Interface Server (AIS), CAI Data Encryption Module (CDEM) for conventional systems with integrated data, PDEG Encryption Units for trunked systems with integrated data, and Telephony Media Gateways for the Enhanced Telephone Interconnect feature. For more information about these features, see the related ASTRO® 25 system manuals.

For more information about a separate Telephony firewall supporting the Enhanced Telephone Interconnect feature, see Enhanced Telephone Interconnect Firewalls on page 19.

For more information about encryption between the ASTRO® 25 zone core and your organization's CEN, see the *Link Encryption and Authentication Feature Guide*.

1.1.2
RNI-DMZ Firewall Service and Radio Authentication Traffic

The Service Access Architecture (SAA) subnet on an RNI-DMZ firewall supports traffic for the following service functions, if implemented in the system:

- Motorola Solutions Support Center (SSC) traffic that uses an SSC router to access a VPN to the ASTRO® 25 system zone core.
- Service technician traffic that uses an SAA terminal server for remote service technicians to access a VPN to the ASTRO® 25 system zone core.

NOTICE: SAA terminal server (VPN) access for remote users is not supported in ASTRO® 25 systems with K core master site configurations.

When a DMZ/SAA switch is implemented, these devices connect to the switch, and the firewall SAA subnet port connects to the port named "SAA_Firewall" in the switch configuration file.

The SAA subnet on an RNI-DMZ firewall also supports data traffic for Radio Authentication, as explained in the following section.

1.1.3
RNI-DMZ Firewall KVL Data Traffic for Radio Authentication

If the Radio Authentication feature is implemented in an ASTRO® 25 system, the RNI-DMZ firewall is configured to provide a virtual private network (VPN) tunnel for uploading data from Key Variable Loader (KVL) devices to the Authentication Center (AuC) server in the zone core.

NOTICE: The Radio Authentication feature is not supported in ASTRO® 25 systems with K core master site configurations.

Uploading may occur in one or more of the following ways:

- **By connecting KVL devices locally at the DMZ:** If a DMZ/SAA switch is present, one or two KVLs can connect to the "local-VPN" ports on the switch (ports 7 and 8), and the switch connects to the SAA subnet port on the RNI-DMZ firewall.
- **By connecting KVL devices to the DMZ through your organization's service provider:** Your organization can set up a device at the DMZ to provide an Internet connection to remote KVLs (16 simultaneous connections from remote KVLs, for a total of 18 simultaneous KVL connections if 2 KVLs are connected locally at the DMZ). Your organization's device at the DMZ connects directly to the RNI-DMZ firewall.
- **By connecting KVL devices to the DMZ through the Motorola Solutions Support Center (SSC) interface:** If Internet access used by the SSC already exists in the system, it can also be

used for remote KVL access to the DMZ (16 simultaneous connections from remote KVLs, for a total of 18 simultaneous KVL connections if 2 KVLs are connected locally at the DMZ).

If a KVL connection is made (locally or remotely), a preshared key on the RNI-DMZ firewall must match a preshared key on each KVL.

The RNI-DMZ firewall ports used for these connections are listed in RNI-DMZ Firewall Port Connections on page 26.

For instructions for determining your switch port assignments, see the *Ethernet LAN Switches Feature Guide*.

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

1.1.4
RNI-DMZ Firewall Dynamic System Resilience

The ASTRO® 25 system Dynamic System Resilience (DSR) feature adds a geographically separate backup for a master site to protect against a catastrophic failure. Each zone in the DSR system is supported by two cores in two separate master sites. The backup core provides redundancy for most of the functionality offered by the primary core.

In systems with the DSR feature, an RNI-DMZ firewall is implemented at the primary core Master Site and at the backup core Master Site. The DSR feature with connectivity to a Customer Enterprise Network (CEN) requires a minimum of two RNI-DMZ firewalls.

The following applies if a system with DSR also includes the Radio Authentication feature, and is configured for remote access to the DMZ by the Key Variable Loader (KVL). In a failure scenario where the RNI-DMZ firewall is not operating, the IP address for a different Remote Gateway can be entered in the KVL user interface, to enable a remote KVL connection to a working DMZ at a different DSR master site (not the one that failed). See instructions for configuring a VPN in the documentation for your KVL.

1.1.5
RNI-DMZ Firewalls Monitoring Considerations

The ASTRO® 25 fault management system may not monitor all of the network security devices between the RNI and your organization's Customer Enterprise Network (CEN). Therefore, consider taking the following actions:

- Monitoring the health of the firewall devices by using the Network and Security Manager user interface application
- Monitoring network security devices as part of your enterprise network monitoring and fault management
- Providing the Motorola Solutions Support Center (SSC) with remote access to the network security devices
- Providing a system administrator or other point of contact who can assist SSC in determining the source of a fault between the radio network and your CEN

1.1.6
RNI-DMZ Firewall High Availability

To enable high availability and automatic switchover (High Availability for Trunked IV&D and HPD feature) in case of a component failure, redundant firewalls are implemented in ASTRO® 25 cores.

The High Availability for Trunked IV&D and HPD feature requires installing two redundant DMZ firewalls in a single Master Site and configuring them for High Availability. In systems with High Availability and DSR, a total of four DMZ firewalls are installed (two in each Master Site).

NOTICE: In High Availability configurations, the firewall only supports one port for local Key Management through the KVL.

1.2
ISSI 8000 Firewall

The ISSI 8000/CSSI 8000 feature regulates network traffic between the ASTRO® 25 RNI and other P25-compliant systems supported by the ISSI/CSSI 8000.

To support this feature, a firewall is added at the zone core to forward traffic between the core and other P25-compliant systems.

The firewall uses Network Address Translation (NAT) to map internal Intersystem Gateway (ISGW) IP addresses to the external IP addresses and the other way around. An Ethernet port on the firewall connects to the external network.

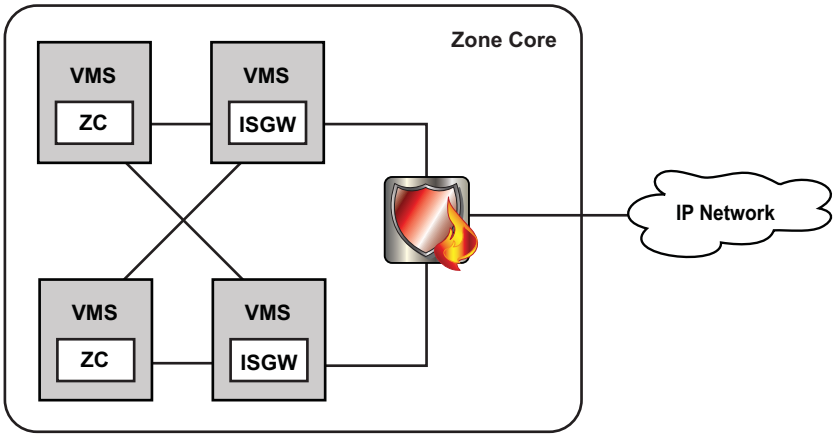
The ISSI 8000/CSSI 8000 feature may require replacing the existing Telephony Firewall with the Fortinet FortiGate firewall only if both Telephony and ISSI 8000 are supported by this firewall. See Enhanced Telephone Interconnect Firewalls on page 19.

ISSI 8000 Firewall in a Non-DSR System

In a system without Dynamic System Resilience (DSR), one firewall is supported at the system level. If Zone Controller (ZC) is redundant, two ISGWs can be implemented in the zone core as an alternative optional configuration. If ZC is not redundant, only one ISGW is supported.

Figure 4: ISSI 8000 Firewall in a Non-DSR Zone Core

The diagram shows a non-DSR core with Zone Controller redundancy and an optional redundant ISSI 8000/CSSI 8000 configuration

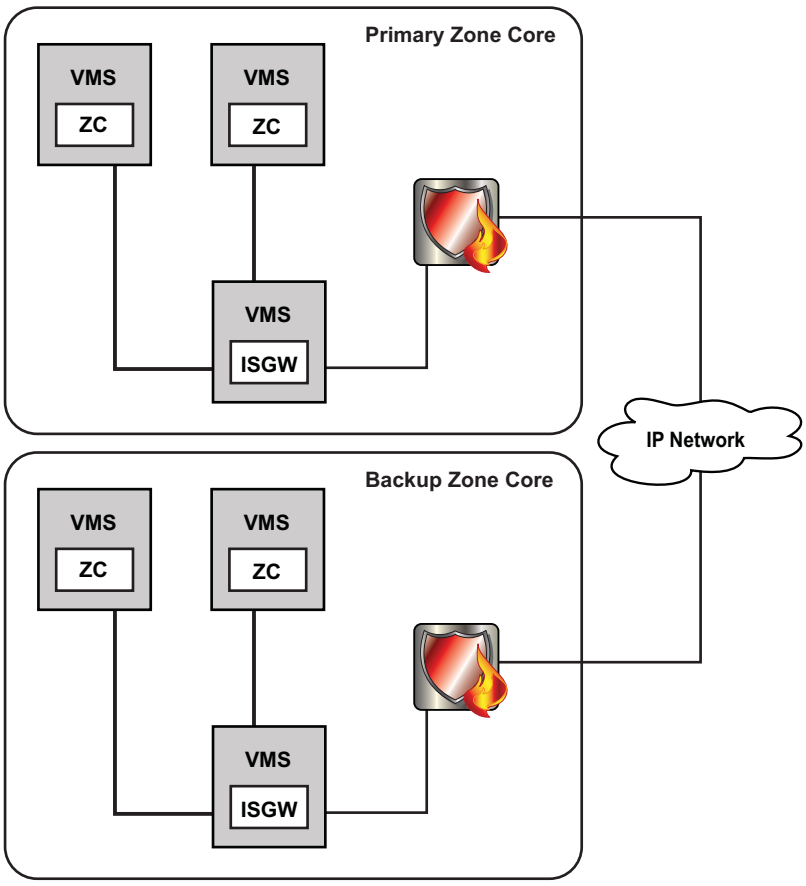


ISSI 8000 Firewall in a DSR System

In a DSR system, two firewalls are supported at a system level: one in the primary core, and one in the backup core. There is one ISGW in each core.

