

Motorola Solutions Technical Notification (MTN)

TITLE: Multiple issues seen with Fortinet firewalls

TECHNOLOGY: Fortinet Firewall

SYMPTOMS:

Issue #1: Firewall gets into a state where SIP traffic source address is NAT'ed as gateway IP

Symptom: Lost console traffic for 3rd party consoles connected to Astro system through a Fortinet Telephony-Inter System firewall, occurring after a network outage.

Issue #2: IPsec tunnels may go down after 420 days of uptime

Symptom: A persistent IPsec tunnel connection (eg. SSC connection through Fortinet Firewall) drops and needs to be reestablished.

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:

Issue #1: Astro releases A7.16, A7.17/A7.17.x and A7.18 with Fortinet Firewalls with FortiOS versions **below** 5.6.2

Issue #2: Astro releases A7.16 with Fortinet Firewalls with FortiOS versions **below** 5.2.3

SEVERITY RECOMMENDATION: Low

Low / Maintenance - Perform if system exhibits above symptoms

ROOT CAUSE / DEFINITIVE TEST:

Issues in Fortinet operating system.

Issue #1: After a failure in CEN network, firewall does not handle SIP session correctly.

The network outage needs to be in the Customer Network (from the firewall perspective: next hop router's interface bounces and ICMP is enabled on the next hop router).

Issue #2: After 420 days of uptime an IPsec tunnel may go down. When this is an SSC-Customer connection, network and security monitoring services do not function.

WORKAROUNDS AND CORRECTIVE ACTIONS:

Temporary workaround is to reboot the firewall.

RESOLUTIONS AND REPAIR PROCEDURES:

If the system exhibits above symptoms, FortiOS should be updated to version 5.6.2.

Note that FortiOS version 5.6.2 introduces other issues that may need to have the below workarounds performed, hence the update should be considered carefully.

The list of issues introduced by updating to FortiOS 5.6.2:

ANY USE NOT APPROVED BY MOTOROLA SOLUTIONS IS PROHIBITED. This Motorola Technical Notification (MTN) is issued pursuant to Motorola's ongoing review of the quality, effectiveness, and performance of its products. The information provided in this bulletin is intended for use by trained, professional technicians only, who have the expertise to perform the service described in the MTN. Motorola disclaims any and all liability for product quality or performance if the recommendations in this MTN are not implemented, or not implemented in compliance with the instructions provided here. Implementation of these recommendations may be necessary for the product to remain compliant with applicable laws or regulations. Please be advised, that failure to implement these recommendations in the manner instructed may also invalidate applicable warranties, or otherwise impact any potential contractual rights or obligations. 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. ©2016 Motorola Solutions, Inc. All rights reserved."

1. SSH key change during the update (loss of UNC connectivity)
2. After the configuration is restored from a backup, both firewalls in the cluster have the same management IP.
3. Auto MDIX does not work.

Workaround for 1 (SSH key change issue)

Procedure:

1. Launch the **VMware vSphere Client** from the Windows-based device where it resides.
A desktop shortcut was created during installation
2. Log on to the Linux server as root.
The vSphere Client Inventory window appears.
3. Select the virtual machine from the pane on the left and click the Console tab for this virtual machine.
The Console tab appears.
4. Click the window, log on to the virtual machine as root.
5. Type **admin_menu** to access administration menu, press Enter.
In order to select a menu item in the following steps, type the number that corresponds to that menu item, then press ENTER.
6. Select **OS Administration**.
7. Select **Security Provisioning**.
8. Select **Delete Device's Public SSH Key**.
9. Type IP address of the device being upgraded.
10. Pull the configuration of the device (as described in the Unified Network Configurator Manual, section 4.9.3.1 - **Pulling the Configuration for a Single Device**).

Workaround for 2 (management IP issue) Please see Appendix B (Fortigate firewall IP address update in cluster configuration). It describes actions that need to be taken after the restore.

Workaround for 3 (Auto MDIX issue) needs to be applied only to firewalls directly connected to routers, such as ZCP firewalls (firewalls connected to switches do not require the workaround). To correct the issue, replace the straight cable between the firewall and a router with a crossover cable (ie. where one end uses the T568A wiring standard and the other the T568B).

All these three issues need to be taken into account when updating to FortiOS 5.6.2.

Upgrade to the appropriate version as listed in the "PARTS REQUIRED (HARDWARE/SOFTWARE):" section below, based on the model.

To obtain software:

1. Initiate a software request case through Motorola Solution, Inc. System Support Center (SSC) at 1-800-221-7144 (1-302-444-9800)
2. Await confirmation email from UOST with instructions
3. Complete the Upgrade Operations Software Team (UOST) Software Order Form:
 - a. Reference **MTN-0023-19-NA** in the 'Reason for Software/Hardware Change' section of the software order form.
 - b. List the part number (**KC #** as listed under "PARTS REQUIRED (HARDWARE/SOFTWARE)" below) in the 'Part # or Version #' section of the software order form.
4. Email completed Software Order Form to UOST for processing

PARTS REQUIRED (HARDWARE/SOFTWARE):

ASTRO Release	KC number
A7.16	KC147C03M000071600
A7.17/A7.17.1/ A7.17.2/A7.17.3	KC147C03M000071700
A7.18	KC147C03M000071800

ADDITIONAL INFORMATION:

Select proper version of OS for Fortigate 100D.
See Appendix A for choosing the proper Fortigate version

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:

WHEN TO APPLY RESOLUTION:

After reboot ___
After (re)installation ___
After upgrade ___
After power cycle ___
After database restoration ___
After failure ___
On FRU replacement ___
During maintenance ___
Immediately ___
As instructed _x_
Information only ___

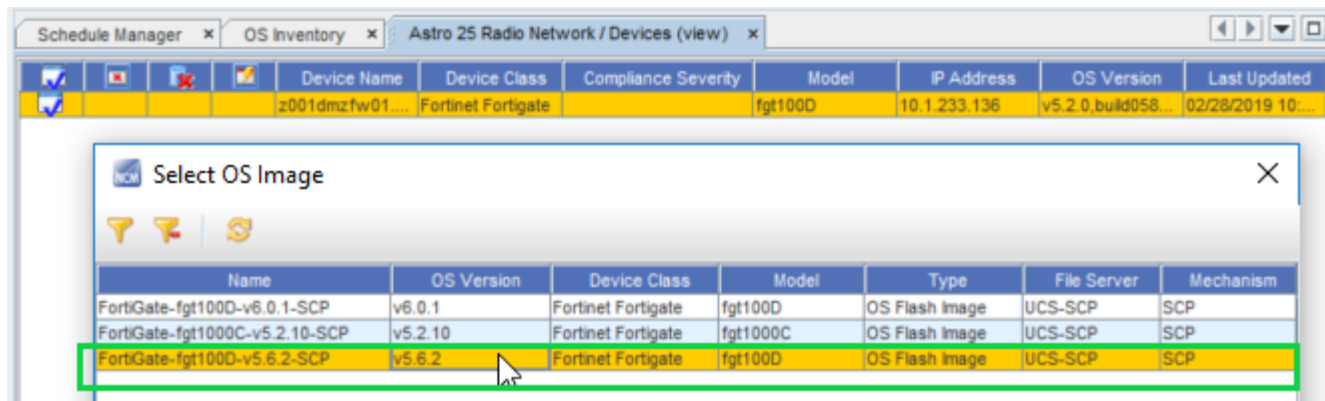
LABOR ALLOWANCE:

This is an informational bulletin. No labor warranty is implied, intended or authorized for U.S. Domestic Partners/Customers. Other regions should follow their own standard procedures.

For assistance with this bulletin please contact your MSI Technical support centre
https://www.motorolasolutions.com/en_us/support.html

Appendix A – Additional Symptom details

During the OS upgrade for Fortigate 100D model system operator should select OS from line 5.x.x. OS images from line 6.x.x are valid only for the Fortigate 101E model. The screenshot below shows the valid OS for Fortigate 100D model (marked in green). Correct version in this case is OS version 5.6.2.



The screenshot displays the Fortinet OS Inventory interface. At the top, there are tabs for 'Schedule Manager', 'OS Inventory', and 'Astro 25 Radio Network / Devices (view)'. Below the tabs is a table with columns: Device Name, Device Class, Compliance Severity, Model, IP Address, OS Version, and Last Updated. The table contains one entry: 'z001dmzfw01...' (Device Name), 'Fortinet Fortigate' (Device Class), 'Compliance Severity' (empty), 'fgt100D' (Model), '10.1.233.136' (IP Address), 'v5.2.0_build058...' (OS Version), and '02/28/2019 10:...' (Last Updated).