Figure 5: ISSI 8000 Firewall in a DSR Zone Core

The diagram shows DSR cores with Zone Controller (ZC) redundancy. If ZC redundancy is not implemented, there is one ZC in each DSR core.



For details of ASTRO® 25 system configurations for the ISSI 8000 feature, see the *ISSI 8000/CSSI 8000 Intersystem Gateway Feature Guide*.

ISSI 8000 Firewall in WAVE to ASTRO 25 Trunking Interface

For trunking systems, the WAVE 5000 interface uses the ISSI 8000 interface on the ISSI 8000 firewall.

ZCP Firewall ISSI 8000/CSI 8000 Information

If Zone Core Protection (ZCP) is implemented, the ISSI 8000/CSSI 8000 feature requires loading new configurations provided by Motorola Solutions for the ZCP firewalls (to allow traffic between the ISGW and the remote sites). See Loading/Restoring a Firewall Configuration Locally with PSCP on page 37 or Loading/Restoring a Firewall Configuration with WebUI on page 38.

For information on the ZCP firewalls, see the ASTRO® 25 system *Zone Core Protection Infrastructure Feature Guide*.

1.3 ISSI.1 Firewall

At least one firewall is required at each ISSI.1 Network Gateway site. One firewall can support up to five ISSI.1 Network Gateway servers.

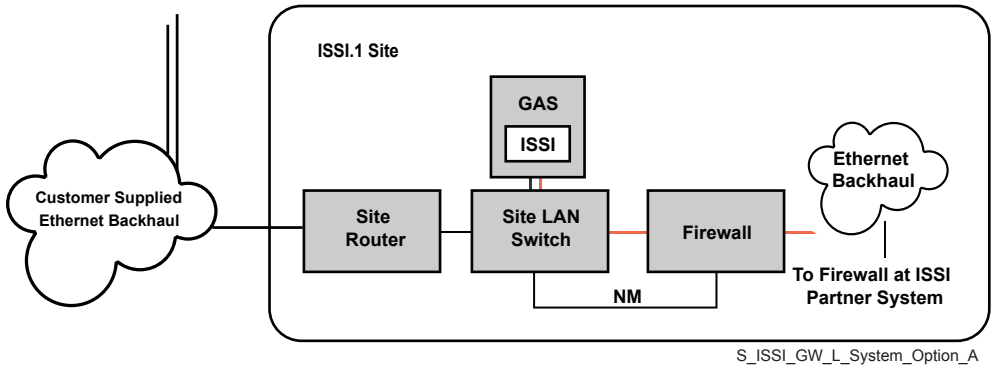
The main function of the ISSI.1 Network Gateway firewall is to permit traffic into the local radio network from another trusted system. At the same time, the firewall blocks all other, unwanted traffic. That is why the tunnel endpoints between systems originate and terminate on the firewalls. Voice and control are both transported over the same physical connection and routed to the peer RF gateway, but they are logically separate. ISSI SIP (Session Initiation Protocol) is used for control transport, and ISSI RTP (Real Time Transport Protocol) is used for voice transport. Both the SIP and ISSI use standard defined interfaces.

ISSI.1 Network Gateway site firewalls are installed and configured the same as other firewalls in the ASTRO® 25 system (see Installing Firewall Hardware on page 24).

- In an ASTRO® 25 system with an M3 (multi-zone capable) master site, all firewalls, including ISSI.1 Network Gateway site firewalls, are managed using the Firewall Management Server and its Windows-based user interface.
- In systems with M1, M2, L1 and L2 master sites, a Firewall Management Server is not required. The web user interface on the firewalls can be used to configure and manage the firewalls.

The following figure shows a firewall in an ISSI.1 Network Gateway Site, connecting to a firewall in an ISSI partner system.

Figure 6: Firewall Between ISSI.1 Network Gateway Sites



1.4

Enhanced Telephone Interconnect Firewalls

In ASTRO® 25 systems with the Enhanced Telephone Interconnect (ETI) feature, a Telephony Firewall must be implemented to prevent security threats from external IP networks, only for configurations where the IP PBX Server connects to landline users over an external IP network.

Telephony Firewall Overview

The Fortinet FortiGate Telephony Firewall clears the following communications:

- SIP Call Control between the IP PBX and the external IP network (IP PBX, SIP-based media gateway) over UDP
- RTP Voice Transmission between the Telephone Media Gateways and the VoIP Endpoints over UDP

RNI-DMZ Firewall Enhanced Telephone Interconnect Information

If a Key Management Facility (KMF) server in the Customer Enterprise Network (CEN) and Over-The-Ethernet-Keying (OTEK) is used for keying Telephone Media Gateways, an RNI-DMZ firewall is also required for the Enhanced Telephone Interconnect feature.

- If the RNI-DMZ firewall does not exist in the system, you can install and configure it using the Installing Firewall Hardware on page 24.

- If the RNI-DMZ firewall exists in the system and is configured for OTEK from a KMF, its configuration already supports the Enhanced Telephone Interconnect feature.

ZCP Firewall Enhanced Telephone Interconnect Information

If Zone Core Protection (ZCP) is implemented, the Enhanced Telephone Interconnect feature requires loading new configurations provided by Motorola Solutions for the ZCP firewalls. See Loading/ Restoring a Firewall Configuration with WebUI on page 38.

For information on the ZCP firewalls, see the *Zone Core Protection Infrastructure Feature Guide*.

ISSI 8000 Firewall Enhanced Telephone Interconnect Information

If the ISSI 8000/CSSI 8000 feature is implemented, the Enhanced Telephone Interconnect feature requires loading new configurations provided by Motorola Solutions for the ZCP firewalls. See Loading/ Restoring a Firewall Configuration with WebUI on page 38.

1.5 Other Firewalls in the ASTRO 25 System

Other firewalls supported in the ASTRO® 25 system include:

Control Room firewall
The control room firewall is used at a console site to allow secured communications with outside networks.

Console Site firewall
The console site firewall prevents unauthorized communications between the dispatch console and the zone core.

LMR Multicast Proxy (LMP) firewall
The LMP firewall is used specifically to separate the WAVE 5000 network from the ASTRO® 25 network.

These firewalls are optional devices that increase ASTRO® 25 system safety. You can install them in one of the following configurations, depending on the policy of your organization:

- Control room firewall and console site firewall
- LMP firewall and console site firewall
- A single firewall per site

MCC 7500E Dispatch Console Considerations

The networking equipment used to establish a path to a remote Dispatch Console is provided by the user. The PRX 7000 Console Proxy communicates to the remote dispatch console through a firewall located at the console site to allow traffic to/from the PRX 7000 Console Proxy and CEN.

For more information, see the *MCC 7500E Dispatch Console User Guide*.

1.5.1 Control Room Firewall

The control room firewall allows secured communications with outside networks.

Control room firewall is configured for Network Address Translation (NAT) functionality to help eliminate conflicts between an IP address in a Customer Enterprise Network (CEN) and an IP address in the ASTRO® 25 system RNI. The control room firewall is configured to only allow dispatch console related traffic to and from the CEN.

The firewall in the CEN and the control room firewall share the link from the console site to the zone core.

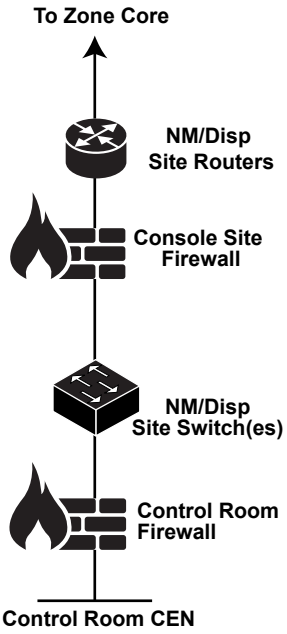
The control room firewall is the demarcation point for the ASTRO® 25 network.

A control room firewall can be installed in the following locations:

- Remote console site
- Sub-tended console site in a trunking subsystem (Tsub)
- Hub site in a conventional subsystem
- Hub site in a K core system (cannot be located at the first hub site that has an RNI/DMZ Firewall)

There can only be one control room firewall for a site.

Figure 7: Single Router Network with both Control Room FW and Console Site FW



Console_Site_FW_and_Control_Room_FW_Single_Router_A

1.5.2
Console Site Firewall

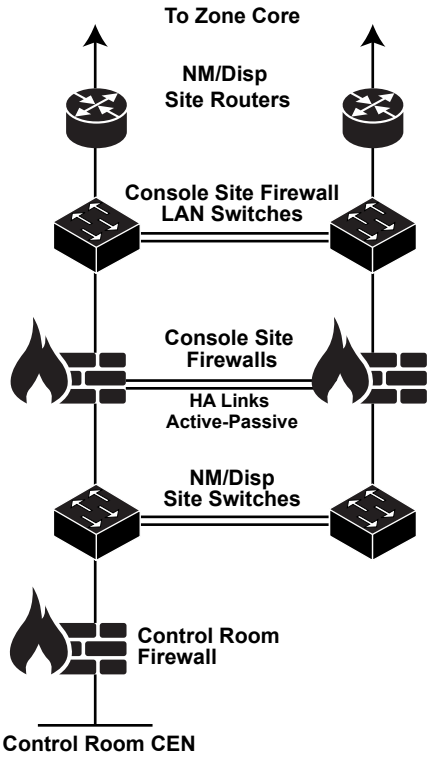
The console site firewall prevents unauthorized communications between the dispatch console and the zone core. It is an optional device that increases ASTRO system safety.

The console site firewall is a further layer of security in the ASTRO® 25 system. It only allows secure communications between the dispatch console and the zone core.

The console site firewall can only be installed at console site.

The console site firewall supports HA (High Availability). This means that if one component fails, a redundant backup component takes its place. To implement the HA configuration, you need console site firewall LAN switches.

Figure 8: Dual Router Network with both Control Room FW and Console Site FW



Console_Site_FW_and_Control_Room_FW_Dual_Router_A

The console site firewall is not supported with Edge Availability (Tsub) configuration or in K core.

1.5.3
LMP Firewall

An LMR Multicast Proxy (LMP) firewall is the control room firewall used specifically to separate the WAVE 5000 network from the ASTRO® 25 network.

The LMP firewall is placed between the Land Mobile Radio (LMR) Multicast Proxy (LMP) on the ASTRO® 25 side and the WAVE Radio Gateway (WRG) on the WAVE 5000 side.

This firewall is an optional device that increases ASTRO® 25 system safety.

The following figures show the LMP firewall in the context of the NM/Dispatch/Conventional site.

Figure 9: Single Router Network with LMP Firewall - Clear Scenario

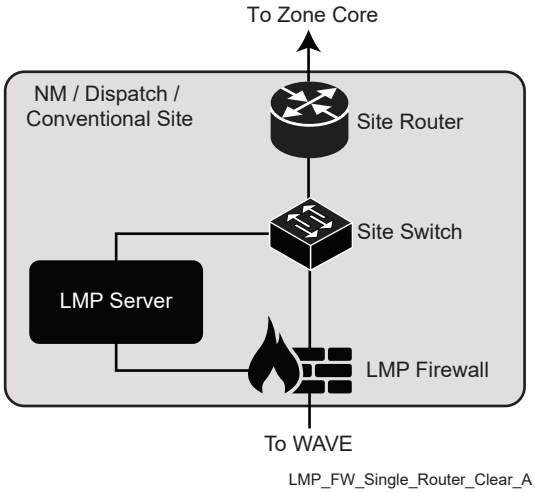
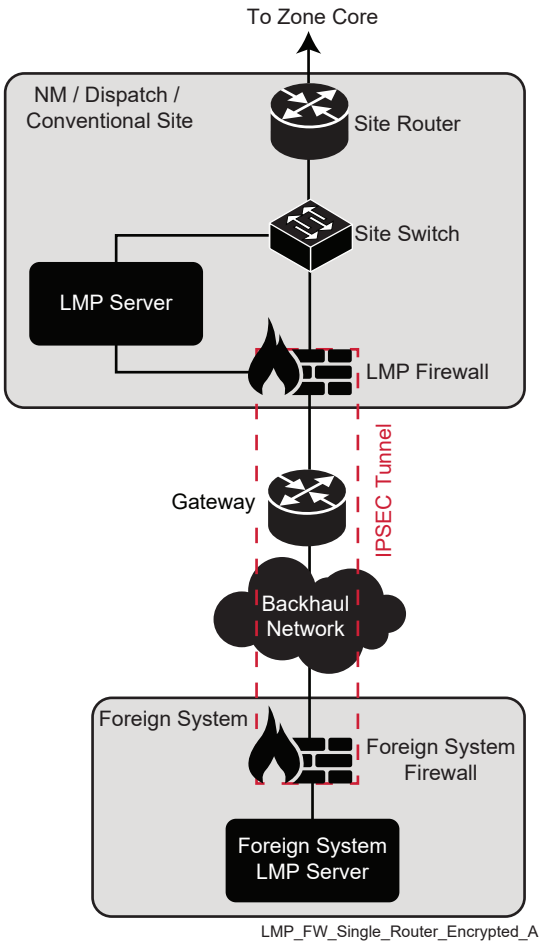


Figure 10: Single Router Network with LMP Firewall - Encrypted Scenario



For more information, see the *WAVE 5000 – ASTRO 25 Console Site Proxy Feature Guide*.

Chapter 2

Firewall Hardware Installation

2.1 Installing Firewall Hardware

This process applies to the firewalls present in the ASTRO® 25 systems except for the Zone Core Protection (ZCP) firewalls.

For information on the ZCP firewalls, see the *Zone Core Protection Infrastructure Feature Guide*. During the initial firewall implementation, Motorola Solutions configures the firewall interfaces and policies. In case of a firewall failure, the interfaces and policies configuration can be restored from the firewall backup.

Prerequisites: Read the information about the firewall that you are going to install in the Firewalls Overview on page 12 section.

Process:

1. Install the firewall hardware. See Rack Mounting Firewalls on page 24.
2. Ground the firewall unit chassis. See Grounding the Firewall Chassis on page 25.
3. Connect devices to the firewall ports by referring to one of the following sections:

   IMPORTANT: To prevent the cables from dislodging or developing stress points, they should be arranged as follows:

   - The cable should not support its own weight as it hangs to the floor.
   - The excess cable should be coiled in a neat loop.
   - Fasteners should be used to maintain the shape of cable loops.

   - For Radio Network Infrastructure (RNI) De-Militarized Zone (DMZ) firewalls, see RNI-DMZ Firewall Port Connections on page 26.
   - For Inter-RF Subsystem Interface 8000 (ISSI 8000) firewalls, see ISSI 8000 Firewall Port Connections on page 29.
   - For the ISSI.1 firewall, see ISSI.1 Network Gateway Site Firewall Port Connections on page 29.
   - For Enhanced Telephone Interconnect (ETI) firewalls, see Telephony Firewall Port Connections on page 30.
   - For Control Room firewalls, see Control Room Firewall Port Connections on page 31.
   - For Console Site firewalls, see Console Site Firewall Port Connections on page 31.
   - For LMR Multicast Proxy (LMP) firewalls, see LMP Firewall Port Connections on page 32.
4. Apply power to the firewall. See Applying Power to Firewalls on page 32.

2.1.1 Rack Mounting Firewalls

The firewall unit can be placed on any flat surface or mounted in any standard 19 in (48.3 cm) rack unit.

For additional information on the FortiGate firewalls installation, see the Fortinet documentation.

CAUTION:
To avoid personal injury or damage to the unit, two or more people should install the firewall unit into the rack.

Electrostatic discharge (ESD) can damage the firewall unit.

Do not place heavy objects on the firewall unit.

Prerequisites: Collect the following provided items:

- Screws
- Rack-mount brackets

Procedure:

1. Ensure that the firewall unit is placed on a stable surface.
2. By using the screws, perform one of the following actions:
   - For four-post racks, attach the rack-mount brackets to the sides of the unit with the handles aligned with the front of the unit.
   - For two-post racks, attach the rack-mount brackets to the sides of the unit with the handles aligned with the middle of the unit.
3. Position the firewall unit in the rack ensuring that there is enough space around the unit to allow for sufficient air flow.
4. Line up the rack-mount bracket holes to the rack holes and ensure that the firewall unit is level.
5. Attach the firewall unit to the rack by finger-tightening four rack-mount screws.
6. Ensure that the spacing around the firewall unit conforms to the Fortinet requirements and that the unit is level.
7. By using a screwdriver, tighten the rack-mount screws.

2.1.2
Grounding the Firewall Chassis

You must ground the firewall chassis adequately before power is connected to meet the safety and electromagnetic interference (EMI) requirements and to ensure proper operation.

CAUTION: Before device installation begins, a licensed electrician must attach a cable lug to the grounding cable you supply. A cable with an incorrectly attached lug can damage the device (for example, by causing a short circuit).

Prerequisites:
Obtain an American Wire Gauge (AWG) number 14 single-strand wire cable that handles up to 6 amperes (A).

Procedure:

1. Connect the grounding cable to the ground.
2. Attach the cable to the lug on the rear of the chassis.

2.1.3
RNI-DMZ Firewall Port Connections

This section shows the Radio Network Infrastructure (RNI) De-Militarized Zone (DMZ) firewall port connections.

FortiGate Firewall Reference

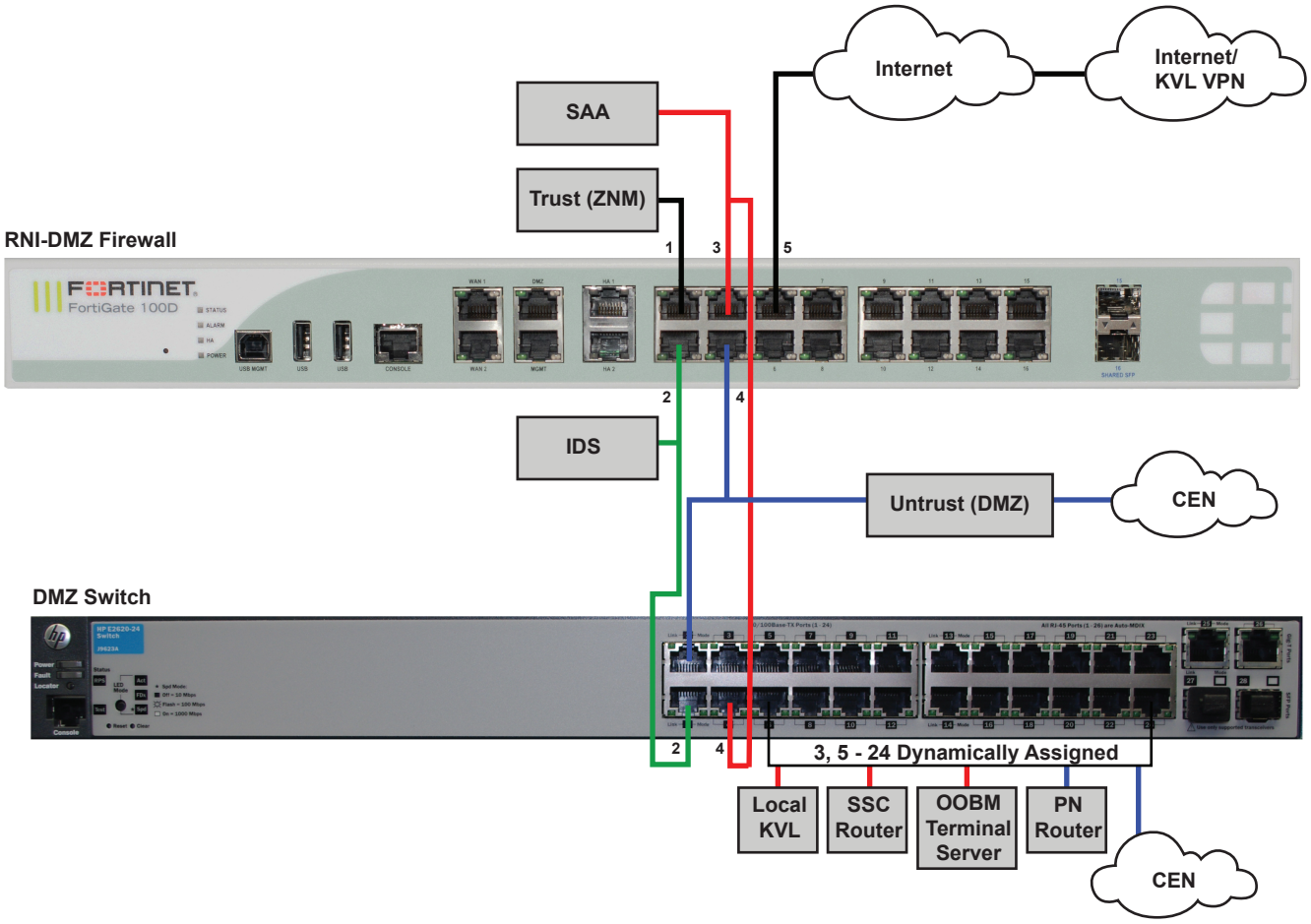
Table 2: RNI-DMZ Firewall Port Connections for Master Sites

Port	Connects to
USB Management	Not supported.
USB	Not supported.
CONSOLE RJ45	Service laptop for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter.
	Terminal for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
2 x GE RJ45 WAN	Not supported.
GE RJ45 DMZ	Not supported.
GE RJ45 Management	Core LAN Switch
2 X GE RJ45 HA	Peer RNI-DMZ redundant firewall
Port 1	Core LAN switch (Trust Interface). For more information, see the figures following this table.
Port 2	IDS (Optional)
Port 3	SAA subnet port on the DMZ/SAA switch (the port named `SAA_Firewall` in the switch configuration file), or if no DMZ/SAA switch is present, this port connects directly to one of the following devices: • Motorola Solutions Support Center (SSC) router, if present • SAA terminal server, if present (not the same as a terminal server in the core) For supported functions, see: RNI-DMZ Firewall Service and Radio Authentication Traffic on page 15. If more than one of the devices listed in this row is required, one solution is to add a DMZ/SAA switch. In that case, the devices connect to the switch, and this SAA subnet port on the firewall connects to the port named “SAA_firewall” in the switch configuration file. Another solution is to connect one of the devices above to additional firewall ports when DMZ switch is not present. The SAA terminal server does not apply for a firewall in an ASTRO® 25 system K core. Service Laptop can be connected here for local VPN service access.
Port 6	Connects to External Facing LAN or the DSR External Facing LAN in the Core LAN Switch.
Port 7 – 9	Additional SAA subnet ports on the DMZ firewall when no DMZ switch is present (when DMZ switch is not selected in the TNCT tool). Local KVLs in the

Port	Connects to
	DMZ (only if Radio Authentication feature is implemented, which is not supported in K core systems). For more information, see RNI-DMZ Firewall KVL Data Traffic for Radio Authentication on page 15. Service Laptop can be connected here for local VPN service access.
Port 4	DMZ subnet port on the DMZ/SAA switch (the port named `Firewall` in the switch configuration file), or if no DMZ/SAA switch is present, this port connects directly to one of the following, if present: • Border gateway to a colocated customer's network • Peripheral Network gateway linking over a WAN to a remote border gateway to a customer network (does not apply for RNI-DMZ firewalls in an ASTRO® 25 system K core) For supported functions, see RNI-DMZ Firewall Customer Network Data Traffic on page 14. **NOTICE:** If more than one of the devices listed in this row requires a connection to the firewall, the solution is to add a switch. In that case, the devices connect to the switch, and this DMZ subnet port on the firewall connects to the port named “Firewall” in the switch configuration file. Service Laptop can be connected here for local VPN service access.
Port 10 – 16	Additional DMZ subnet ports on the DMZ firewall when no DMZ switch is present (when DMZ switch is not selected in the TNCT tool). Service Laptop can be connected here for local VPN service access.
Port 5	Connects to customer-provided device for Internet access to remote KVLs (only if Radio Authentication feature is implemented, and the SAA subnet port is not used for this purpose instead). For more information, see RNI-DMZ Firewall KVL Data Traffic for Radio Authentication on page 15. Service Laptop can be connected here for local VPN service access.
2 x GE SFP Shared Ports	Not supported.

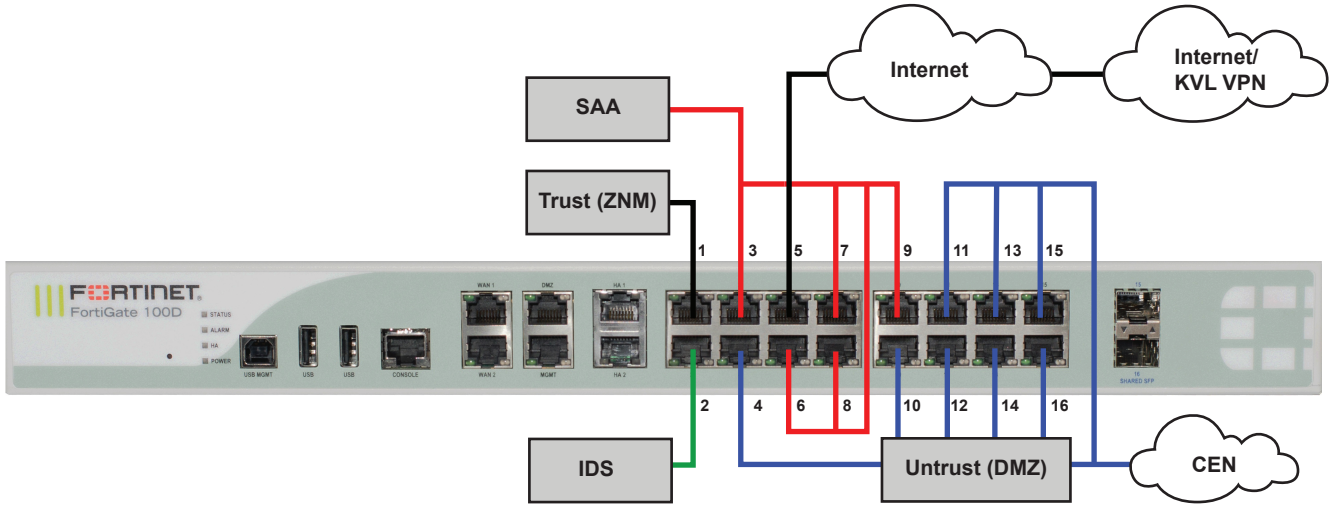
FortiGate Firewall in ASTRO® 25 System

Figure 11: FortiGate Firewall with DMZ Switch



ASTRO_FortiGate_1000D_Firewall_with_DMZ_A

Figure 12: FortiGate Firewall without DMZ Switch



ASTRO_FortiGate_1000D_Firewall_without_DMZ_A

2.1.4
ISSI 8000 Firewall Port Connections

Table 3: ISSI 8000 Firewall Port Connections

Port	Connects to
USB Management	Not supported.
USB	Not supported.
CONSOLE RJ45	Service laptop, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter.
	Terminal, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
WAN1	Not supported.
WAN2	Not supported.
DMZ	Not supported.
HA1	Not supported.
HA2	Not supported.
Port 1	• The core LAN switch (its allocation is dynamic) • The Radio Network Infrastructure (RNI) side in the Telephony subnet Speed duplex is 100-full
Port 2	Disconnected, unless the Telephony firewall feature is present, in which case it is connected to an external IP network. Speed duplex is 100-full
Port 3	• The backhaul switch (its allocation is dynamic) • Wide Area Network (WAN) to communicate to remote systems Speed duplex is auto/auto
Other Ethernet ports	Not supported.

2.1.5
ISSI.1 Network Gateway Site Firewall Port Connections

This table lists the ISSI.1 Network Gateway port connections.

IMPORTANT: Arrange the cable as follows to prevent it from dislodging or developing stress points:

- Secure the cable so that it is not supporting its own weight as it hangs to the floor.
- Place excess cable out of the way in a neatly coiled loop.
- Use fasteners to maintain the shape of cable loops.

Table 4: Firewalls Between ISSI.1 Network Gateway Sites – FGT100D Port Connections

Port	Connects To:
USB Management	Not supported in ASTRO® 25 systems.
USB	Not supported in ASTRO® 25 systems.

Port	Connects To:
CONSOLE RJ45	Service laptop, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter. Terminal, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
WAN1	Not supported in ASTRO® 25 systems.
WAN2	Not supported in ASTRO® 25 systems.
HA1	Use is not supported in ASTRO® 25 systems.
HA2	Use is not supported in ASTRO® 25 systems.
Port 1	ISSI partner System
Port 2	ISSI Gateway 1 LAN Switch
Port 3 – 16	Additional ISSI Gateway (if present)
MGMT	Core LAN Switch
DMZ	Not supported in ASTRO® 25 systems.

2.1.6
Telephony Firewall Port Connections

Table 5: Telephony Firewall Port Connections

Port	Connects to
USB Management	Not supported.
USB	Not supported.
CONSOLE RJ45	Service laptop, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter.
	Terminal, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
WAN1	Not supported.
WAN2	Not supported.
DMZ	Not supported.
HA1	Not supported.
HA2	Not supported.
Port 1	Telephony subnet on the core LAN switch (Trust).
Port 2	External IP network.
Other Ethernet ports	Not supported.

2.1.7
Control Room Firewall Port Connections

Table 6: Control Room Firewall Port Connections

Port	Connects to
USB Management	Not supported.
USB	Not supported.
CONSOLE RJ45	Service laptop, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter.
	Terminal, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
WAN1	Not supported.
WAN2	Not supported.
DMZ	Not supported.
HA1	Not supported.
HA2	Not supported.
Port 1	The NM/Dispatch or Conventional Hub site LAN switch. It is also the trust interface within the Radio Network Infrastructure (RNI).
Port 2	A customer-provided device for remote access to MCC 7500E Dispatch Consoles located outside the RNI.
Other Ethernet ports	Not supported.

2.1.8
Console Site Firewall Port Connections

Table 7: Console Site Firewall Port Connections

Port	Connects to
USB Management	Not supported.
USB	Not supported.
CONSOLE RJ45	Service laptop, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter.
	Terminal, for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
WAN1	Not supported.
WAN2	Not supported.
DMZ	Not supported.
HA1	Supported in HA (High Availability) configuration. Connects to backup firewall HA2 port.
HA2	Supported in HA configuration. Connects to backup firewall HA1 port.
Port 1	An NM/Dispatch or Conventional Hub site LAN switch It is also the trust interface within the Radio Network Infrastructure (RNI).

Port	Connects to
Port 2	A Console Firewall LAN Switch port 5.
Other Ethernet ports	Not supported.

Table 8: Console Firewall LAN Switch Port Connections

Port	Connects to
Port 1	Site Router port 1
Port 5	Console site firewall port 2

2.1.9
LMP Firewall Port Connections

The WAVE – ASTRO® 25 Console Site Proxy employs the LMR Multicast Proxy (LMP) firewalls.

Table 9: LMP Firewall Port Connections

Port	Connects To:
USB Management	Not supported.
USB	Not supported.
CONSOLE RJ45	Service laptop for local administration. Connect using an RJ-45 to DB-9 (female-to-male) serial cable with a null modem adapter.
	Terminal for local administration. Connect using an RJ-45 to DB-9 (female-to-male) straight-through serial cable.
WAN1	Not supported.
WAN2	Not supported.
DMZ	Not supported.
HA1	Not supported.
HA2	Not supported.
Port 1	The LMP firewall.
Port 2	The WRG/WAVE 5000 Server. If encryption is used, the port connects to Remote Gateway towards WRG/WAVE 5000.
Ports 3-16	Not used.
Management (MGMT)	Site LAN switch.

2.1.10
Applying Power to Firewalls

Perform this procedure to connect power to the firewall unit.

IMPORTANT: To meet safety and electromagnetic interference (EMI) requirements, and to ensure proper operation, ground the firewall chassis adequately. The AC power cord shipped with the device connects the device to earth ground when plugged into an AC grounding-type power outlet. The device must be connected to earth ground during normal operation.

Prerequisites: Collect the provided power cords.

Procedure:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strip to the ESD point on the chassis.
2. By using the power cords, perform one of the following actions:
   - If the firewall unit has a single power supply, plug the power cable to the unit and connect the other end of the cable to a power source.
   - If the firewall unit has a redundant power supply, plug the power cables to the unit and connect the other end of each cable to a different power source.

   In a redundant power supply configuration, if one power source fails, the other may still provide power to the firewall unit.
3. Verify that the power cord does not block access to device components or drape where people can trip on it.

Chapter 3

Firewall Software Installation

3.1 Installing Firewall Software

All Fortinet firewalls are shipped from the factory with firmware pre-installed. To prepare a firewall for operation, you must upgrade or downgrade its software to match your system.

Prerequisites:
Obtain:

- A service laptop with a TFTP server installed
- An Ethernet cable

Review the *Supported Upgrade Paths for FortiOS Firmware* document on the Fortinet website.

Process:

1. Perform one of the following actions:
   - If your upgrade or downgrade path is supported and telnet/TFTP is disabled on the firewall, load the firmware by using PSCP. See Loading Firewall Firmware Locally with PSCP on page 34.
   - If your upgrade or downgrade path is supported and telnet/TFTP is enabled on the firewall, load the firmware by using WebUI. See Loading Firewall Firmware Locally with WebUI on page 35.
   - If your upgrade or downgrade path is not supported, perform a clean install of the firewall firmware. See Clean Installing the Firewall Firmware on page 36.
2. Perform one of the following actions:
   - If telnet/TFTP is disabled on the firewall, load the firewall configuration file by using PSCP. See Loading/Restoring a Firewall Configuration Locally with PSCP on page 37.
   - If telnet/TFTP is enabled on the firewall, load the firewall configuration file by using WebUI. See Loading/Restoring a Firewall Configuration with WebUI on page 38.

     IMPORTANT: For High Availability (HA) firewalls, some configuration parameters cannot be overwritten when a HA firewall configuration is loaded through PSCP, WebUI, or UNC. Configuration changes in HA mode can be performed manually by using CLI or WebUI, but are not recommended.
3. Configure the firewall for other systems and functionalities. See Completing the Fortinet Firewall Configuration on page 39.

3.1.1 Loading Firewall Firmware Locally with PSCP

Perform this procedure to upgrade or downgrade the firewall firmware if telnet/TFTP is disabled on the firewall.

Prerequisites:
Ensure that the following conditions are met:

- SSH (ssh and scp) is enabled on the firewall. This is a part of the configuration provided by Motorola Solutions.
- PuTTY is installed on the laptop.

Procedure:

1. Perform one of the following actions:
   - If the Motorola Solutions configuration file is loaded on the firewall, open the command prompt on an NM Client. Go to step 3.
   - If the Motorola Solutions configuration file in not yet loaded on the firewall (for example, when replacing the firewall), open the command prompt on a service laptop connected to the MGMT port on the firewall. Go to step 2.
2. Configure the laptop with the IP address matching the subnet of the MGMT IP address of the firewall.

   The factory default IP address on the firewall is 192.168.1.99.
3. Copy the firewall firmware file to NM Client or service laptop.
4. Navigate to the PuTTY directory.

   Step example: If you installed PuTTY from the ASTRO® 25 system *Windows Supplemental* media, at the prompt, enter:
   `cd Program Files (x86)\Motorola\Motorola PuTTY\Bin`
5. From the PuTTY directory, enter:
   `pscp -scp <firewall image><username>@<IP address of fortigate>:fgt-image`

   where `<username>` is the administrator account for the firewall (the default firewall administrator account is `admin`).
6. When prompted, enter the password for the administrator account on the firewall.
7. After firewall comes up after automatic reboot, verify the correct version of the firewall OS by entering: `get system status | grep -i version`

3.1.2
Loading Firewall Firmware Locally with WebUI

Prerequisites:
Obtain the user name and password of the firewall administrator from your system administrator.

Ensure that the “manage web” is enabled on the Trust interface.

Procedure:

1. Open a WebUI connection and log in to the firewall. See Logging into the Firewall Web User Interface on page 43.
2. If you are configuring a Zone Core Protection (ZCP) firewall, from the left pane of the WebUI, select **Global** → **Dashboard** → **Status**.
3. If you are not configuring a ZCP firewall, from the left pane of the WebUI, select **System** → **Dashboard** → **Status**.
4. On the **System Information** widget, perform the following actions:
   a. Select **Firmware Version**.
   b. Select **Update**.
5. Click **Browse** and navigate to the configuration file.

6 Select the **Boot the new firmware** option.

7 Click **OK**.

After the image is loaded, the firewall reboots automatically. This process may take from three to five minutes.

3.1.3
Clean Installing the Firewall Firmware

Clean installation re-images the boot device, including the signatures that were current at the time that the firmware image file was created.

The clean installation can only be done during a boot interrupt, before network connectivity is available, and requires a local console connection to the Command Line Interface (CLI). The clean installation cannot be performed through a network connection.

Prerequisites:
Obtain the following items:

- Laptop with a TFTP server installed
- Ethernet cable

Obtain the credentials to log on to the firewall by performing one of the following actions:

- If the firewall device comes from Factory Default, the user name is always `admin` with no password.
- If the Motorola Solutions configuration file is loaded on the firewall device, obtain the logon information from your system administrator.

Procedure:

1 Connect the service laptop to the firewall console port. See Establishing a Terminal Emulator Session with the Firewall Console Port on page 44.

2 Using the Ethernet cable, connect the MGMT port of the firewall directly to the laptop.

3 Copy the new firmware image file to the service laptop.

4 Configure the service laptop IP address as follows: `192.168.1.168/24`

5 Verify that the TFTP server is running and that it was configured with the correct upload/download directory to include the new firmware image file.

6 **IMPORTANT:** You have only three seconds to press any key in step step 6 b. If you do not press a key soon enough, the firewall reboots and you must perform step 6 again.

Enter the firewall configuration menu by performing the following actions:

a Restart the firewall by entering: `execute reboot` or power off and power on the firewall.

The firewall starts and system startup messages display.

b When the following information displays, press any key to interrupt the system startup.

```
Press any key to display configuration menu.....
```

If you successfully interrupted the startup process, the following message appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[I]: Configuration and information.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

```
Enter G,F,B,I,Q,or H:
```

7 Format the boot device by entering: `F`

8 At the `All data will be erased, continue:[Y/N]?` prompt, enter: `Y`

9 Get the firmware image from the TFTP server by entering: `G`

10 When prompted to enter server IP, perform one of the following actions:

- If you did not configure the service laptop IP address, enter the IP address of the service laptop.
- If you configured the service laptop IP address, press ENTER.

11 At the `Enter Local Address [192.168.1.188]:` prompt, press ENTER.

12 At the `Enter File Name [image.out]:`, enter the firmware image file name.

The firewall downloads the firmware image file from the TFTP server and displays a message similar to the following: `Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]`

13 Enter: `D`

The firewall downloads the firmware image file from the TFTP server. The firewall installs the firmware and restarts.

14 To verify that the firmware was successfully installed, log in to the CLI and enter: `get system status`

The firmware version number appears.

3.1.4
Loading/Restoring a Firewall Configuration Locally with PSCP

You can load or restore the firewall configuration from an NM Client service laptop.

Prerequisites:
Obtain a laptop.

Ensure that:

- SSH (ssh and scp) is enabled on the firewall. This is a part of the Motorola Solutions-provided configuration.
- PuTTY is installed on the service laptop.
- An admin password is configured on the firewall.

Procedure:

1 Perform one of the following actions:

- If the Motorola Solutions configuration file is loaded on the firewall, open the command prompt on an NM Client. Go to step 3.
- If the Motorola Solutions configuration file in not yet loaded on the firewall (for example, when replacing the firewall), open the command prompt on a service laptop connected to the MGMT port on the firewall. Go to step 2.

2 Configure the laptop with an IP address matching the subnet of the MGMT IP address on the firewall.

The factory default IP address on the firewall is 192.168.1.99.

3 Copy the configuration file to the NM Client or service laptop.

4 Navigate to the PuTTY directory.

Step example: If you installed PuTTY from the ASTRO® 25 system *Windows Supplemental* media, enter the following at the prompt:
`cd Program Files (x86)\Motorola\Motorola PuTTY\Bin`

5 From the PuTTY directory, enter:

`pscp` ***<path\configuration file><username>@<IP address of fortigate>***`:fgt-restore-config`

where ***<username>*** is the administrator account for the firewall (the default firewall administrator account is `admin`)

6 When prompted, enter the password for the administrator account on the firewall.

The firewall configuration file is loaded into the firewall.

3.1.5
Loading/Restoring a Firewall Configuration with WebUI

NOTICE: This procedure cannot be performed if “manage web” is disabled on the firewall's Trust interface.

Prerequisites: Obtain the username and password of the firewall’s administrator account.

Procedure:

1 Open a WebUI connection and log in to the firewall. See Logging into the Firewall Web User Interface on page 43.

2 From the left pane of the WebUI, select **System** → **Dashboard** → **Status**.

For ZCP Firewalls, select **Global** → **Config** → **Dashboard** → **Status**.

3 On the System Information widget, select **System Configuration**, then **Restore**.

4 Select the configuration file to be restored from your local service laptop.

5 Enter the path and file name of the configuration file, or select **Browse** to locate the file.

6 Enter the password if the configuration file was encrypted during backup (the password is the same as the one set during backup).

IMPORTANT: No need to enter password if the configuration file is not encrypted.

7 Select **Restore**.

The Firewall automatically reboots. The firewall configuration file is loaded onto the firewall.

3.1.6
Changing a Pre-Shared Key on a Fortinet Firewall with WebUI

Prerequisites: Obtain the username and password of the firewall’s administrator account.

NOTICE: Motorola Solutions enters and maintains the firewall rules for your ASTRO® 25 system. If you have questions about your firewall rules, you can contact the Motorola Solutions Support Center (SSC).

When and where to use: Follow these steps to change a Pre-Shared Key (PSK) and properly configure the firewall for encryption.

Procedure:

1. Log into the firewall following Logging into the Firewall Web User Interface on page 43.
2. Click the following selections in the left pane of the WebUI:
   a. **VPNs**
   b. **IPsec**
   c. **Tunnels**
3. Under **Interface Mode (Dedicated VPN)** or **Tunnel Mode (Dial-up VPN)**, double-click the tunnel name you want to edit.

   The firewall's **Edit VPN Tunnel** window displays.
4. In the **Authentication** section, click **Edit**.
5. Type in a new key in the **Pre-Shared Key** field.

   NOTICE: The PSK that you enter here must match the PSK on the transport device at the other end of the VPN.
6. Click **OK** to close the window.
7. Click **Logout** in the left pane of the WebUI.

3.1.7
Completing the Fortinet Firewall Configuration

Prerequisites: If applicable, for systems with RADIUS and SNMPv3 enabled, obtain:

- RADIUS shared secret
- SNMPv3 auth/priv passphrases

If applicable, for systems with link encryption or protocol authentication, obtain:

- Pre-Shared Keys (PSKs)
- OSPF MD5 keys
- BGP MD5 keys

When and where to use: Follow these steps to load a firewall configuration file when installing a new firewall appliance.

Process:

1. For the centralized authentication feature, the RADIUS authentication sources are already set up in firewall configuration files provided by Motorola Solutions. The only RADIUS configuration task you need to perform on firewall is changing the secret key that matches the "shared secret" for this RADIUS client on the RADIUS server.

   See the *Authentication Services Feature Guide*.
2. On systems with SNMPv3 enabled, if auth/priv is used, change the SNMPv3 passphrases from default to your system's desired option.

   See the *SNMPv3 Feature Guide*.
3. On systems with link encryption, enter the correct pre-shared keys (PSKs) for the new firewall, so that it can be authenticated by its encryption peer.

   See the *Link Encryption and Authentication Feature Guide*.

4 On systems with protocol authentication, enter the correct OSPF MD5 key or BGP MD5 key for the new firewall, so that it can authenticate with its authentication neighbor/peer.

   See the *Link Encryption and Authentication Feature Guide*.

5 If the UNC application is present in the system, discover the firewall using the application.

   See the *Unified Network Configurator User Guide*.

6 If the UEM application is present in the system, discover the firewall using the Unified Event Manager application.

   See the *Unified Event Manager User Guide*.

   NOTICE: If you are configuring a FortiGate 101E or FortiGate 100D firewall, during the UEM discovery, the 23rd port may appear. This is a modem port that you can ignore.

7 For details on setting up Centralized Event Logging, if this optional feature is being implemented in the system, see the *Centralized Event Logging Feature Guide*.

Chapter 4

Firewall Configuration Backup

You can perform firewall configuration backup by using WebUI or PuTTY Secure Copy (PSCP).

You can back up the firewall configuration locally by using WebUI. See Backing Up a Firewall Configuration Locally with WebUI on page 41.

If telnet/TFTP or the WebUI functionality is disabled on the firewall, you can back up the firewall configuration locally by using PSCP. See Backing Up a Firewall Configuration Locally with PSCP on page 41.

4.1 Backing Up a Firewall Configuration Locally with WebUI

Prerequisites: Ask your system administrator for the username and password of the firewall's administrator account.

NOTICE: This procedure assumes that the source IP address used to access the Web UI of the Firewall resides in the trusted host list configured on the firewall and http/https is enabled on the management interface of the firewall.

Procedure:

1. Open a WebUI connection and log in to the firewall. See Logging into the Firewall Web User Interface on page 43.
2. From the left pane of the WebUI, select **System** → **Dashboard** → **Status**.

   For ZCP Firewalls, select **Global** → **Config** → **Dashboard** → **Status**.
3. On the System Information widget, select **System Configuration**, then **Backup**.
4. Select a backup to your local service laptop.

   IMPORTANT: Do not check the **Encrypt configuration file** option. If you select this option, you will need to enter the admin password and remember it (you will have to use the same password when you restore this backup configuration).

   The web browser prompts for a location to save the configuration file.
5. Provide the location where the configuration file is to be saved.

   NOTICE: The configuration file is saved with a `.conf` extension.

   The current system configuration is saved to a backup configuration file in the desired backup location of the computer.

4.2 Backing Up a Firewall Configuration Locally with PSCP

Perform this procedure to save the configuration from a firewall to a service laptop when telnet/TFTP is disabled on the firewall or if the WebUI functionality is disabled on the firewall.

Prerequisites: Ensure that:

- SSH (ssh and scp) are enabled on the firewall. This is part of the Motorola Solutions-provided configuration.

- PuTTY is installed on a service laptop.
- An admin password is configured on the firewall.

Procedure:

1 Perform one of the following actions:

If...	Then...
Motorola Solutions configuration is loaded on the firewall,	open the command prompt on an NM Client, then go to step 3.
Motorola Solutions configuration is not yet loaded on the firewall (for example, when replacing the firewall),	open the command prompt on a service laptop connected to the MGMT port on the firewall, then go to step 2.

2 Set up the laptop.

The IP address for the firewall and the service laptop must be in the same subnet. If the default firewall IP address has not been changed yet, configure the laptop with the following:

- IP address: 192.168.1.2
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.99

3 Open the command prompt window on the service laptop and navigate to the PuTTY directory.

Step example: If you installed PuTTY from the ASTRO® 25 system *Windows Supplemental* media, enter the following at the prompt:
`cd Program Files (x86)\Motorola\Motorola PuTTY\Bin`

4 From the PuTTY directory, enter:

`pscp` ***<username>***`@`***<IP address of fortigate>***`:fgt-config` ***<path>***

where:
<username> is the firewall administrator account name (initially, the name is `admin`)

<path> is a local directory of the service laptop, for example: `c:\config`

5 When prompted, enter the password for the firewall administrator account.

The firewall configuration is copied to the service laptop. The filename will be `fgt-config` and will be in the location specified in ***<path>***.

6 Store the cfg file in a secure location in case it is needed to recover the firewall.

Chapter 5

Firewalls Operation

This chapter provides information and procedures that enable you to operate on an ASTRO® 25 system firewall.

5.1 Logging into the Firewall Web User Interface

Prerequisites:

- Contact your system administrator for the username and password of the firewall's administrator account.
- If the firewall device is configured with factory default settings, then the user name is always `admin` (no password).
- If the firewall device has already been loaded with a proper Motorola Solutions configuration file, obtain the logon information from your system administrator.

NOTICE: This procedure assumes that the source IP address used to access the WebUI of the Firewall resides in the trusted host list configured on the firewall and http/https is enabled on the management interface of the firewall.

Procedure:

1. Configure the laptop with an IP address allowed for access to the firewall's MGMT IP.

   The factory default IP address on the firewall is 192.168.1.99.

2. Launch a web browser on the laptop.

   The supported web browsers are:

   - Chromium version 75 or later
   - Microsoft Edge version 44 or later
   - Mozilla Firefox version 66 or later
   - Apple Safari version 12.1 or later

3. In the web browser URL field, enter: `https://<IP address of firewall>`

   - If the firewall is factory-default, the IP address of the firewall is: `192.168.1.99`
   - If Motorola Solutions configuration has been loaded onto the firewall, refer to the IP Plan document for correct IP addresses.

   The firewall's WebUI may display a **Login Disclaimer**.

4. Click **Accept**.

   The firewall's WebUI displays a login window for the firewall.

5. Type the username and password for the firewall's administrator account (the default username is `admin` and the default password is empty).

6. Click **Login**.

   The firewall's WebUI home page displays.

5.2 Establishing a Terminal Emulator Session with the Firewall Console Port

Prerequisites:
Obtain the credentials to log on to the firewall by performing one of the following actions:

- If the firewall device comes from Factory Default, the user name is always `admin` with no password.
- If the Motorola Solutions configuration file is loaded on the firewall device, obtain the logon information from your system administrator.

Ensure that the terminal emulation software is installed (for example: HyperTerminal, Procomm Plus, or Tera Term Pro).

Obtain the following items:

- DB-9 adapter
- RJ-45 console cable
- Laptop

Procedure:

1. Plug and secure the female end of the supplied DB-9 adapter into the serial port of your computer.
2. Plug the RJ-45 console cable into the console port of the firewall device.
3. With the serial terminal emulation software, launch a Command Line Interface (CLI) session between the laptop and the firewall device by using the following settings:
   - Baud Rate: `9600`
   - Parity: `None`
   - Data Bits: `8`
   - Stop Bit: `1`
   - Flow Control: `none`
4. Press ENTER.
5. At the login prompt, enter the administrator user name.

   Initially, the administrator name is `admin`
6. At the password prompt, enter the default password for the firewall device.

The command prompt displays.

Chapter 6

Firewalls Disaster Recovery

This chapter provides references and information that enable you to recover an ASTRO® 25 system firewall in the event of a failure.

6.1 Recovering Firewalls

During the initial firewall implementation, Motorola Solutions configures the firewall interfaces and policies. In case of a firewall failure, the interfaces and policies configuration can be restored from the firewall backup.

This process applies to the following firewall types:

- Inter-RF Subsystem Interface 8000 (ISSI 8000) (NGI) firewall
- Telephone Interconnect firewall
- Control Room firewall
- LMR Multicast Proxy (LMP) firewall
- Radio Network Infrastructure (RNI) De-Militarized Zone (DMZ) firewall

IMPORTANT: Do **not** connect the replacement firewall network cables to the switch port until instructed to do so.

Prerequisites:
If you are recovering an RNI-DMZ firewall that has two-factor tokens provisioned, regain the functionality of the tokens. See the *Service Access Architecture Feature Guide*.

Obtain the following items:

- Laptop
- Replacement firewall

Process:

1. Connect power to the replacement firewall by performing the following actions:
   a. Ground the replacement firewall chassis. See Grounding the Firewall Chassis on page 25.
   b. Connect power to the replacement firewall. See Applying Power to Firewalls on page 32.
2. Connect the laptop to the console port of the replacement firewall. See Establishing a Terminal Emulator Session with the Firewall Console Port on page 44.
3. Check the firewalls software version by performing the following actions:
   a. Obtain the replacement firewall firmware version by using the following command: `get system status | grep -i version`
   b. Using the firewall management application, obtain the failed firewall software version.
   c. Compare the replacement firewall software version with the failed firewall software version.
4. Perform one of the following actions:

If…	Then…
If the firmware versions of the replacement firewall and the failed firewall are the same,	copy the failed firewall backup configuration to the laptop.
If the firmware versions of the replacement firewall and the failed firewall are not the same,	perform the following actions: **a** Upgrade or downgrade the replacement firewall firmware to match the failed firewall firmware version. Depending on the availability of each method, perform one of the following procedures: • Loading Firewall Firmware Locally with PSCP on page 34 • Loading Firewall Firmware Locally with WebUI on page 35 • Clean Installing the Firewall Firmware on page 36 **b** Copy the failed firewall backup configuration to the laptop.

5 Transfer the failed firewall backup configuration to the firewall. Depending on the availability of each method, perform one of the following actions:

IMPORTANT: If the firewall has been configured in the High Availability (HA) mode, some parameters (for example, hostname, management IP address, and engine-id) which cannot be overwritten by loading or restoring the HA firewall configuration using PuTTY Secure Copy (PSCP), WebUI or Unified Network Configurator (UNC). Avoid making any intentional changes to these parameters in the HA mode. If for any reason these parameters need to be changed, you can do it manually by using a CLI or WebUI procedure.

- Restore the firewall configuration locally by using PSCP. See Loading/Restoring a Firewall Configuration Locally with PSCP on page 37.
- Restore the firewall configuration by using WebUI. See Loading/Restoring a Firewall Configuration with WebUI on page 38.

6 Ensure that each cable connected to the failed firewall is labeled to indicate the appropriate firewall port assignment.

Cables should be connected to the same ports on the replacement firewall as on the failed firewall.

7 Disconnect the cables from the failed firewall, and remove the failed firewall from the rack.

8 Install the replacement firewall hardware. See Installing Firewall Hardware on page 24.

9 If a FortiManager is implemented in your system, perform the following actions:

a In the management application, on the **Devices** section, under **Device Manager**, right-click the failed firewall and select **Delete**.

b On the dialog box, click **Next**.

c Add the new firewall to the management application. See the *Fortinet Firewall Manager User Guide*.

10 If the Unified Network Configurator (UNC) application is present in the system, replace the device in the UNC. See the *Unified Network Configurator User Guide*.

11 If the Unified Event Manager (UEM) is present in the system, delete and discover the firewall in the UEM. See the *Unified Event Manager User Guide*.

Chapter 7

Firewalls Hardware Reference

This chapter provides references and information about ASTRO® 25 system firewalls hardware.

7.1 FortiGate 101E Physical Description

Figure 13: FortiGate 101E Front Panel

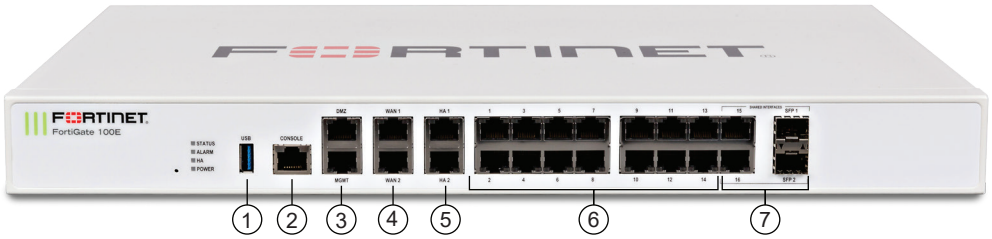


Table 10: FortiGate 101E Front Panel Description

Annotation	Description
1	USB Port
2	Console Port
3	2x GE RJ45 MGMT/DMZ Ports
4	2x GE RJ45 WAN Ports
5	2x GE RJ45 HA Ports
6	14x GE RJ45 Ports
7	2x GE RJ45/SFP Shared Media Pairs

7.2 FortiGate 101E LEDs

If any significant problems are suspected with the firewall, contact Motorola Solutions for assistance.

Figure 14: FortiGate 101E Front Panel LEDs

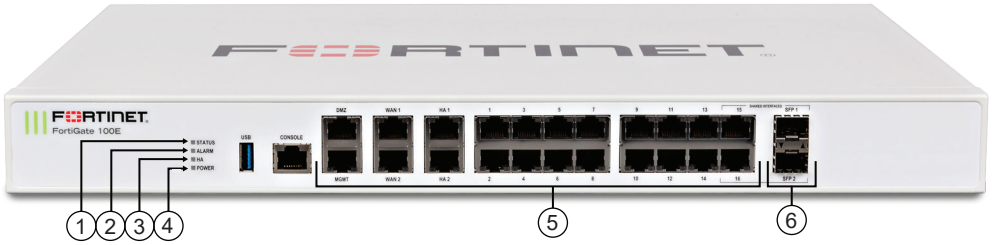


Table 11: FortiGate 100D Front Panel LEDs

Item	LED Label	State	Description
1	Status	Green	The unit is operating normally.
		Red	The unit has an error.
		Off	The unit is turned off.
2	Alarm		Not in use.
3	HA (High Availability)	Off	The unit is not operating in HA mode.
		Green	The unit is operating in normal HA mode.
4	Power	Green	The unit is on.
		Off	The unit is off.
5	Ethernet Ports Activity	Green	Port is active.
		Flashing Green	Port is transmitting and receiving data.
		Off	Port is not in use.
5	Ethernet Port Speed	Green	Port is connected at 1Gbps.
		Amber	Port is connected at 100Mbps.
		Off	Port is connected at 10Mbps or is not in use.
6	Small form-factor pluggable transceiver (SFP) Port Activity	Green	Port is active.
		Flashing Green	Port is transmitting and receiving data.
		Off	Port is not in use.

7.3 FortiGate 100D Physical Description

The front panel of the FortiGate 100D firewall is configured with the following components:

- 22 Network interfaces
  - 1 MGMT interface
  - 2 WAN interfaces
  - 1 DMZ interface
  - 2 HA interfaces
  - 2 10/100/1000Mbps shared configurable RJ45/SFP interfaces
- 1 Console port
- 1 USB port
- 1 USB Management port

Figure 15: FortiGate 100D - Front View

The back panel of the FortiGate 100D firewall is configured with a 100-240V AC, 60-50Hz, 3-1.5A power socket.

Figure 16: FortiGate 100D - Rear View

7.4 FortiGate 100D LEDs

If any significant problems are suspected with the firewall, contact Motorola Solutions for assistance.

Figure 17: FortiGate 100D Front Panel LEDs

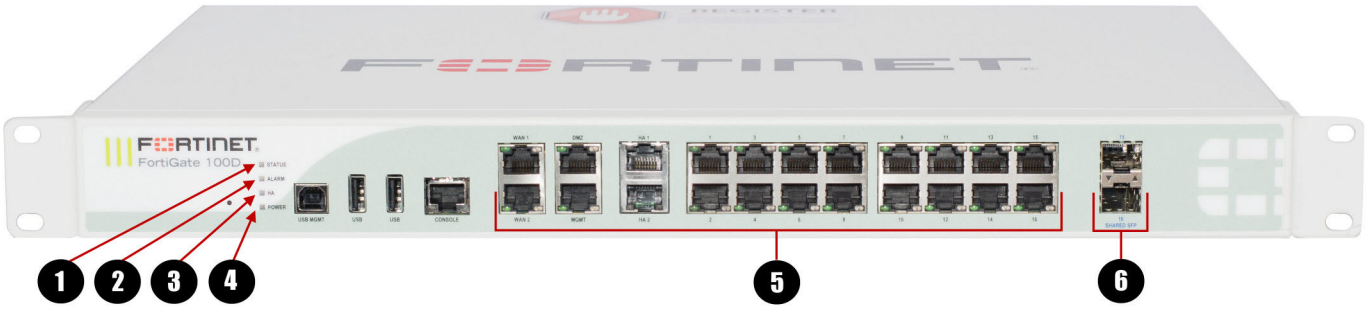


Table 12: FortiGate 100D Front Panel LEDs

Item	LED Label	State	Description
1	STATUS	Green	The unit is operating normally.
		Red	The unit has an error.
		Off	The unit is turned off.
2	ALARM		Not in use
3	HA (High Availability)	Off	The unit is not operating in HA mode.
		Green	The unit is operating in normal HA mode.
4	POWER	Green	The unit is on.

Item	LED Label	State	Description
		Off	The unit is off.
5	Ethernet Ports Activity	Green	Port is active.
		Flashing Green	Port is transmitting and receiving data.
		Off	Port is not in use.
5	Ethernet Port Speed	Green	Port is connected at 1Gbps.
		Amber	Port is connected at 100Mbps.
		Off	Port is connected at 10Mbps or is not in use.
6	Small form-factor pluggable transceiver (SFP) Port Activity	Green	Port is active.
		Flashing Green	Port is transmitting and receiving data.
		Off	Port is not in use.

7.5 FortiGate Firewalls Environmental Specifications

Table 13: FortiGate Firewalls Environmental Specifications

This table refers to the following firewalls: FortiGate 101E, Fortigate 100D.

Characteristic	Requirement
Operating Temperature	32–104°F (0–40°C)
Storage Temperature	-31–158°F (-35–70°C)
Operating Humidity (non-condensing)	20–90%
Operating Altitude	< 7400 ft (2250 m)

7.6 FortiGate Firewalls FRE

Field replaceable entities (FRE) are components that can be removed from electronic equipment and replaced without the need to repair the entire product or system.

Table 14: Firewalls FRE Kit Numbers

Firewall Model	FRE Kit Number
FortiGate 101E Firewall FRE	T8586A
FortiGate 100D Firewall FRE	T8126A