A 'Select OS Image' dialog box is open, showing a table with columns: Name, OS Version, Device Class, Model, Type, File Server, and Mechanism. The table contains three entries:

Name	OS Version	Device Class	Model	Type	File Server	Mechanism
FortiGate-fgt100D-v6.0.1-SCP	v6.0.1	Fortinet Fortigate	fgt100D	OS Flash Image	UCS-SCP	SCP
FortiGate-fgt1000C-v5.2.10-SCP	v5.2.10	Fortinet Fortigate	fgt1000C	OS Flash Image	UCS-SCP	SCP
FortiGate-fgt100D-v5.6.2-SCP	v5.6.2	Fortinet Fortigate	fgt100D	OS Flash Image	UCS-SCP	SCP

The row 'FortiGate-fgt100D-v5.6.2-SCP' is highlighted in green, indicating it is the selected OS image for the Fortigate 100D model.

Appendix B – Fortigate firewall IP address update in cluster configuration

Purpose

This document is intended to provide procedure for updating IP management address of one cluster member via the second one.

In case of 5.6.2 firmware version, configuration restore of the one firewall in cluster causes the second firewall to have the same management IP thus second firewall IP management address must be restored.

Timeline

This task should take approximately up 2 minutes per firewall cluster.

Detailed steps

1. Login to firewall which configuration was previously restored (vi SSH to trust interface).
2. Execute following command to login to the second member of the cluster:

execute ha manage <id>

where *id* is the number of the cluster member. It can be checked using following command:

get system ha status

Example:

```
Firewall # get system ha status
```

```
HA Health Status: OK
```

```
Model: FortiGate-100D
```

```
Mode: HA A-P
```

```
.....
```

```
Active:0 FG100D3G13818335
```

```
Passive:1 FG100D3G12808574
```

3. Set IP management address as it was before restore, using commands below (below is example for Zone1 RNI DMZ FW02:

```
config system interface
```

```
edit mgmt
```

```
set ip 10.1.233.137 255.255.255.0
```

```
next
```

```
end
```

4. Verify if the IP was set correctly.

```
Firewall $ config system interface
```

```
Firewall (interface) $ edit mgmt
```

```
Firewall (mgmt) $ show
```

```
config system interface
```

```
edit "mgmt"
```

```
set ip 10.1.233.137 255.255.255.0
```

```
set allowaccess ping https ssh snmp
```

```
set type physical
```

```
set snmp-index 6
```

```
set speed 100full
```

```
next
```

```
end
```

5. Enter ***exit*** to return to the first firewall.
6. Check if it is possible to log to the second firewall using its own IP.

Upgrade Operations Software Team

SECTION 1: General Information

NOTE: PRICE QUOTES GIVEN BY UOST ARE VALID FOR ONLY 90 DAYS

Date _____	Case Number _____
System ID _____	Site ID _____
System Name _____	Site Name _____
Customer Name _____	
Form Completed by _____	Field Contact _____
Organization _____	Organization _____
Phone Number _____	Phone Number _____
Pager Number _____	Pager Number _____
Fax Number _____	Fax Number _____

SECTION 2: Order Information

Product Type: _____ Serial Number _____

Reason for Software / Hardware Change: _____
Downgrade? If so, list current and target releases. _____

Software / Hardware Description: _____

Part # or Version # _____ Quantity _____

Date Required _____

SECTION 3: Shipping / Billing Information

Ship To: _____ Bill To: _____

Email: _____ Attn: _____

Attn: _____

Phone: _____ Phone: _____

Customer Billing**Internal Billing**

P.O. #: _____
 CUST #: _____
 TAG #: _____

PROJECT #: _____
 FSB #: _____
 DEPT #: _____
 APC #: _____



Software Order Form

Upgrade Operations Software Team

Phone Number: (800) 221-7144

- ° This form has been sent to you because you have requested an order from the Upgrade Operations Software Team.
- ° Please fill out the order form and email back to the Upgrade Operations Software Team
- ° If desired, please provide your email address on the order form and we will provide a tracking number when your order ships for your convenience.
- ° Orders will normally be processed in 3-5 business days once all information has been received.
- ° If additional space is required for software information, please use the optional addendum on page 3 below in addition to the original order form. This form is for use with large orders with multiple part numbers.

NOTE:

- 1) If this in an SSA CUSTOMER please order via Motorola factory order.
- 2) Limited Liability is Implied to the maximum of order amount.
- 3) Price quotes provided by UOST are valid for 90 days

Thank you and have a good day!

Supplemental Order Information Addendum

(Optional)

Software Description

Part# or Version #

Quantity:

Software Description

Part# or Version #

Quantity:

Software Description

Part# or Version #

Quantity:

Software Description

Part# or Version #

Quantity:

Software Description

Part# or Version #

Quantity:

Software Description

Part# or Version #

Quantity:
