

## Troubleshooting Guide



# **Enhanced Load Balancing Cluster**

Version 3 Troubleshooting Guide

Author: Minh Ly Consulting Security Engineer

# Change Log

Revision	Date	Change Description	Owner
1	2014-06-20	Initial Release	Minh Ly

## **Table of Contents**

About This Guide	5
Related Publications	5
Intended Audience	5
Management Software	6
System Overview	7
FortiSwitch Architecture	
Hardware	
Functions	
Traffic Processing	
Traffic Load Balancing	
Understanding NAT & Load Balancing	
FortiSwitch Concepts	
FortiGate Architecture	
Hardware	
Functions	
Traffic Processina	
Naming Scheme	21
FortiSwitch	21
Master FortiSwitch Chassis 15 Slot 1 Configuration Example	
Slave FortiSwitch Chassis 15 Slot 2 Configuration Example	
Slave FortiSwitch Chassis 16 Slot 1 Configuration Example	
Slave FortiSwitch Chassis 16 Slot 2 Configuration Example	
FortiSwitch Installation	
Method 1	
Method 2	
FortiSwitch HA Synchronization	
Verification	
Troubleshooting FortiSwitch HA	
Understanding Service Groups	
Manaaina Service Group Slots	
Troubleshooting Service Groups	
Installing a New FortiGate into an Existing Service Group	52
FortiGate	54
ELBCv3 Installation	54
Management Routing	56
Trauhleshaatina FartiGate Iains	57
Reducina Sinale Core CPII IIsaae	
FortiSwitch & FortiGate SNMP	
Query the FortiSwitch	60
Query the FortiGate	
FortiSwitch Service Group Worker Blades Commonly Used OIDs	
SNMP Interface Statistics	

Traps	64
FortiManager	66
FortiGate Management	
Install FortiGate Firewalls	
Associating FortiGate Interfaces with Zones	
Adding Policy Package	
Deploy System Configuration and Firewall Policy Packages	83
FortiGate Firmware Upgrade	
FortiSwitch Management	
Add FortiSwitch	
Chassis Shelf Manager	
Add The Shelf Manager	
FortiAnalyzer	
FortiGate Log Settings	
Logging to the Analyzer	

## **About This Guide**

The purpose of this guide is to describe the user tasks required to configure, troubleshoot and manage Enhanced Load Balancing Cluster version 3 using the FortiGate-5000 Series Chassis platform, FortiManager and FortiAnalyzer.

**Note:** The FortiGate-5000 Series Chassis can be installed with various network and security blades with distinct sets of network processors and ports. For example the FortiGate-5001C contains the latest NP4 network processors while the FortiGate-5101C contains SP3 processors. This guide describes user tasks for all 5000 Series security blades that are supported by the release of this FOS software.

This Guide covers four Fortinet Operating Systems.

- FortiSwitch 5.0 Build 15
- FortiGate 5.0.3 Build 208
- FortiManager 5.0.4 Build 232
- FortiAnalyzer 5.0.4 232

## **Related Publications**

Use this documentation in conjunction with FortiSwitch, FortiGate CLI, FortiAnalyzer and FortiManager publications, which provide syntax description and usage guidelines for commands. Blades System Guides will also be useful in providing description and differences between various types of network and security blades.

Publications can be found at <u>http://docs.fortinet.com</u>.

## **Intended Audience**

This publication is intended for system, network and security administrators experienced in access, internetwork and security administration.

## **Management Software**

ELBC contains a large number of devices to manage. Initial setup and configuration is best accomplished when using terminal emulation software that is capable of broadcasting commands to the multiple similar devices at once. Using such software will decrease deployment and troubleshooting time: software upgrade, sniffing packets, etc.

Figure 2-1-1		
1.	Inot	
		* -
S Shell Shell Shell	3 Default	*
c15s01 login:	c15s02 login:	0100
c15s01 login:	c15s0Z login:	
c15s01 login:	c15s02 login: admin	
c15s01 Login: admin	Password:	
Password:	c15s02 # get system status	
c15s01 # get system status		
	Version: FortiSwitch-5003B v5.0, build0015, 130827 (Patch 2)	
Version: FortiSwitch-5003B v5.0, build0015,130827 (Patch Z)	Branch Point: 0015	
Branch Point: 0015	Serial-Number: FS503B3E11700244	
Serial-Number: FS503B3E11700005	BIUS version: 04000006	
BIUS Version: 04000004	System Part-Number: P08//3-03	
Hostname: C15501	Hostname: C15502	
Current HA mode: a-p, master	Current HA mode: d-p, backup	
System time: Wed Nov 06 20:17:28 2013	System time: wed Nov 06 20:17:28 2015	
Daylight Time Saving: Tes	Daylight Time Saving: Tes	
Time Zone: (GMT-8:00)Pacific Time(US&Canada)	Time Zone: (GMI-8:00)Pacific Time(USacanada)	
c15s01 # diagnose system ha status 🗌	c15s02 # diagnose system ha status 🗌	
c15s01 # diagnose system ha status ] ⊗ Default & *	c15s02 # diagnose system ha status [	☆ -
c15s01 # diagnose system ha status [] ③ Default c16s01 # admin	c15s02 # diagnose system ha status [] ③ Default c16s02 login:	<b>☆</b> -
c15s01 # diagnose system ha status ]	c15s02 # diagnose system ha status ] Default c16s02 login: c16s02 login:	¢ ▼
c15s01 # diagnose system ha status []  Default c15s01 # admin Unknown action 0	c15s02 # diagnose system ha status ]  Default  c16s02 login: c16s02 login: c16s02 login: c16s02 login: dis02	☆ <b>▼</b>
c15s01 # diagnose system ha status ]  Default  C16s01 # admin Unknown action 0  c16s01 #	c15s02 # diagnose system ha status Default c16s02 login: c16s02 login: c16s02 login: domin Password: Password:	☆ <b>-</b>
c15s01 # diagnose system ha status Default C16s01 # admin Unknown action 0 C16s01 # c16s01 # c16s01 # get system status	c15s02 # diagnose system ha status ] Control Default c16s02 login: c16s02 login: c16s02 login: admin Password: c16s02 # get system status	¢ ▼ □ *
c15s01 # diagnose system ha status [ Default ** * c16s01 # admin Unknown action 0 c16s01 # c16s01 # c16s01 # get system status	c15s02 # diagnose system ha status ] S Default c16s02 login: c16s02 login: c16s02 login: admin Password: c16s02 # get system status	* *
c15s01 # diagnose system ha status Default C16s01 # admin Unknown action 0 C16s01 # c16s01 # c16s01 # get system status Version: FortiSwitch-50038 v5.0,build0015,130827 (Patch 2)	c15s02 # diagnose system ha status ] Default c16s02 login: c16s02 login: c16s02 login: admin Password: c16s02 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)	* •
c15s01 # diagnose system ha status C15s01 # admin Unknown action 0 c16s01 # c16s01 # c16s01 # c16s01 # get system status Version: FortiSwitch-50038 v5.0,build0015,130827 (Patch 2) Branch Point: 0015	<pre>c15802 # diagnose system ha status ] C15802 login: c16802 login: c16802 login: c16802 login: admin Password: c16802 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015</pre>	* *
c15s01 # diagnose system ha status Default  C16s01 # admin Unknown action 0  C16s01 #  C16s01 #  C16s01 # C16s01 # C16s01 # C16s01 # get system status Version: FortiSwitch-50038 v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Branch Point: 0015 Serial-Number: F55083811700266	<pre>c15s02 # diagnose system ha status ] S Default C16s02 login: c16s02 login: c16s02 login: c16s02 login: c16s02 login: c16s02 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: FS50383E11700261</pre>	☆ <b>*</b>
c15s01 # diagnose system ha status Default ** c16s01 # admin Unknown action 0 c16s01 # c16s01 # c16s01 # get system status Version: FortiSwitch-50038 v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F550303E11700266 BIOS version: 04000006	<pre>c15s02 # diagnose system ha status ] C15s02 # diagnose system ha status ] C16s02 login: c16s02 login: c16s02 login: admin Password: c16s02 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F5S0383E11700261 BIOS version: 04000006</pre>	☆ ▼ 2 ×
c15s01 # diagnose system ha status C15s01 # admin Unknown action 0 c16s01 # get system status Version: FortiSwitch-50038 v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F550338311700266 BIOS version: 04000006 System Part-Number: P08773-03	c15802 # diagnose system ha status Default C16502 login: C16502 login: C16502 login: C16502 login: C16502 login: C16502 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F550383E11700261 BIOS version: 04000006 System Part-Number: P08773-03	☆ ▼ 2
c15s01 # diagnose system ha status Default C16s01 # admin Unknown action 0 C16s01 # C16s01#	c15x02 # diagnose system ha status C15x02 # diagnose system ha status c16s02 login: c16s02 login: c16s02 login: c16s02 login: c16s02 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F5503B3E11700261 BIOS version: 04000006 System Part-Number: P08773-03 Hostname: c16s02	☆ ▼ *
c15s01 # diagnose system ha status Default  C16501 # admin Unknown action 0  C16s01 #  C16s01#  C16s01 #  C16s01 #  C16s01 #  C16s01 #  C16s01 #	<pre>c15s02 # diagnose system ha status [] C15s02 # diagnose system ha status [] C16s02 login: c16s02 login: c16s02 login: admin Password: c16s02 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F580383E11700261 BIOS version: 04000006 System Part-Number: P80773-03 Hostname: C16s02 Current HA mode: a-p, backup </pre>	*
c15s01 # diagnose system ha status C15s01 # admin Unknown action 0 c16s01 # c16s01 # c16s01 # c16s01 # c16s01 # Serial-Number: F5S03B3511700266 BIOS version: 04000006 System Part-Number: P00773-03 Hostname: c16s01 Current HA mode: a-p, backup System Version Web 20:17:28 2013	<pre>c15802 # diagnose system ha status [] Cl5802 login: c16802 login: c16802 login: c16802 login: c16802 login: c16802 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F580383E11700261 BIOS version: 04000006 System Part-Number: P08773-03 Hostname: c16802 Current HA mode: a-p, backup System time: Wed Nov 06 20:17:28 2013</pre>	*
c15s01 # diagnose system ha status Default  C16s01 # admin Unknown action 0  C16s01 # C16s01 C17c8 C15 C15c8 C15	<pre>c15s02 # diagnose system ha status [] C15s02 # diagnose system ha status [] C16s02 login: c16s02 login: c16s02 login: admin Password: c16s02 # get system status Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: FS503B3E11700261 BIOS version: 04000006 System Ture-Number: P08773-03 Hostname: c16s02 Current HA mode: a-p, backup System Ture: Wed Nov 66 20:17:28 2013 Doylight Time Saving: Yes</pre>	*
c15s01 # diagnose system ha status Default  C16501 # admin Unknown action 0  C16s01 # C16s01 C17:03 Hould # C	<pre>c15s02 # diagnose system ha status [] C15s02 # diagnose system ha status [] C16s02 login: c16s02 login: admin Password: c16s02 login: admin Password: c16s02 # get system status Version: FortiSwitch-50038 v5.0,build0015,130827 (Patch 2) Branch Point: 0015 Serial-Number: F5S0383E11700261 BIOS version: 04000006 System Part-Number: P08773-03 Hostname: c16s02 Current HA mode: a-p, backup System time: Wed Nov 06 20:17:28 2013 Daylight Time Saving: Yes Time Zone: (GMT-8:00)Pacific Time(US&amp;Canada)</pre>	\$ * *

Recommended Software:

MAC: iTerm2 Linux: Terminator

## **System Overview**

This Chapter describes the FortiSwitch hardware and software, including where the product fits in today's high-speed security networks, and an overview of concepts and terminology.

- FortiSwitch Architecture
- FortiSwitch Concepts
- FortiGate Architecture
- FortiGate Concepts

## **FortiSwitch Architecture**

Ultra High-speed networks have grown to a point where traditional appliance firewalls can no longer handle all of the complex functions necessary to secure services without being an inline performance bottleneck. Security administrators have to choose between lowering security standards or maintain higher network performance. To compensate for the lack of a single powerful security device that is capable of handling both security and performance, networks are partitioned into smaller less consuming entities and traffic is sent through multiple different security devices. The FortiSwitch combined with the FortiGate enables ELBC. This technology bridges the gap between maintaining Ultra High-speed networks and security without compromise.

The FortiSwitch Architecture is described in the following sections.

- Hardware
- Functions
- Traffic Processing

The FortiSwitch can be installed into a FG5140B or FG5060 chassis. Some older chassis versions are also supported.

Refer to <u>http://docs.fortinet.com</u> for further information.



Figure 3-1-1

FG5140B

FG5060

- Switching blades must be installed into hub slots 1 and/or 2 in either chassis.
- Security blades are installed into slots 3 14 on the FG5140B and slots 3-6 on the FG5060.

Hub slots interconnect to all other slots through both the fabric and base channels. The Fabric is 10 Gigabit per channel while the base channel is 1 Gigabit. Fabric channels are used for traffic while base channels are used for management.

The diagram conceptualizes internal connectivity for an FG5140B chassis.



Below shows internal Inter-switch fabric detail of the FS5003B.





Ports F1-F8 are used for data while B1 an B2 are redundant ports used for HA Heart Beats, Configuration Sync, Session Sync and per slot management. The Base-mgmt interface is used to NAT management traffic to individual slots. Refer to the section *Understanding Service Groups* for further information.

Each FortiGate contains a set of base interfaces. Base 1 connects to the FortiSwitch in slot-1 and base 2 connects to the FortiSwitch in slot-2 as depicted on page 9. Each FortiSwitch also contains a set of interfaces named B1 and B2. Do not be confused by the naming scheme on the FortiSwitch. Both B1 and B2 on a FortiSwitch connect to the same base interface on the FortiGate. For example, a FortiSwitch in slot-1 does not have its B2 interface connected to base 2 on the FortiGate. Figure 3-1-4



## FS5003B External Interfaces

Figure 3-1-5



The topology shows an example ELBCv3 architecture. FortiSwitch blades connect to both LAN and WAN switches because there is only one FortiSwitch processing traffic at any give time. All other FortiSwitch blades are dormant slaves waiting to become master. Since ELBCv3 supports a single active switch both the LAN and WAN external switches connect to the same FortiSwitch. The redundant heartbeat switches are used for HA health checks, configuration sync and session sync between clusters.



#### **Functions**

The FortiSwitch provides an effective way of load balancing traffic across multiple security blades in a single solution.

- The FS5003B contains eight 10G fabric ports with a throughput limit of 80 Gbps.
- ELBCv3 can be deployed using a single switch or multiple switches for activepassive high availability.
- FortiGate security blades have connectivity to both active and passive FortiSwitches at the same time.
- A Single chassis can support up to twelve FortiGates.
- Redundant chassis would require an equal number of devices.
- The load balance algorithm is based upon a session's source IP, destination IP or source plus destination IP. To line up with FortiSwitch configuration terms, for the remainder of this document the following names will be used synonymously: source IP/SNAT, destination IP/DNAT, source plus destination IP/NONAT.
- Heath checks are maintained by the FortiSwitch to determine the number of existing security blades in the cluster.
- FortiGate configuration synchronization is verified before being allowed to enter the cluster.
- Service groups are used to distinguish between multiple security clusters within a given chassis.

## **Traffic Processing**

The FortiSwitch acts as a layer 3 load balancer and uses a hash to direct traffic among existing FortiGate blades.

- The Switch contains no session table and does not terminate nonmanagement traffic.
- TCP, UDP, IPv4 and IPv6 are load balanced between all FortiGate blades.
- The Master FortiGate responds to ICMP, SCTP and any neighboring for BGP.
- VPNs are not supported.

There are up to 64 Calendar entries that are divided between working FortiGate slots. For each calendar entry a working FortiGate is chosen to be it's target. Traffic is hashed to produce a key that acts as an index in to the calendar.

- service-group-hash-size normal uses 32 Calendar entries
- service-group-hash-size expanded uses 64 Calendar entries but reduces the amount of service groups allowed from four to two

In the example below there are four FortiGates in an ELBC cluster: slots 3, 4, 5 and 6.

The Hash Keys produced are shown for each blade.

A source address of 1.1.1.1 to a destination of 2.2.2.2 will use hash key 2 and would be forwarded to slot-3.

FortiSwitch	- c15s01	+		FortiSwitch – c15s01				
10.100.23.2	21/index			රු⊽ C (8	how to turn in r	maverickQ) 💽	- 4	)(
FortiSwitch	5003B					🐌 FI	BTI	
Svetom	Status	Config	<u>Ca</u>	Iculator Traffic Monitor				
Suddell				Service Group #1 Traffic Calculate				
witch				Service Group #1 france Calculato				
ervice Groups	Load Balancing Algorithm			Hash IP Least 6-Bits				
Service Group 1								
ervice Group 2	SICIP			1.1.1.1				
	Dst IP			2.2.2.2				
				Apply				
	1.0							
	Hash Key			2				
	Traffic To			Slot #3				
	Group Membe	rship						
	Worker Blade	Role	Weight	Hash Keys	Bytes Tx	Bytes Rx	Status	
	Slot #3	Active	5	2/5/8/11/14/17/20/23/26/29/48/51/54/57 /60/63	304,768,626	2,007,166,526	0	Ø
	Slot #4	Active	5	15/18/21/24/27/32/35/38/41/44/47/50/53/56/59/62	304,770,898	2,007,166,526	0	
							-	-
	Slot #5	Active	5	16/19/22/25/28/31/34/37/40/43/46/49/52/55/58/61	304,770,112	2,007,166,526	0	



The hash key value generated by the algorithm, the hash keys accepted by the worker blades, and the blade the traffic is sent to are automatically calculated by the <u>FortiSwitch</u>.

Calendar entries for all working slots are shown below. Notice the Calendar Legend slot number mapping.

When a slot fails such as slot-6, only its calendar entry is remapped to exiting slots. Should there be no HA chassis to failover, only sessions for slot-6 are affected when remapping occurs. The calendar entries for slot-6 redistributed to existing slots.

**Understanding NAT & Load Balancing** 

The modes: SNAT, DNAT and NONAT designate whether to hash based upon the source or destination IP address or both.

The best way to think about this is to use a mode on the FortiSwitch that will hash upon an IP address that does not change in transit to avoid breaking state.

• SNAT is used when the FortiGate translates all internal source traffic to a different IP address. With this mode the FortiSwitch will hash based upon the destination IP address on the internal interface and source IP address on the external interface.



• DNAT is used when the FortiGate translates all external source traffic to a different IP address. With this mode the FortiSwitch will hash based upon the destination IP address on the external interface and source IP address on the internal interface.



Figure 3-1-10 DNAT, Single LAG Port Shown on FS Per Direction

• NONAT is used when translations do not occur on either side.



The easiest way to visualize ELBCv3 is to imagine a traditional network that contains link aggregation using a north and south switch architecture with devices sandwiched in between. Each "Red" security blade processes traffic independently from its neighbor.

The "S" below stands for the slot number in a FG5140B chassis.



## FortiGate Architecture

The FortiGate-5000 series chassis and blades offer unmatched performance and scalability for your high-speed service provider, data centers or telecommunications carrier network. Native 10-GbE support and a highly flexible AdvancedTCA™ (ATCA)-compliant architecture enables the FortiGate-5000 series to deliver next-gen protection of complex, multi-tenant cloud-based Security-as-a-Service and Infrastructure-as-a-Service environments.

The FortiGate Architecture is described in the following sections.

- Hardware
- Functions
- Traffic Processing

### Hardware

The 5000 Series FortiGates can be installed into a FG5140B or FG5060 chassis. Some older chassis versions are also supported.

Refer to <u>http://docs.fortinet.com</u> for further information.

The figure below shows one example of the many 5000 Series FortiGates supported.

#### FG5001B External Interfaces



## Internal Inter-switch fabric detail of the FG5001B

Figure 3-2-2



## Functions

All Firewall and UTM features are supported. Performance increase can be close to linear depending on the number of blades installed and network address mix. When the number of active firewall blades is a non-power of 2, resource utilization of worker blades in a service group can be skewed.

The FortiGate performs the following tasks.

- Processes security traffic.
- Sends heartbeats to the FortiSwitch.
- Synchronizes session tables to neighboring FortiGate in inter-chassis deployments.
- Session sync occurs between two FortiGates in the same slot of different chassis.
- Master FortiGate provides configuration sync to all slave blades through base channels.

## **Traffic Processing**

The FortiGate processes traffic received through the FortiSwitch as if it were a standalone device.

- Hash values of the FortiSwitch for ingress and egress traffic must match to ensure that traffic remains on the same FortiGate to maintain state.
- Different FortiGate models can be used when separated by service groups.

## **Naming Scheme**

In ELBC there are many devices working together to form a cluster. A single deployment can contain up to 32 devices, 16 per chassis: 2 FortiSwitches 12 FortiGates and 2 Shelf Managers. It is recommended to use a naming scheme that easily identifies each slot number.

Example Naming Scheme

Slots

- cXXsYY
  - c = chassis, XX = chassis ID, s = slot, YY = slot number
  - Example: c15s01, c16s14

Shelf Manager

- cXXshY
  - c = chassis, XX = chassis ID, sh = shelf manager, Y = shelf number
  - Example: c15sh1, c16sh2

## FortiSwitch

**NOTE**: Prior to configuring the FortiSwitch ensure that all switches are of the same hardware revision. Different revisions may not successfully synchronize HA configurations.

The FS5003B contains two revisions that have slight hardware differences.

- Rev 1 maps front port F8 to Slot-14.
- Rev 2 maps front port F8 to Slot1/2.
- Displaying the physical switch ports will be a good indicator of hardware revision.

```
c15s01 # show switch fabric-channel physical-port
config switch fabric-channel physical-port
edit "slot-3"
next
edit "f8/slot-14"
```

Since rev 1 allows usage of either fabric port F8 **or** Slot-14, one has to choose between using all 8 front data ports or populating an additional FortiGate in slot-14.

Using slot-14 requires a DIP switch position change on the FortiSwitch.

Refer to the FS5003B System Guide.

http://docs.fortinet.com

The interconnected port between slot-1 and slot-2 named slot1/2 is not used in ELBCv3. This means rev 2 allows access to all 8 front ports and 12 FortiGate slots without sacrificing performance.

Refer back to these configuration examples for the duration of this chapter.

config system global set hostname "c15s01" set service-group-mode 2-port-lag set service-group-hash-size expanded end config system interface edit "mgmt" set ip 10.100.23.221 255.255.255.0 set allowaccess ping https ssh snmp telnet http next edit "base-mgmt" next end config route static edit 1 set gateway 10.100.23.254 next end config admin user edit "admin" next end config system ha set mode a-p set password ENC 7vXgU5gIGwe4iT9Lor/eVNgL2j0JcYbGoB3P1UAvrn0Z4u1sr4VEejirW3XRDHIf1f40 GZ85qDsRkgQSql9oxlvA5wfLhkTk1HO3MTwkP8/+6LH9 set group-id 22 set priority 200 set hbdev-vlan-id 999 set chassis-redundancy enable set hbdev "b1" "b2" end config system central-management set fmg "172.30.71.92" end config service group edit 1 set status enable set base-mgmt-internal-mac 00:09:0f:ec:0b:72 set base-mgmt-internal-network 10.101.10.0 255.255.255.0 config base-mgmt-interfaces edit "b1" set vlan-id 101

```
next
        edit "b2"
          set vlan-id 101
        next
      end
   set base-mgmt-interface-mode active-active
    set elbc-base-ctrl-network 10.101.11.0 255.255.255.0
      config elbc-base-ctrl-interfaces
        edit "b1"
          set vlan-id 301
        next
        edit "b2"
          set vlan-id 301
        next
      end
      config slots
        edit 3
        next
        edit 4
        next
        edit 5
        next
        edit 6
        next
      end
      config traffic-interface
        edit "internal"
            set interface "f1" "f2"
          set port-mac-address 00:09:0f:ec:0b:73
        next
        edit "external"
            set interface "f3" "f4"
          set port-mac-address 00:09:0f:ec:0b:74
        next
      end
   set base-mgmt-external-ip 10.100.23.222 255.255.255.0
   set elbc-base-ctrl-interface-mode active-active
   set base-mgmt-allowaccess ping https ssh snmp telnet http fgfm
 next
 edit 2
 next
end
```

## Slave FortiSwitch Chassis 15 Slot 2 Configuration Example

```
config system global
  set hostname "c15s02"
 set service-group-mode 2-port-lag
  set service-group-hash-size expanded
end
config system interface
  edit "mgmt"
    set ip 10.100.23.221 255.255.255.0
    set allowaccess ping https ssh snmp telnet http
  next
  edit "base-mgmt"
  next
end
config route static
  edit 1
    set gateway 10.100.23.254
  next
end
config admin user
  edit "admin"
  next
end
config system ha
  set mode a-p
  set password ENC
7vXgU5gIGwe4iT9Lor/eVNgL2j0JcYbGoB3P1UAvrn0Z4u1sr4VEejirW3XRDHIf1f40
GZ85qDsRkgQSql9oxlvA5wfLhkTk1HO3MTwkP8/+6LH9
  set group-id 22
  set priority 200
  set hbdev-vlan-id 999
  set chassis-redundancy enable
    set hbdev "b1" "b2"
end
config system central-management
  set fmg "172.30.71.92"
end
config service group
 edit 1
    set status enable
    set base-mgmt-internal-mac 00:09:0f:43:9d:7c
    set base-mgmt-internal-network 10.101.10.0 255.255.255.0
      config base-mgmt-interfaces
       edit "b1"
         set vlan-id 101
       next
       edit "b2"
```

```
set vlan-id 101
        next
      end
   set base-mgmt-interface-mode active-active
    set elbc-base-ctrl-network 10.101.11.0 255.255.255.0
      config elbc-base-ctrl-interfaces
        edit "b1"
          set vlan-id 301
        next
        edit "b2"
          set vlan-id 301
        next
      end
      config slots
        edit 3
        next
        edit 4
        next
        edit 5
        next
        edit 6
        next
      end
      config traffic-interface
        edit "internal"
            set interface "f1" "f2"
          set port-mac-address 00:09:0f:ec:0b:73
        next
        edit "external"
            set interface "f3" "f4"
          set port-mac-address 00:09:0f:ec:0b:74
        next
      end
   set base-mgmt-external-ip 10.100.23.222 255.255.255.0
   set elbc-base-ctrl-interface-mode active-active
   set base-mgmt-allowaccess ping https ssh snmp telnet http fgfm
 next
 edit 2
 next
end
```

## Slave FortiSwitch Chassis 16 Slot 1 Configuration Example

```
config system global
  set hostname "c16s01"
  set service-group-mode 2-port-lag
  set service-group-hash-size expanded
end
config system interface
  edit "mgmt"
    set ip 10.100.23.221 255.255.255.0
    set allowaccess ping https ssh snmp telnet http
  next
  edit "base-mgmt"
  next
end
config route static
  edit 1
    set gateway 10.100.23.254
  next
end
config admin user
  edit "admin"
  next
end
config system ha
  set mode a-p
  set password ENC
7vXgU5gIGwe4iT9Lor/eVNgL2jNlNk+f0zMa7WJry7nTqhz9AI8B0iR8bH/D4/ePkY3
kmttyaTNlmKZEbZPz50zUETDUVZKJfj7jPi89kaoV3a+5
  set group-id 22
  set priority 100
  set hbdev-vlan-id 999
  set chassis-redundancy enable
  set chassis-id 2
    set hbdev "b1" "b2"
end
config system central-management
  set fmg "172.30.71.92"
end
config service group
  edit 1
    set status enable
    set base-mgmt-internal-mac 00:09:0f:43:9d:d4
    set base-mgmt-internal-network 10.101.10.0 255.255.255.0
      config base-mgmt-interfaces
       edit "b1"
         set vlan-id 101
       next
```

```
edit "b2"
          set vlan-id 101
        next
      end
    set base-mgmt-interface-mode active-active
    set elbc-base-ctrl-network 10.101.11.0 255.255.255.0
      config elbc-base-ctrl-interfaces
        edit "b1"
          set vlan-id 301
        next
        edit "b2"
          set vlan-id 301
        next
      end
      config slots
        edit 3
        next
        edit 4
        next
        edit 5
        next
        edit 6
        next
      end
      config traffic-interface
        edit "internal"
            set interface "f1" "f2"
          set port-mac-address 00:09:0f:ec:0b:73
        next
        edit "external"
            set interface "f3" "f4"
          set port-mac-address 00:09:0f:ec:0b:74
        next
      end
    set base-mgmt-external-ip 10.100.23.222 255.255.255.0
    set elbc-base-ctrl-interface-mode active-active
    set base-mgmt-allowaccess ping https ssh snmp telnet http fgfm
  next
  edit 2
 next
end
```

## Slave FortiSwitch Chassis 16 Slot 2 Configuration Example

```
config system global
  set hostname "c16s02"
  set service-group-mode 2-port-lag
  set service-group-hash-size expanded
end
config system interface
  edit "mgmt"
    set ip 10.100.23.221 255.255.255.0
    set allowaccess ping https ssh snmp telnet http
  next
  edit "base-mgmt"
  next
end
config route static
  edit 1
    set gateway 10.100.23.254
  next
end
config admin user
  edit "admin"
  next
end
config system ha
  set mode a-p
  set password ENC
7vXgU5gIGwe4iT9Lor/eVNgL2jNlNk+f0zMa7WJry7nTqhz9AI8B0iR8bH/D4/ePkY3
kmttyaTNlmKZEbZPz50zUETDUVZKJfj7jPi89kaoV3a+5
  set group-id 22
  set priority 100
  set hbdev-vlan-id 999
  set chassis-redundancy enable
  set chassis-id 2
    set hbdev "b1" "b2"
end
config system central-management
  set fmg "172.30.71.92"
end
config service group
  edit 1
    set status enable
    set base-mgmt-internal-mac 00:09:0f:43:9d:c0
    set base-mgmt-internal-network 10.101.10.0 255.255.255.0
      config base-mgmt-interfaces
       edit "b1"
         set vlan-id 101
       next
```

```
edit "b2"
          set vlan-id 101
        next
      end
    set base-mgmt-interface-mode active-active
    set elbc-base-ctrl-network 10.101.11.0 255.255.255.0
      config elbc-base-ctrl-interfaces
        edit "b1"
          set vlan-id 301
        next
        edit "b2"
          set vlan-id 301
        next
      end
      config slots
        edit 3
        next
        edit 4
        next
        edit 5
        next
        edit 6
        next
      end
      config traffic-interface
        edit "internal"
            set interface "f1" "f2"
          set port-mac-address 00:09:0f:ec:0b:73
        next
        edit "external"
            set interface "f3" "f4"
          set port-mac-address 00:09:0f:ec:0b:74
        next
      end
    set base-mgmt-external-ip 10.100.23.222 255.255.255.0
    set elbc-base-ctrl-interface-mode active-active
    set base-mgmt-allowaccess ping https ssh snmp telnet http fgfm
  next
  edit 2
 next
end
```

During initial switch deployment it is easy to make mistakes if copying configurations from the master switch to the slave. There are two methods to configure the switches. Method 1 is the safest however it requires all switches to be interconnected which may not be possible during an initial deployment.

### Method 1

Configure the master FortiSwitch

Enable Service Group Mode

- Set service-group-mode.
- Set service-group-hash-size [ basic | expanded ].
- Expanded allows for a 64 entry calendar vs 32 which provides a better hash distribution to security modules. It is limited to two service groups and supports SNAT, DNAT, NONAT.

Configure Service Group(s) (refer to section Understanding Service Groups)

**Configure HA** 

- **IMPORTANT**: **chassis-id** is set to **1** by default. This ID sets into place the preset IP addresses that are configured for each FortiGate. For example chassis-id 1 slot-3's base-mgmt IP is 10.101.10.3 while chassis-id 2 slot-3's base-mgmt IP is 10.101.10.103. If both chassis IDs are set to 1 there will be an IP conflict between the FortiGates that will break synchronization.
- Always set the **password** and **group-id** to avoid conflicts if there are multiple clusters of chassis.
- In an inter-chassis HA deployment set the Master chassis HA priority higher than the slave chassis.
- Enable **chassis-redundancy** and set **hbdev** ports to use **b1** or **b2** or both.

Configure all Slave FortSwitches

Slave FortiSwitches includes the switch that is located in slot-2 of the master chassis as well all switches across chassis.

- Configure HA
- **IMPORTANT**: The slave switch in the master chassis has the same HA settings as slot-1 including its priority number.

- **IMPORTANT**: All switches in the slave chassis have their **chassis-id** set to **2**.
- **NOTE**: The HA **boot-holddown** timer is used to mitigate an external switch's Spanning Tree blocked ports upon link-up. The timer prevents FortiSwitches to assume master immediately upon boot for the specified period unless a neighbor has been detected or the timer expires. Spanning Tree's default block port time is 30 seconds while the boot-holddown's default timer is 40.

## Method 2

This method is used to configure inter-chassis HA but the chassis are not physically interconnected at time of setup. Once completed, the chassis can be interconnected at a later time.

Follow all master configuration directions in method 1.

- Copy and paste the master configuration into all other FortiSwitches.
- Service groups in all FortiSwitches contain the same configuration except for the MAC address of the base-mgmt-internal interface. This interface is used for remote management access of individual slots. Only the master switch responds to ARPs for the base-mgmt IP address and each switch will contain a different MAC address.
- The MAC address that belongs to the base-mgmt-internal interface in service group 1 can be found with the following command.

c16s02 # diagnose switch base-channel mac-address MAC: 00:09:0f:43:9d:c0 VLAN: **101** Port: base-mgmt(port-Id 25)

- In service group 1 issue the command **set base-mgmt-internal-mac 00:09:0f:43:9d:c0** to replace the copied MAC.
- For each additional service group, increment the 5<sup>th</sup> octet of the mac address by one. For example service group 2's MAC address would be 00:09:0f:43:9**e**:c0.

Follow the section 'Configure All Slave FortiSwitches' in method 1.

 NOTE: A common mistake is forgetting to change the chassis ID. This causes both chassis to produce a master FortiGate. In turn configuration sync will not occur across chassis. All heart beat interfaces between different FortiSwitches must be interconnected. If there is only one chassis and two FortiSwitch, slot-1 and slot-2 must still be connected externally to each other. Heartbeats are sent from an interface that is tagged VLAN 999. If required, change the VLAN ID and ensure that ports from external switches are set to VLAN trunk.

Generally the same interface will be used for base management, ELBC control and HA heartbeats. Each type of traffic resides on a different VLAN ID so VLAN trunks must account for this variable. Each service group also varies the base-mgmt and ELBC control VLAN ID by one.

Ports used for HA are mgmt, B1 or B2 or both depending on the configuration.

#### Verification

HA packets are broadcasted between all FortiSwitches that are participating within a cluster. These packets traverse the heart beat virtual interface. There is one HA interface per service group. Interfaces for each FortiSwitch can be found by looking at the network interface list.

The IP address 169.254.128.233 is used to exchange heartbeats in chassis 15 slot 1.

c15s01 **# diagnose network interface list** HA\_01\_28 Link encap:Ethernet HWaddr 00:09:0F:ED:0B:8F inet addr:169.254.128.233 Bcast:169.254.128.239 Mask:255.255.255.248 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:3322138 errors:0 dropped:0 overruns:0 frame:0 TX packets:2884413 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:2093765575 (1.9 GiB) TX bytes:2096032240 (1.9 GiB)

Heartbeats are sent between all FortiSwitch blades using the HA interface.

c15s01 **# diagnose sniffer packet HA\_01\_28 "** interfaces=[HA\_01\_28] filters=[] 0.583080 169.254.128.234.32789 -> 169.254.128.233.720: 2460564698 ack 2475492712 0.583094 169.254.128.233.720 -> 169.254.128.234.32789: ack 2460564698 0.820242 169.254.128.235.32815 -> 169.254.128.233.720: 2446268340 ack 2431857109 0.820256 169.254.128.233.720 -> 169.254.128.235.32815: ack 2446269788 0.877035 169.254.128.233.720 -> 169.254.128.236.32817: psh 2416849431 ack 2437782090

#### **Troubleshooting FortiSwitch HA**

#### **Misconfiguration**

Misconfiguration of chassis IDs can lead to synchronization issues of FortiGate blades. The chassis IDs are used to distinguish automatic configuration of FortiGate IP addresses within each chassis.

For Example: A chassis with an ID of 1 uses IP addresses that range between 1-16 while a chassis ID of 2 uses an IP range of 101-116 for internal IP addresses.

Below is an example misconfiguration.

• All FortiSwitch blades have the same chassis ID. Although the chassis ID is wrong, HA status will still show that there is only one master FS.

```
c15s01 # diagnose system ha status
c15s01(FS503B3E11700005), Master(priority=0), ip=169.254.128.233,
chassis=1(1)
sync: conf_sync=1, elbc_sync=1
c15s02(FS503B3E11700244), Slave(priority=1), chassis=1(1)
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
c16s02(FS503B3E11700261), Slave(priority=2), chassis=1(1)
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
c16s01(FS503B3E11700266), Slave(priority=3), chassis=1(1)
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
```

• Service group status shows that output in different chassis claiming the ELBC Master Blade is in local slot-3. This means a change of configuration to the FortiGate on the master chassis will not be reflected to the FortiGates in the slave chassis. This is because both chassis claim to have a master FortiGate.

```
c15s01 # get service group status
Service Group: 1
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
Working: 2 [ 2 Active 0 Standby]
c16s02 # get service group status
Service Group: 1
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
Working: 2 [ 2 Active 0 Standby]
```

• A split brain for the service group's base-mgmt-internal-network IP address will occur resulting in sporadic connectivity to the security blades. The output below shows intermittent connectivity between the master and slave chassis.

64 bytes from 10.100.23.222: icmp\_seq=0 ttl=252 time=42.008 ms Request timeout for icmp\_seq 1 Request timeout for icmp\_seq 2 64 bytes from 10.100.23.222: icmp\_seq=4 ttl=252 time=26.247 ms 64 bytes from 10.100.23.222: icmp\_seq=5 ttl=252 time=27.150 ms

• Packet sniffing on all the FortiSwitches will reveal that switches in two different chassis are receiving and responding to ICMP requests when pinging the service group's base-mgmt-internal IP.

```
c15s01 # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
0.140251 10.69.69.2 -> 10.100.23.222: icmp: echo request
0.140262 10.101.10.15 -> 10.101.10.3: icmp: echo request
0.140264 10.101.10.15 -> 10.101.10.3: icmp: echo request
```

```
c16s01 # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
0.142576 10.101.10.3 -> 10.101.10.15: icmp: echo reply
1.144799 10.101.10.3 -> 10.101.10.15: icmp: echo reply
```

• A proper ICMP response should only be responding from a single master FortiGate and coming from through master FortiSwitch. The master FortiGate below has an IP address of 10.101.10.3. The IP address 3 signifies that traffic is coming from a chassis with ID of 1.

```
15s01 # diagnose sniffer packet any 'icmp' 4
interfaces=[any]
filters=[icmp]
6.604791 10.69.69.2 -> 10.100.23.222: icmp: echo request
6.604819 10.101.10.15 -> 10.101.10.3: icmp: echo request
6.604821 10.101.10.15 -> 10.101.10.3: icmp: echo request
6.605087 10.101.10.3 -> 10.101.10.15: icmp: echo reply
6.605096 10.100.23.222 -> 10.69.69.2: icmp: echo reply
```

• When the HA chassis-id is set properly the slave chassis should show N/A for it's ELBC Master Blade and the master chassis configuration sync blade will be displayed. Configuration sync occurs through the cross connected interfaces of the FortiSwitches. This is generally the B1 or B2 interface and sometimes the management interface depending on the configuration. The amount of throughput that can traverse an inter-chassis design can exceed 1 Gbps, it is recommended to use the 10 Gbps interfaces B1 or B2 as opposed to the mgmt interface on the FortiSwitch.

c15s01 **# get service group status** Service Group: 1 **ELBC Master Blade: slot-3** Confsync Master Blade: slot-3 Blades: Working: 2 [ 2 Active 0 Standby] c16s02 **#** get service group status Service Group: 1 **ELBC Master Blade: N/A** Confsync Master Blade: slot-3 Blades: Working: 2 [ 2 Active 0 Standby]

When a FortiSwitch leaves the cluster for any reason, heartbeat messages will result.

Debug command to show a FortiSwitch leaving and joining a cluster. Serial numbers are used to determine the FortiSwitch in question.

#### c15s01 # diagnose debug application fswhbd 255 c15s01 # diagnose debug enable c15s01 # \_\_fsw\_process\_hb\_packet 958 0:0 role change [fsw\_ha\_select\_best\_hbdev:1110] no change best(0)[b1] \_\_fsw\_process\_hb\_packet 958 0:0 role change [fsw\_ha\_select\_best\_hbdev:1110] no change best(0)[b1] \_\_fsw\_process\_hb\_packet 958 0:0 role change [fsw\_ha\_select\_best\_hbdev:1110] no change best(0)[b1] memeber 'FS503B3E11700261' hb failure on hbdev 0:b1 last\_hb(710904.4) now(710905.38) ←heart beat failure detected while rebooting memeber 'FS503B3E11700261' hb failure on hbdev 1:b2 last\_hb(710904.4) now(710905.38) member 'FS503B3E11700261' is gone now(710905.38) ← FS deemed down member 'FS503B3E11700261' deleted ← FS removed from cluster \_\_fsw\_hb\_check 582 role change [fsw\_ha\_select\_best\_hbdev:1110] no change best(0)[b1] [fsw\_ha\_select\_best\_hbdev:1110] no change best(0)[b1] new member 'FS503B3E11700261' added (710991.87) ← FS booted and joined cluster \_\_fsw\_process\_hb\_packet 958 0:0 role change [fsw\_ha\_select\_best\_hbdev:1110] no change best(0)[b1]
Communication between the master FortiSwitch and all slave FortiSwitches. Use this command to verify if one FS is not sending heartbeats by looking for the missing serial number.

```
c15s01 # diagnose sniffer packet HA 01 28 " 3
interfaces=[HA_01_28]
filters=[]
pcap lookupnet: HA 01 29: no IPv4 address assigned
0.170714 Ether type 0x9890 printer havn't been added to sniffer.
0x0000 ffff ffff ffff 0009 0fed 0b90 9890 0101
0x0010 4653 3530 3342 3345 3131 3730 3030 3035 FS503B3E11700005
0x0020 6331 3573 3031 0000 0000 0000 0000 0000 c15s01......
0.218687 Ether type 0x9890 printer havn't been added to sniffer.
0x0000 ffff ffff ffff 0009 0f44 9dde 9890 0101
                                                   .....D.....
0x0010 4653 3530 3342 3345 3131 3730 3032 3631 FS503B3E11700261
0x0020 6331 3673 3032 0000 0000 0000 0000 0000 c16s02.....
0.271316 Ether type 0x9890 printer havn't been added to sniffer.
0x0000 ffff ffff ffff 0009 0f44 9d9a 9890 0101
                                                   .....D.....
0x0010 4653 3530 3342 3345 3131 3730 3032 3434 FS503B3E11700244
0x0020 6331 3573 3032 0000 0000 0000 0000 0000 c15s02.....
0.343475 Ether type 0x9890 printer havn't been added to sniffer.
0x0000 ffff ffff 6009 0f44 9df2 9890 0101......D.....
0x0010 4653 3530 3342 3345 3131 3730 3032 3636 FS503B3E11700266
0x0020 6331 3673 3031 0000 0000 0000 0000 0000 c16s01.....
```

## **Constant Failover During Testing**

During Lab test it is common to see multiple failover attempts between chassis within a short amount of time. This type of testing although useful is not indicative of a real world situation and may create problems. Being aware of this behavior will set expectations for future testing.

- As with a traditional FortiGate HA Active-Passive configuration, there is a HA uptime difference margin timer of 5 minutes that affects how the state of two FortiSwitches that is in HA behaves after boot.
- The time difference between two HA switches must be greater than 5 minutes else the master election switch will be based upon priority setting and not the device that has been up longest. This timer is useful in cases where both the master and slave switches are rebooted at roughly the same time and guarantees that the higher priority switch will be master.
- Reboot of HA switches in testing with an interval of less that 5 minutes of a previous reboot may yield in the higher priority switch always remaining master or taking back master state.
- Constant failovers while testing may also yield in old sessions building up on FortiGates that could eventually lead to conserve mode.

#### HA Failover Order

Hardware, port and software failures that affect the health status of a cluster will cause an HA failover. Failures are shown below in the state section for workers and interface.

• A difference in state between the FortiSwitches in the master and slave chassis will cause an HA event to occur. The device chassis with the least failed state will become master.

```
c15s01(FS503B3E11700005), Master(priority=0), ip=169.254.128.177, uptime=17400.56, chassis=1(1)
 sync: conf_sync=1, elbc_sync=1
 state: worker_failure=0/4, intf_state=(total/good/down/bad-score)=2/2/0/0, force-state(1:force-to-
master)
 hbdevs: local_interface= b1 best=yes
     local interface= b2 best=no
c15s02(FS503B3E11700244), Slave(priority=1), ip=169.254.128.178, uptime=102223.38, chassis=1(1)
 sync: conf_sync=1, elbc_sync=1, conn=3(connected)
 state: worker_failure=0/4, intf_state=(total/good/down/bad-score)=2/2/2/0, force-state(1:force-to-
master)
 hbdevs: local_interface= b1 last_hb_time=102265.46 status=alive
     local_interface= b2 last_hb_time= 0.00 status=dead
c16s02(FS503B3E11700261), Slave(priority=3), ip=169.254.128.180, uptime=102220.61, chassis=2(1)
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
 state: worker_failure=0/4, intf_state=(total/good/down/bad-score)=2/2/2/0, force-state(-1:force-to-
slave)
 hbdevs: local_interface= b1 last_hb_time=102265.52 status=alive
     local_interface= b2 last_hb_time=20550.43 status=dead
c16s01(FS503B3E11700266), Slave(priority=2), ip=169.254.128.179, uptime=16572.06, chassis=2(1)
 sync: conf_sync=1, elbc_sync=1, conn=3(connected)
 state: worker_failure=0/4, intf_state=(total/good/down/bad-score)=2/2/0/0, force-state(-1:force-to-
slave)
 hbdevs: local_interface=
                          b1 last_hb_time=102265.36 status=alive
     local_interface= b2 last_hb_time=20550.43 status=dead
```

Service groups are used to distinguish between multiple security clusters within a given chassis. Depending on the number of service groups supported, different FortiGates can be put in different service groups to form independent security clusters. A FortiGate can only belong to only one service group. The number of service groups supported is directly tied to the number of external physical interfaces on the switch. There are three service group modes supported.

The mode can be set within global configuration: **set service-group mode**.

- Basic Mode (no lag) requires one internal and one external port per service group. With 8 ports total, basic mode allows for four service groups.
- 2-Port link aggregation requires two internal ports and two external ports per service groups yielding a maximum of two service groups.
- 4-Port link aggregation requires four internal ports and four external ports using up all eight front interfaces. This yields in a maximum of one service group.
- All port pairs are preconfigured, any port to any port is not supported Example: port1 cannot be paired with port 5.

Internal=Blue, External=Red, Base=Green (Left to Right F1-F8, B1 & B2)



Figure 5-3-2 Two-Port LAG



#### Figure 5-3-3 Four-Port LAG



• Hash table calendar size also determines the maximum amount of service groups allowed. Setting the size to basic allows for 32 calendar entries while

expanded allows for 64 entries. More entries equate to better load distribution between security blades.

- Basic Hash supports four service groups. Basic Mode supports SNAT or DNAT.
- Expanded Hash supports two service groups. Expanded mode supports SNAT, DNAT or NONAT.

```
config system global
set service-group-mode 2-port-lag
set service-group-hash-size expanded
end
```

• A service group configuration with a two-port lag and expanded hash looks like the following.

```
config service group
  edit 1
    set status enable
    set base-mgmt-internal-mac 00:09:0f:ec:0b:72
    set base-mgmt-internal-network 10.101.10.0 255.255.255.0
    set elbc-base-ctrl-network 10.101.11.0 255.255.255.0
    config slots
        edit 3
        next
        edit 4
        next
        edit 5
        next
        edit 6
        next
      end
   config traffic-interface
        edit "internal"
            set interface "f1" "f2"
          set port-mac-address 00:09:0f:43:9d:c1
        next
        edit "external"
            set interface "f3" "f4"
          set port-mac-address 00:09:0f:43:9d:c2
        next
      end
    set base-mgmt-external-ip 192.168.1.101 255.255.255.0
next
end
```

- As stated in the HA section, all FortiSwitch devices need to be interconnected for HA operations to function. The same physical connection is used to manage all FortiGates across chassis and to perform configuration and session sync between security blades.
- Inter-chassis deployments require additional configurations with the service group. The **base-mgmt-interface** and **elbc-base-ctrl-interfaces** needs to be

added into the configuration. Any external switch that sits between these interfaces are required to have VLAN Trunks enabled with the proper access list.

• Set the base-mgmt and elbc-base-ctrl modes to active-active. This configuration is used to determine how b1 and b2 interfaces are utilized should one fail. In the default active-passive mode all FortiSwitches will send and listen on their primary interface b1. In active-active mode b1 is preferred but each FortiSwitch will also listen on its b2 interface. This command is not associated with Inter-chassis HA between FortiSwitch devices.

```
config service group
edit 1
set base-mgmt-interface-mode active-active
set elbc-base-ctrl-interface-mode active-active
next
end
```

The charts below display the result of a down port relative to the state of configuration sync.

In this scenario there are four FortiSwitches. Each FortiSwitch has its b1 and b2 interfaces connected to external switches used for heartbeats.

Base Interface Mode: Active-Passive u = interface up, d = interface down YES = Configuration Sync Works, No = Configuration Doesn't Work

Chart 1-1-1 shows various scenarios in which a single or multiple "b" interface fails. Assuming that c15s01 is the master FortiSwitch, when it's b1 interface goes down management and sync traffic will traverse b2. However, in A/P mode, all other FortiSwitches will only listen out of their primary active interface b1. Hence, scenario B-E shows configuration sync not working. Chart 5-3-1

Scenario A			
c15s01b1	u	c16s01b1	u
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	YES		
Scenario B			
c15s01b1	d	c16s01b1	u
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	NO		
Scenario C			
c15s01b1	u	c16s01b1	u
c15s01b2	d	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	NO		
Scenario D			
c15s01b1	u	c16s01b1	d
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	NO		
Scenario E			
c15s01b1	u	c16s01b1	d
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	d
c15s02b2	u	c16s02b2	u
Conf Sync	NO		

## Base Interface Mode: Active-Active

Chart 5-3-1 shows various scenarios in which a single or multiple "b" interface fails. Assuming that c15s01 is the master FortiSwitch, when it's b1 interface goes down management and sync traffic will traverse b2. In A/A mode, all other FortiSwitches will listen on both "b" interfaces to allow for management and configuration sync.

Chart 5-3-2				
	Scenario A			
	c15s01b1	u	c16s01b1	u
	c15s01b2	u	c16s01b2	u
	c15s02b1	u	c16s02b1	u
	c15s02b2	u	c16s02b2	u
	Conf Sync	YES		
	_			
	Scenario B			
	c15s01b1	d	c16s01b1	u
	c15s01b2	u	c16s01b2	u
	c15s02b1	u	c16s02b1	u
	c15s02b2	u	c16s02b2	u
	Conf Sync	YES		
	Scenario C			
	c15s01h1	11	c16s01h1	11
	c15s01b1	d	c16s01b1	u 11
	c15s01b2	u 11	c16s02b1	u 11
	c15s02b1	u	c16s02b1	u
	Conf Sync	YES	01030202	u
		-		
	Scenario D			
	c15s01b1	u	c16s01b1	d
	c15s01b2	u	c16s01b2	u
	c15s02b1	u	c16s02b1	u
	c15s02b2	u	c16s02b2	u
	Conf Sync	YES		
	Commis E			
	Scenario E		-1(-01)-1	J.
	c15sU1D1	u		a
	c15s01b2	u	C16SU1D2	u
	c15s02b1	u	c16s02b1	d
	c15s02b2	u	c16s02b2	u
	Conf Sync	YES		

Use A/P mode only when cables are directly connected between two FortiSwitches. However, it is recommended to use A/A for all cases.

• The base-mgmt-interface is used to communicate to all blades in the second chassis by leapfrogging through the first. Since ELBCv3 supports active-passive HA, only the master FortiSwitch in the master chassis will answer to management requests.

The diagram below depicts a management connection to slot-4 using IP address 10.101.23.221 via HTTP port 8004. The connection is PAT to 10.101.10.4 to access slot-4.



The diagram below depicts a management connection to slot-4 using IP address 10.101.23.221 via HTTP port 8024. The connection is PAT to 10.101.10.104 to access slot-4. Only the master FortiSwitch responds to management requests. Translation occurs on the master switch and traffic traverses the b1 or b2 interface to reach slot-4.





When an external switch is used to connect b1 and b2, verify its VLAN configuration is setup properly by pinging from the master FS to any base-mgmt IP address on the slave chassis.

c15s01 # execute ping 10.101.10.103 PING 10.101.10.103 (10.101.10.103): 56 data bytes 64 bytes from 10.101.10.103: seq=0 ttl=255 time=1.438 ms 64 bytes from 10.101.10.103: seq=1 ttl=255 time=0.098 ms

If a response does not occur, verify the FS and external switch VLAN configuration.

• The elbc-base-ctrl-interface is used to perform configuration sync between the Master FortiGate and all slave FortiGates in the second chassis. It is also where session sync of security blades occurs. Session sync is performed between a single FortiGate slot in the master chassis to the same slot number in the slave chassis. Session sync is never performed with blades in the same chassis.

```
config service group
  edit 1
      config base-mgmt-interfaces
        edit "b1"
          set vlan-id 101
        next
        edit "b2"
          set vlan-id 101
        next
      end
      config elbc-base-ctrl-interfaces
        edit "b1"
          set vlan-id 301
        next
        edit "b2"
          set vlan-id 301
        next
      end
```

Below depicts session sync between security blades in an HA cluster.





The elbc-base-ctrl VLAN configuration can be verified by pinging a FortiGate in the slave chassis from a FortiGate in the master chassis. To do so the elbc-base-ctrl interface in each FortiGate must be independently set to allow ping. Configuration sync does not make changes to this interface.

```
config system interface

edit "elbc-base-ctrl"

set vdom "elbc-mgmt"

set ip 10.101.11.3 255.255.255.0

set allowaccess ping

next

end

c15s01 # execute ping 10.101.11.103

PING 10.101.11.103 (10.101.11.103): 56 data bytes

64 bytes from 10.101.11.103: seq=0 ttl=255 time=1.438 ms

64 bytes from 10.101.11.103: seq=1 ttl=255 time=0.098 ms
```

If a response does not occur, verify the FS and external switch VLAN configuration.

Managing individual blades within a service group is performed by accessing the base-mgmt-external-ip and using the access port numbers listed below. Ensure that the proper allow access configuration is in place. Setting the allow access rules within the service group will automatically configure the FortiGate accordingly. There is no need to individually set management access rules on each FortiGate.

```
config service group
set base-mgmt-external-ip 10.100.23.222 255.255.255.0
set base-mgmt-allowaccess ping https ssh snmp telnet http fgfm
end
```

- The FortiSwitch uses the externally accessible base-mgmt-external-ip address to port map to any slots unique internal IP address.
- If no ports are specified, management access is redirected to the master FortiGate.
- Since all ingress management traffic is translated, FortiGate event logs will show that management access originates from the FortiSwitch's base-mgmt interface.
- FortiGates have **Redirect to HTTPS** by default; disable that option under **Admin Settings** to access HTTP.

## Example: https://10.100.23.222:44301 ssh -p 2230 admin@10.100.23.222 snmpwalk -v 2c -c password 10.100.23.222:16101

Chart 5-3-3

Chassis ID 1	Internal IP	Individual Access Port	Chassis ID 2	Internal IP	Individual Access Port
Slot 1	10.101.10.15	16101,2201,8001,44301	Slot 1	10.101.10.115	16121,2221,8021,44321
Slot 2	10.101.10.16	16102,2202,8002,44302	Slot 2	10.101.10.116	16122,2222,8022,44322
Slot 3	10.101.10.3	16103,2203,8003,44303	Slot 3	10.101.10.103	16123,2223,8023,44323
Slot 4	10.101.10.4	16104,2204,8004,44304	Slot 4	10.101.10.104	16124,2224,8024,44324
Slot 5	10.101.10.5	16105,2205,8005,44305	Slot 5	10.101.10.105	16125,2225,8025,44325
Slot 6	10.101.10.6	16106,2206,8006,44306	Slot 6	10.101.10.106	16126,2226,8026,44326
Slot 7	10.101.10.7	16107,2207,8007,44307	Slot 7	10.101.10.107	16127,2227,8027,44327
Slot 8	10.101.10.8	16108,2208,8008,44308	Slot 8	10.101.10.108	16128,2228,8028,44328
Slot 9	10.101.10.9	16109,2209,8009,44309	Slot 9	10.101.10.109	16129,2229,8029,44329

Slot 10	10.101.10.10	16110,2210,8010,44310	Slot 10	10.101.10.110	16130,2230,8030,44330
Slot 11	10.101.10.11	16111,2211,8011,44311	Slot 11	10.101.10.111	16131,2231,8031,44331
Slot 12	10.101.10.12	16112,2212,8012,44312	Slot 12	10.101.10.112	16132,2232,8032,44332
Slot 13	10.101.10.13	16113,2210,8013,44313	Slot 13	10.101.10.113	16133,2233,8033,44333
Slot 14	10.101.10.14	16114,2214,8014,44314	Slot 14	10.101.10.114	16134,2234,8034,44334

### **Troubleshooting Service Groups**

A FortiGate can only belong to one service group. Up to 12 FortiGates can be added to a single service group. Once a slot is added it is automatically configured with IP addresses to join and communicate with the FortiSwitch and Master FortiGate.

- FortiGates **base-mgmt** and **elbc-base-ctrl** IP addresses will be populated with predefined values. The last octet is defined by the FortiSwitch's chassis ID and FortiGates slot position.
- If a security blade is removed from the service group, the IP addresses associated with ELBC management and control are immediately revoked. However, all prior configurations are still retained. The revoked security blade will no longer perform any configuration sync to the master FortiGate.
- Status of individual security blades within a service group can be viewed from every switch. It is a good idea to poll the status of service groups from every FortiSwitch when troubleshooting a problem. There could be scenarios in which one FortiSwitch detects a particular FortiGate properly and another FortiSwitch does not.

c15s01 # get service group status Service Group: 1 ELBC Master Blade: slot-3 Confsync Master Blade: slot-3 Blades: Working: 4 [ 4 Active 0 Standby] Ready: 0 [ 0 Active 0 Standby] Dead: 0 [ 0 Active 0 Standby] Total: 4 [ 4 Active 0 Standby] Slot 3: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Management: Good Data: Good Status Message:"Running" Slot 4: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Management: Good Data: Good Status Message:"Running"

Slot 5: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Management: Good Data: Good Status Message:"Running" Slot 6: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Good Data: Good Status Message:"Running"

c16s01 **# get service group status** Service Group: 1 ELBC Master Blade: slot-3 Confsync Master Blade: N/A Blades: Working: 4 [ 4 Active 0 Standby] Ready: 0 [ 0 Active 0 Standby] Dead: 0 [ 0 Active 0 Standby] Total: 4 [ 4 Active 0 Standby]

Slot 3: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Good Data: Good Status Message:"Running" Slot 4: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Good Data: Good Status Message:"Running" Slot 5: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Good Data: Good Status Message:"Running" Slot 6: Status:Working Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Good Data: Good Status Message:"Running"

- There are multiple iterations of status messages for **get service group status** based on the state of communication between the FortiSwitch and FortiGate.
- ELBC and Confsync: slot-3 below signifies that c15s01 is the master chassis. Under normal circumstances, the first configured slot number in the service group in the master chassis is the master FortiGate. An easy way to tell which chassis contains the master FortiGate is when both **ELBC Master Blade** and **Confsync Master Blade** list the same FortiGate.

c15s01 **# get service group status** Service Group: 1 ELBC Master Blade: slot-3 Confsync Master Blade: slot-3

• C16s01 below shows that the config sync status is NA. This signifies that the configuration sync master blade is not part of chassis 16.

c16s01 **# get service group status** Service Group: 1 ELBC Master Blade: slot-3 Confsync Master Blade: N/A

• The master FortiSwitch will show it's Base channel as up since it is used for external management access. The slave FortiSwitch in the same chassis will show the base Channels to the slots as down to avoid a split brain of management access. The Fabric data path ports should always show status up unless there is a problem.

c15s01 **# get service group status** Service Group: 1 Slot 6: Status:Working Function:Active Link: Base: **Up** Fabric: **Up** Heartbeat: Management: Good Data: Good Status Message:"Running"

c15s02 **# get service group status** Service Group: 1 Slot 6: Status:Working Function:Active Link: Base: **Down** Fabric: **Up** Heartbeat: Management: Good Data: Good Status Message:"Running"

• In the slave chassis, which ever FortiSwitch that is responding to interchassis communication for the FortiGates will have it's Base interface status up.

c16s01 **# get service group status** Service Group: 1 Slot 6: Status:Working Function:Active Link: Base: **Up** Fabric: **Up** Heartbeat: Management: Good Data: Good Status Message:"Running"

c16s02 **# get service group status** Service Group: 1 Slot 6: Status:Working Function:Active Link: Base: **Down** Fabric: **Up** Heartbeat: Management: Good Data: Good Status Message:"Running"

There are various status messages for a FortiGate slot during the cluster joining process or during communication errors.

• Slot is down, turned off or not working. Verify the slot is receiving power, the card is fully inserted and boot or reboot the FortiGate.

Slot 6: Status:Dead Function:Active Link: Base: Down Fabric: Down Heartbeat: Managment: Failed Data: Failed Status Message:"Waiting for fabric channel link."

• Slot is booting up but has not send any heartbeats to the FortiSwitch. Wait for the heartbeats to be sent.

Slot 6: Status:Dead Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Failed Data: Failed Status Message:"Waiting for management heartbeat."

• Heartbeats have been sent and recognized however the slot has not or unsuccessfully synchronized it's configuration with the master. Upon a full reboot, security blades are not allowed to join the master until it's configuration has been synced. In the case where configuration sync has occurred but became unsynced due to a configuration change, the FortiGate is still allowed to stay in the cluster and pass traffic.

Slot 6: Status:Dead Function:Active Link: Base: Up Fabric: Up Heartbeat: Managment: Good Data: Failed Status Message:"Waiting for configuration sync."

• Configuration has synced and the blade is allowed to join the cluster.

Slot 6: Status:Working Function:Active Link: Base: Up Fabric: Up Heartbeat: Managment: Good Data: Good Status Message:"Running"

Additional Status Message.

• The following message shows that the FortiGate has not sent any heartbeat messages to the FortiSwitch. These packets are used to determine if the data path is working and are required to achieve running state.

Slot 5: Status:Dead Function:Active Link: Base: Down Fabric: Up Heartbeat: Managment: Good Data: Failed Status Message:"Waiting for data heartbeat."

• In the FortiGate that is showing "Waiting for data hearbeat," run a packet sniff to determine if it is sending out any heartbeat packets. Be sure to sniff the interface connected to the proper FortiSwitch: elbc-ctrl/1 pertains to switch slot 1 and elbc-ctrl/2 switch slot 2.

From the packet sniff below notice the MAC address **01-80-c2-00-00-0c**. The address is used for heartbeats. If a configured elbc-ctrl slot is not sending messages every few seconds it will not be permitted to join the cluster. The serial number **FG-5KB3E11700411** shown below belongs to the FortiGate that is sending heartbeats.

Below is an example of a good heartbeat message. If no messages are captured then the FortiGate is not sending the proper packets. A quick remediation may involve rebooting the FortiGate.

c15s05 (elbc-mgmt) # diagnose sniffer packet elbc-ctrl/1 '' 3 interfaces=[elbc-ctrl/1] filters=[]

0.801910 Ether type 0x8895 printer havn't been added to sniffer. 0x0000 **0180 c200 000c** 0009 0fff 44d7 8895 411c .....D..A. 0x0010 0000 0005 0146 472d 354b 4233 4531 3137 ....FG-5KB3E117 0x0020 3030 3431 3100 0000 0000 090f ff44 cd 00411.....D.

Installing a New FortiGate into an Existing Service Group

All FortiGate firewalls within the same service group must be of the same type. This allows for consistency of configuration, session and OS synchronization.

Installing a new FortiGate to an existing service group requires completing the followin1g steps.

• Add the new slot configuration parameters to the service group. In the following configuration example, slot-7 will be the new slot.

```
config service group
edit 1
config slots
edit 3
next
edit 4
next
edit 5
next
edit 6
next
edit 7
next
edit 7
next
end
```

• If desired, a slot order can be moved before or after an existing slot with the following command within the slot **config slots** section. This command is useful if a slot must be completely removed then reinstalled for troubleshooting purposes.

(slots)# move 4 before 5

- Install the FortiGate into the chassis at the newly configured slot. Verify that the IPM light changes from blue to green. Green indicates that the FortiGate has communicated successfully with the Shelf Manager. Blue indicates that the communication channel is not working. If the light is not green, verify the card is fully inserted and that the lever containing the micro switch is in it's locked position. Push the lever in towards the board. Please refer to the hardware installation guide found at <a href="http://kb.fortinet.com">http://kb.fortinet.com</a> for further information.
- Once the firewall has fully booted, reset its configuration to factory. This ensures that all prior configurations have been removed and allows for a shorter upgrade process to occur. Upgrade the operating system to match existing blades within the same cluster. Perform a second factory reset to ensure that any prior OS configuration conversions have been removed to avoid configuration synchronization issues.
- Follow the steps specified in the section ELBCv3 Installation within the FortiGate chapter to complete the process.

# FortiGate

All FortiGate firewalls participating in an ELBCv3 cluster must be installed with the same firmware. Each slave FortiGate will need to complete a configuration sync with the ELBC Master FortiGate before deeming itself ready to join the cluster. The chassis loadbalance (chlbd) process is used to synchronize with the ELBC Master. Once chlbd synchronization occurs, heartbeats are sent back to the FortiSwitch.

## **ELBCv3 Installation**

Enabling ELBC requires entering a small set of commands from a factory default configuration.

FG-5KB3E11700315**# conf system elbc** FG-5KB3E11700315 (elbc) **# set mode service-group** FG-5KB3E11700315 (elbc) **# end** This operation will reset your system to work in ELBC service-group mode. Please ensure the device supports ELBC service group mode. This operation will reboot the device. Do you want to continue? (y/n)y

The system is going down NOW !!

Please stand by while rebooting the system.

FG-5KB3E11700315 login: slave's configuration is not in sync with master's, sequence:0 slave's configuration is not in sync with master's, sequence:1 slave's configuration is not in sync with master's, sequence:4 slave starts to sync with master logout all admin users slave succeeded to sync with master

- Once configuration sync has successfully occurred the FortiGate joins the service group and is ready to process traffic.
- Verify that the FortiGate can see all neighbors and switches in the same chassis. The **diag sys fortiswitch-heartbeat status** command reveals information about whether the FortiGate's chassis is master or slave, which slot is master and all serial numbers of each FortiGate that has joined the cluster. If a configured slot number is missing, that slot has not joined the cluster or is having problems. The command does not reveal the status of any switch or FortiGate blades in another chassis.

• Channel-0 is the FortiSwitch in slot-1 and Channel-1 is the switch in slot-2.

```
c15s03 (global) # diagnose sys fortiswitch-heartbeat status
Heartbeat mode: 1 (service-group), Status: 3 (active)
Heartbeat Packet Interval: 0.2s
My Slot: 3
My Chassis: 1
Channel-0: flags(0xb)
  Status: enabled FSW-HB: good FSW-Active: no HB-Tx: enabled
  Heartbeat Packet Sending Device: elbc-ctrl/1 last rx=1
  Traffic Handling Devices: 2
   internal
    external
  Swdev: elbc-base-ctrl
  Slot Swdev MAC
                          Serial-Number
      ff:ff:ff:ff:ff:ff
                          N/A
   0
      ff:ff:ff:ff:ff
   1
                          N/A
   2
      ff:ff:ff:ff:ff:ff
                          N/A
                          FG-5KB3E11700407 ←MAC of Base1 MGMT
   3
      00:09:0f:ff:44:75
   4
      00:09:0f:43:96:39
                          FG-5KB3E11700636
      00:09:0f:ff:44:cd
   5
                          FG-5KB3E11700411
   6
      00:09:0f:4d:97:42
                          FG-5KB3E12700041
  7
      ff:ff:ff:ff:ff:ff
                          N/A
      ff:ff:ff:ff:ff
  8
                          N/A
      ff:ff:ff:ff:ff:ff
  9
                          N/A
  10
      ff:ff:ff:ff:ff
                          N/A
  11
      ff:ff:ff:ff:ff:ff
                          ,m-N/A
  12
      ff:ff:ff:ff:ff
                          N/A
  13
      ff:ff:ff:ff:ff
                          N/A
  14
      ff:ff:ff:ff:ff
                          N/A
  15
      ff:ff:ff:ff:ff
                          N/A
 Service Group: 1
 Active Slots: 00000078(1.3,1.4,1.5,1.6)
 Master Slot: 3
 Master Chassis: yes
Channel-1: flags(0xf)
  Status: enabled FSW-HB: good FSW-Active: yes HB-Tx: enabled
  Heartbeat Packet Sending Device: elbc-ctrl/2 last rx=16
  Traffic Handling Devices: 2
   internal
    external
  Swdev: elbc-base-ctrl
                          Serial-Number
  Slot Swdev MAC
  0 ff:ff:ff:ff:ff:ff
                          N/A
  1
      ff:ff:ff:ff:ff:ff
                          N/A
   2
      ff:ff:ff:ff:ff
                          N/A
   3
      00:09:0f:ff:44:75
                          FG-5KB3E11700407
      00:09:0f:43:96:39
                          FG-5KB3E11700636
   4
   5
      00:09:0f:ff:44:cd
                         FG-5KB3E11700411
      00:09:0f:4d:97:42
                          FG-5KB3E12700041
   6
      ff:ff:ff:ff:ff
   7
                          N/A
  8
      ff:ff:ff:ff:ff:ff
                          N/A
      ff:ff:ff:ff:ff:ff
   9
                          N/A
  10
      ff:ff:ff:ff:ff
                          N/A
  11
      ff:ff:ff:ff:ff
                          N/A
      ff:ff:ff:ff:ff
  12
                          N/A
  13
      ff:ff:ff:ff:ff:ff
                          N/A
  14
      ff:ff:ff:ff:ff
                          N/A
      ff:ff:ff:ff:ff
  15
                          N/A
  Service Group: 1
 Active Slots: 00000078(1.3,1.4,1.5,1.6)
```

```
Master Slot: 3
Master Chassis: yes
```

- Looking at configuration sync on a FortiGate will reveal all FortiGates in the entire cluster and whether any blades are out of sync. The result in\_sync=0 signifies out of sync.
- Only FortiGates that at least in **Waiting for configuration sync** state will appear. Any FortiGate that is completely down will not show up.

```
c15s03 (global) # diagnose sys confsync status
ELBC: svcgrp_id=1, slot_id=3
ELBC HB devs:
        elbc-ctrl/1: active=1, hb_count=61174
        elbc-ctrl/2: active=1, hb_count=61174
ELBC mgmt devs:
        elbc-base-ctrl: mgmtip_set=1
FG-5KB3E11700407, Master, uptime=61173.57, priority=0, slot_id=1:3, in_sync=1
FG-5KB3E11700315, Slave, uptime=2277.80, priority=103, slot_id=2:6, in_sync=0
         elbc-base-ctrl: state=3(connected), ip=169.254.1.106, last_hb_time=61241.69, hb_nr=22744
FG-5KB3E11700378, Slave, uptime=61149.56, priority=100, slot_id=2:3, in_sync=1
        elbc-base-ctrl: state=3(connected), ip=169.254.1.103, last_hb_time=61241.62, hb_nr=90648
FG-5KB3E11700411, Slave, uptime=61171.89, priority=2, slot_id=1:5, in_sync=1
         elbc-base-ctrl: state=3(connected), ip=169.254.1.5, last_hb_time=61241.72, hb_nr=45451
FG-5KB3E11700636, Slave, uptime=61174.27, priority=1, slot_id=1:4, in_sync=1
         elbc-base-ctrl: state=3(connected), ip=169.254.1.4, last_hb_time=61241.68, hb_nr=45453
FG-5KB3E12700001, Slave, uptime=61148.53, priority=101, slot_id=2:4, in_sync=1
         elbc-base-ctrl: state=3(connected), ip=169.254.1.104, last_hb_time=61241.68, hb_nr=90650
FG-5KB3E12700041, Slave, uptime=9102.92, priority=3, slot_id=1:6, in_sync=1
         elbc-base-ctrl: state=3(connected), ip=169.254.1.6, last_hb_time=61241.62, hb_nr=45452
FG-5KB3E12700088, Slave, uptime=61145.09, priority=102, slot_id=2:5, in_sync=1
         elbc-base-ctrl: state=3(connected), ip=169.254.1.105, last_hb_time=61241.60, hb_nr=90652
```

### **Management Routing**

- **IMPORTANT**: Although management access to the FortiGate will occur through PAT, outbound access for logging/Reporting and SNMP traps will require a default route to be configured in the elbc-mgmt VDOM.
- The default route must be set to the hidden virtual base-mgmt IP address **10.101.10.1.** This IP address floats and always follows the master switch.

```
c15s03 (elbc-mgmt) # config router static
config router static
edit 1
set device "base-mgmt"
set gateway 10.101.10.1
end
```

FortiGates contain two base channels that are used for Heart Beats as well as management. Base channel 1 connects to the FortiSwitch in slot-1 and channel 2 connects to slot-2. The channel associated with the active FortiSwitch must be up. Only one channel should be up per chassis at any given time.

c15s03 (elbc-mgmt) **# diagnose netlink redundant name base-mgmt** status: up npu: y oid: 37 ports: 2 MAC addr: 00:09:0f:ff:44:75 current slave: base1 slave: base1

link status: up link failure count: 1 permanent MAC addr: 00:09:0f:ff:44:75

slave: base2 link status: down link failure count: 1 permanent MAC addr: 00:09:0f:ff:44:7e

Chassis Loadbalance must match between all FortiGates in a Service Group. Channel below designates base channel.

c15s03 (global) # diagnose test application chlbd 1 my service group id=1 my chassis=1 active channel=1 ← Base1 best active channel=1 master chassis=yes Other chassis is master=no my slot=3 master slot=3 other chassis master slot=19 ← Slot-3 Other Chassis chassis master slot=3 active slot mask=00780078(1.3,1.4,1.5,1.6,2.3,2.4,2.5,2.6) chassis active slot mask=00000078(1.3,1.4,1.5,1.6) update\_timer is running last\_rx of update msg is 4 ago FortiGate firewalls contain multicore CPUs. The number of CPUs varies between models. When a single core is fully utilized, traffic handling by the entire firewall can be impacted.

The default configuration of a FortiGate is optimized to distribute UTM traffic handling between multiple cores. However, further optimization can be configured to use all CPU cores for other processes thereby reducing the chance that a single core is overloaded.

The command get system performance status will display the number of CPU cores on a FortiGate. A total of eight cores are shown below (0-7).

C15s03 (global) **# get system performance status** CPU states: 0% user 0% system 0% nice 100% idle CPU0 states: 0% user 0% system 0% nice 100% idle CPU1 states: 0% user 0% system 0% nice 100% idle CPU2 states: 0% user 0% system 0% nice 100% idle CPU3 states: 0% user 0% system 0% nice 100% idle CPU4 states: 0% user 0% system 0% nice 100% idle CPU5 states: 0% user 0% system 0% nice 100% idle CPU6 states: 0% user 0% system 0% nice 100% idle CPU7 states: 0% user 0% system 0% nice 100% idle

Set both the logging and SSL inspection process to 8 for a FortiGate 5101C.

config system global set miglogd-children 8 set ssl-worker-count 8 end

Set the session sync process to 8 for a FortiGate 5101C.

config system ha set session-sync-daemon-number 8 set override disable end

# FortiSwitch & FortiGate SNMP

In ELBC there are generally two types of devices that people want SNMP information from: FortiGate and FortiSwitch.

- Query the FortiSwitch
- Query the FortiGate

MIBs for both the FortiSwitch and FortiGate can be found at <u>http://support.fortinet.com</u>.

## **Enable SNMP**

There are three steps to enabling SNMP for both the FortiGate and FortiSwitch.

• Configure the FortiSwitch's public community.

```
c15s01 # config system snmp community
edit 1
config hosts
edit 1
end
set name "fortinet"
end
c15s02 # conf system snmp sysinfo
set status enable
```

end

• Configure the FortiSwitch's private internal SNMP community. This community is only used between the FortiSwitch and FortiGate. When a query is made to the switch's public community for a specific OID, it uses the private community to retrieve information from to the FortiGates.

```
config system global
set service-group-snmp-community "superfly"
end
```

• Configure the FortiGate's community. This community must match the FortiSwitch's private community.

```
c15s03 (global) # conf system snmp community
edit 1
config hosts
edit 1
set interface "base-mgmt"
end
set name "superfly"
end
c15s03 (global) # conf system snmp sysinfo
set status enable
end
```

## **Query the FortiSwitch**

There are two ways to SNMP query the FortiSwitch. This can be done either directly to the switch's management IP address on the mgmt interface or through the Service Group's **base-mgmt-external-ip** address using SNMP access port number for the FortiSwitch. Please refer to the FortiSwitch section **Managing Service Group Slots** when using the base-mgmt-external-ip.

• Querying the FortiSwitch via the **mgmt** interface is straightforward. Since there is only one master FortiSwitch in a cluster, only the master will respond. Querying other switches directly through the management IP address is not supported.

Example Query:

• Retrieving the Software Version for the Master FortiSwitch.

In this example, the master FortiSwitch is in slot-1. It will answer for any SNMP query to the mgmt IP address.

```
snmpwalk -v 2c -c fortinet 10.100.23.221 .1.3.6.1.4.1.12356.106.4.1.1.0
SNMPv2-SMI::enterprises.12356.106.4.1.1.0 = STRING: "FortiSwitch-5003B
v5.0,build0015,130827 (Patch 2)"
```

Querying the base-mgmt-external-ip address and specifying the SNMP access port numbers will allow access to individual switches.

snmpwalk -v 2c -c fortinet **10.100.23.222:16101** .1.3.6.1.4.1.12356.106.4.1.1.0 SNMPv2-SMI::enterprises.12356.106.4.1.1.0 = STRING: "FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)"

snmpwalk -v 2c -c fortinet **10.100.23.222:16102** .1.3.6.1.4.1.12356.106.4.1.1.0 SNMPv2-SMI::enterprises.12356.106.4.1.1.0 = STRING: "FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)"

snmpwalk -v 2c -c fortinet **10.100.23.222:16103** .1.3.6.1.4.1.12356.106.4.1.1.0 SNMPv2-SMI::enterprises.12356.106.4.1.1.0 = STRING: "FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)"

snmpwalk -v 2c -c fortinet **10.100.23.222:16104** .1.3.6.1.4.1.12356.106.4.1.1.0 SNMPv2-SMI::enterprises.12356.106.4.1.1.0 = STRING: "FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)"

### **Query the FortiGate**

There are three ways to retrieve SNMP information from the FortiGate firewalls.

• Method 1: Queries can be made to the FortiSwtich's management IP address. OIDs used for this method belong to the fsServiceGroupWorkerBlades section of the FortiSwitch MIB.

snmpwalk -v 2c -c fortinet **10.100.23.221** .1.3.6.1.4.1.12356.106.14.2.1.1.9 SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.1 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.2 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.3 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.4 = STRING: "v5.0.3,build0208,130603"

 Method 2: Queries can be made directly to the FortiGate firewalls using the service group's base-mgmt-external-ip address the plus SNMP access port for the FortiGate. Please refer to the FortiSwitch section Managing Service Group Slots. Only individual blades can be queried using this option.

snmpwalk -v 2c -c superfly **10.100.23.222:16103** .1.3.6.1.4.1.12356.101.4.1.1.0 SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v5.0.3,build0208,130603" snmpwalk -v 2c -c superfly **10.100.23.222:16104** .1.3.6.1.4.1.12356.101.4.1.1.0 SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v5.0.3,build0208,130603"  Method 3: Queries can be made directly to the FortiSwitch using the service group's base-mgmt-external-ip address plus the SNMP access port number for the FortiSwitch. Please refer to the FortiSwitch section Managing Service Group Slots. OIDs used in this method belong to the fsServiceGroupWorkerBlades section of the FortiSwitch MIB.

Note that the ports used are different between these two examples. Port 16101 connects to chassis 1 slot 1 and port 16121 connects to chassis 2 slot 1.

snmpwalk -v 2c -c fortinet **10.100.23.222:16101** .1.3.6.1.4.1.12356.106.14.2.1.1.9 SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.1 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.2 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.3 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.4 = STRING: "v5.0.3,build0208,130603"

snmpwalk -v 2c -c fortinet **10.100.23.222:16121** .1.3.6.1.4.1.12356.106.14.2.1.1.9 SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.1 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.2 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.3 = STRING: "v5.0.3,build0208,130603" SNMPv2-SMI::enterprises.12356.106.14.2.1.1.9.4 = STRING: "v5.0.3,build0208,130603"

#### FortiSwitch Service Group Worker Blades Commonly Used OIDs

Below are commonly used OIDs for all workers in a service group.

FortiGates Host Name snmpwalk -v 2c -c fortinet 10.100.23.222:16101 1.3.6.1.4.1.12356.106.14.2.1.1.11 FortiGates UpTime snmpwalk -v 2c -c fortinet 10.100.23.222:16101 1.3.6.1.4.1.12356.106.14.2.1.1.13 FortiGates Firmware snmpwalk -v 2c -c fortinet 10.100.23.222:16101 .1.3.6.1.4.1.12356.106.14.2.1.1.9 FortiGates Average CPU Usage snmpwalk -v 2c -c fortinet 10.100.23.222:16101 .1.3.6.1.4.1.12356.106.14.2.1.1.18 FortiGates Individual CPU Usage snmpwalk -v 2c -c fortinet 10.100.23.222:16101 .1.3.6.1.4.1.12356.106.14.2.5.1.3 FortiGates Session Rate snmpwalk -v 2c -c fortinet 10.100.23.222:16101 .1.3.6.1.4.1.12356.106.14.2.1.1.26 FortiGates Session Count snmpwalk -v 2c -c fortinet 10.100.23.222:16101 .1.3.6.1.4.1.12356.106.14.2.1.1.25 FortiGates Memory Usage snmpwalk -v 2c -c fortinet 10.100.23.222:16101 1.3.6.1.4.1.12356.106.14.2.1.1.19 FortiGates Serial Number snmpwalk -v 2c -c fortinet 10.100.23.222:16101 1.3.6.1.4.1.12356.106.14.2.1.1.12

A real-time SNMP reporting application is useful when working with ELBC or a large number of interfaces. SNMP statistics is helpful in determining traffic distribution and bottlenecks. The application used below is called **SNMP Test Utility** and is free for MAC OSX.

Traffic distribution is shown for the front ports of the master FS5003B. F1and F2 is receiving more traffic than F3-F7 as expected with an uneven number of ports. Overall the distribution of traffic us under maximum capacity and flowing nicely.

Figure 7-1-1

Status	Interface	Туре	Upload	Download	Upload Speed	Download Speed
	f1(fabric)	ethernetCs	11.69 GB	9.01 GB	319.7 MB/s	250.2 MB/s
	f2(fabric)	ethernetCs	11.68 GB	9.00 GB	318.9 MB/s	247.9 MB/s
•	f3(fabric)	ethernetCs	7.79 GB	9.02 GB	218.8 MB/s	249.7 MB/s
	f4(fabric)	ethernetCs	7.81 GB	9.00 GB	215.6 MB/s	247.9 MB/s
	f5(fabric)	ethernetCs	7.80 GB	8.77 GB	214.3 MB/s	241.3 MB/s
	f6(fabric)	ethernetCs	7.77 GB	8.77 GB	211.6 MB/s	243.9 MB/s
•	f7(fabric)	ethernetCs	7.77 GB	8.76 GB	213.6 MB/s	240.0 MB/s
•	f8(fabric)	ethernetCs	0 B	0 B	0 B/s	0 B/s
٠	slot-1/2(fa	ethernetCs	0 B	0 B	0 B/s	0 B/s
D C PI	an't find a def lease select or	ault network ne from the lis	interface to st above.	o monitor.		

Traffic distribution to the FortiGates (slots) is relatively equal.

Figure 7-1-2

Status	Interface	Type	Upload	Download	Upload Speed	Download Speed	L
٠	slot-1/2(fa	ethernetCs	0 B	0 B	0 B/s	0 B/s	
٠	slot-3(fabric)	ethernetCs	10.82 GB	10.80 GB	233.5 MB/s	227.1 MB/s	
٠	slot-4(fabric)	ethernetCs	10.80 GB	10.80 GB	225.8 MB/s	224.8 MB/s	
٠	slot-5(fabric)	ethernetCs	10.80 GB	10.82 GB	236.4 MB/s	225.9 MB/s	
	slot-6(fabric)	ethernetCs	10.83 GB	10.81 GB	237.4 MB/s	225.0 MB/s	
	slot-7(fabric)	ethernetCs	10.81 GB	10.79 GB	233.8 MB/s	220.4 MB/s	
	slot-8(fabric)	ethernetCs	10.81 GB	10.80 GB	235.1 MB/s	226.5 MB/s	
	slot-9(fabric)	ethernetCs	10.82 GB	10.84 GB	234.9 MB/s	228.4 MB/s	
	slot-10(fab	ethernetCs	10.79 GB	10.83 GB	232.9 MB/s	225.7 MB/s	
•	slot-11(fab	ethernetCs	0 B	0 B	0 B/s	0 B/s	
C PI	an't find a dei lease select o	fault network ne from the lis	interface to st above.	o monitor.		Com	

#### **Traps**

Traps are sent from the Master FortiSwitch in the active chassis. If an event causes an HA failover to occur, only the HA trap event that is sent from the new master FortiSwitch will be seen. Root cause failure traps cannot be sent out of a down or slave FortiSwitch.

For example, a FortiGate card failure causes the demotion of FortiSwitch c15s01 to slave. The failure would have normally sent an fsTrapHaMemberDown trap event. Since the master/slave change supersedes the local failure, only the trap fsTrapHaSwitch will sent by the new master FS indicating that a new FortiSwitch has become master.

Trap Scenarios

- FortiGate Card Failure Standalone FS (fsTrapHAMemberDown) High Availability (fsTrapHaSwitch)
- Missing Heartbeats High Availability (fsTrapHaSwitch)
- LAG Port Down Standalone FS (fsTrapMemberDown) High Availability (fsTrapHaSwitch)
- FS Management Port Failure Standalone FS (No Trap Sent) High Availability (No Trap Sent)
- FS B1/B2 Port Failure High Availability (fsTrapHaSwitch)
- FS Joins Cluster High Availability (fsTrapHaMemberUp)

# FortiManager

Management of an ELBCv3 cluster from the FortiManager is broken down into three parts.

- FortiGate
- FortiSwitch
- Chassis Shelf Manager

For additional FortiManager configuration information, please refer to <u>http://docs.fortinet.com</u>.

## FortiGate Management

In ELBCv3 there could be as many as 24 FortiGate firewalls to manage. The FortiManager is aware of all firewalls that make up a cluster. It simplifies the process by managing only the master FortiGate. The master FortiGate then syncs its configuration to all slave devices in all chassis.

Install FortiGate Firewalls

To add the FortiGate Firewalls, right click **All FortiGate** to access the pop out menu and follow the screen shots below.



















Each chassis contains four firewalls and the figure below shows that all four FortiGates have been added. **System Information** gives a good overview of which FortiGate master and each slot's health status.



00		FortiManager: FMG-VM64 HA(Group-ID:1)									
FortiManager: FMG-VM64 HA(G.	× 🔛 Plea	se login	× +			_					
<ul> <li>Transformed and the second seco</li></ul>	action=login					ĥ	- ⊂ C' (	🕙 🕆 jessica herrin facebook	Q 🛃 🏠 🖾 -		
E FortiManager VM	64				)			j.			
	Devic	e Manager	Policy & Objects	Fortiguard	Log Vi	ew D	nii Down	Event Management R	eports System Settings		
evice Manager	-li	_		San's	_	_	-	Search			
All FortiGate(2)	ame	me - YConfig Status YPolicy Package Status					Connectivity	IP Platform			
	so ELBC		L Pending				<ul> <li>FG-1</li> <li< td=""><td>5KB3E11700407 (Master) 5KB3E11700315 (Slave) 5KB3E11700378 (Slave) 5KB3E11700411 (Slave) 5KB3E11700636 (Slave) 5KB3E12700001 (Slave)</td><td>10.100.23.222 FortiGate-5001</td></li<></ul>	5KB3E11700407 (Master) 5KB3E11700315 (Slave) 5KB3E11700378 (Slave) 5KB3E11700411 (Slave) 5KB3E11700636 (Slave) 5KB3E12700001 (Slave)	10.100.23.222 FortiGate-5001		
	🍪 Menu 🔻							ELBC: Sy	stem > Dashboard [Custo		
	System Informatio	n			Connection Summary						
	Hostname	c15s03						IP	10.100.23.222		
	Serial Number	FG-5KB3E11700407						Interface	base-mgmt		
	Firmware Version	FortiGate 5.0.3 (0208) [Update]						Connecting User	admin		
	Hardware Status	8 CPU, 11975	5 MB RAM		Connectivity	O [Refresh]					
	HA Mode	ELBC Cluster						Connect to CLI via	OTELNET OSSH		
	Cluster Members	Chassis:Sl	ot # Serial Nun	nber R	ole	Status	Action	Configuration and I	Installation Status		
		1:3	FG-5KB3E1	1700407 M	aster	0		System Template	default [Change]		
		1:4	FG-5KB3E1	1700636 S	lave 4	0		Logging Device	None		
		1:5	FG-5KB3E1	1700411 S	lave 3	0		FortiGuard Update	None		
		1:6	FG-5KB3E1	2700041 S	lave 6	0		Device			
		2:3	FG-5KB3E1	1700378 S	lave 2	0		Database	View		
		2:4	FG-5KB3E1	2700001 S	lave 5	0		Total Revisions			
		2:5	FG-5KB3E1	2700088 S	lave 7	0		Even Status	Support		
		2:6	FG-5KB3E1	1700315 S	lave 1	0		Warning	None		
	VDOM	Enabled [Dis	able]					Installation Tracking	HOUR		
	Session Information	[View Sessi	on List]					Device Settings	Modified		
	System Time	Sat Oct 26 14	4:13:57 PDT 2013 [	Change]				Status	ribuincu		
	Description							Installation Preview	<u>é</u>		
		7 m	-								

After importing the FortiGates, there are no zones associated with any interface. In order to create firewall policies, the FortiManager must match a Zone in the database to an interface on a FortiGate. Although not used in this example, Zones allow multiple different interfaces on different devices to share the same firewall policy. For example, an FG200D's LAN port 1 and FG300C's LAN port 2 can be put into a zone named LAN. Firewall policies can then be associated with the zone but during installation the FortiManager makes appropriate changes to the unique interfaces of each device.

To create Zones navigate to the **Policy & Objects** section. Select the **Zone** section and click **Create New** then follow the figures below.

Figure 8-1-11									
000			FortiManager:	FMG-VM64 HA	(Group-ID:	1)			
FortiManager: FMG-VM64 HA(G	× 🛄 🛛	Please login	× +						
(172.30.71.92/index.htm?act	ion=login#					∰ ₹ C (	🙁 🛪 jessica herrin fac	ebook	۹
FortiManager VM6	4 —						\	5	
	De	vice Manager	Policy & Objects	FortiGuard	Log View	Drill Down	Event Management	Reports	System Settings 🛛 🧉
Policy Package	Policy								OSection View 💿 Global
Policy Package	Seq.# S	ource Interface	Destination Interface	Source Dest	ination Sche	edule Service	Authentication Ac	tion Profile	e Log NAT Comments
default									
				Land	Demai				
				Local	Domai	n Polici	es		
Objects	Create New Zo	ne							
Zone	Name	externa	f						
E Firewall Objects	Description	Write a	comment			0/4096			
Address	Interface Temp	late 🕞							
- Ca Service						Canaal			
Construction Schedule					N	Cancer			
Traffic Shaper									
User & Device									
Figure 8-1-12									
--	-----------------------------------	-----------------------------------	-------------------------	-------------------------------	-----------------------------------	------------------			
000		FortiManager	FMG-VM64 HA(Group-ID	0:1)					
FortiManager: FMG-VM64 HA(G	× Plea	se login × +							
172.30.71.92/index.htm?ac	tion=login#			☆ ▼ C' (8 ▼ jessica herrin	facebook Q				
E FortiManager VM6	4 Device	Manager Policy & Objects	FortiGuard Log View	Drill Down Event Manager	nent Reports System S	ettings 🔋 🕻			
Display Options Revisions Policy Package	Policy Seq.# Source	te Interface Destination Interfac	e Source Destination Sc	hedule Service Authentication	OSection Action Profile Log N.	View  Global Vie			
⊞default			Local Doma	in Policies					
Objects	Create New Zone								
Zone	Name	internal							
Firewall Objects Address	Description Interface Template	Write a comment		20/4096					
-Ca Service Ca Schedule			OK	Cancel					
Traffic Shaper  Virtual IP  Gecurity Profiles  User & Device									
×						4			

000			FortiManager:	FMG-VM64 H	HA(Group-ID:	1)						10
FortiManager: FMG-VM64 HA(G 3	< (1)	Please login	×)+)						_		_	
( 172.30.71.92/index.htm?actio	n=login#					∰ ₹ C	8 × jessica herr	in facebo	ok	۹ (	<b>b</b>	
E FortiManager VM64	_	Device Manager	Policy & Objects	FortiGuard	Log View	Drill Down	Event Manage	ement	Reports	Syste	m Setti	ngs ? 🕻
Display Options Revisions												
Policy Package	Policy				_					OSec	tion Viev	v 💿 Global Vie
Policy Package	Seq.#	Source Interface	Destination Interface	Source De	estination Sche	edule Service	Authentication	Action	Profile	Log	NAT	Comments
				Loca	l Domai	n Polici	es					
Objects	Creat	e New	elete 🔲 Colu	mn Settings		_	_	_	Sea	rch		
Zone	Name	- T)	/pe De	scription								
Firewall Objects	internal	Zo	one									
	a internal	20	one									
Schedule  Traffic Shaper  Virtual IP  G Security Profiles  D User & Device												
¥												

Navigate back to the **Device Manager** section to associate Zones with Interfaces.



FortiManager: FMG-VM64 HA(G	× (	Please log	in	×					
(172.30.71.92/index.htm?ac	tion=login#					☆▽	C issica herrin face	book Q	
E FortiManager VM6	4	Device Mar	nager P	olicy & Objects	FortiGuard L	.og View Drill	Down Event Management	Reports Sy	/stem Settings 🛛 🖓 🛐
Device Manager					1		Search		
All FortiGate(2)	D	evice Name		Config Status	Policy Pa	ckage Status	Tonnectivity	IP	Platform
all Log Arrays(0) ₪	B∰ ELBC			Pending			Ŷ           FG-5KB3E11700407 (Masta P FG-5KB3E11700315 (Slave P FG-5KB3E11700378 (Slave P FG-5KB3E11700411 (Slave P FG-5KB3E11700636 (Slave P FG-5KB3E12700001 (Slave P FG-5KB3E12700001 (Slave	10.100.23.2 ar) ) ) ) ) ) ) )	222 FortiGate-5001B
	🎒 Menu 🔻						ELBC: Sys	tem 👂 Zone &	Interface [Customize
	Hide U	nmapped Zo	nes	O Create New	Colun	nn Settings		Search	
	Virtual Domain	Zone	Interface	Member	Туре	Addressing Mode	IP/Netmask	Access	
	root	external	9						
			external (	Unmapped)	Physical	Manual	0.0.0/0		
			internal (C	(llemonad)	Physical	Manual	0.0.0/0		
			mean.root	(Unmanned)	T WIFI 331D	Manual	0.0.0.0/0		
			npu0-viini	(Unmapped)	Physical	Manual	0.0.0/0		
			nput-wint	(Unmapped)	Physical	Manual	0.0.0.0/0		
			npu1-wint	(1 (Unmanned)	Physical     Physical	Manual	0.0.0.0/0		
			sel root (I	(onniciped)	Tuppel	Manual	0.0.0.0/0		
	elbc-mont	( ovtornal	Jani oor (o	mappeay	· · · · · · · · · · · · · · · · · · ·	Hunder	0.0.0,0		
	cibe nighte	internal							
			hase-mon	t (Unmapped)	** Redundant	Manual	10 101 10 3/255 255 255 0	HTTP. HTTPS	SSH. PING. SNMP. TELNE
			base1 (Un	mapped)	Physical	Manual	0.0.0.0/0		,,,,
			base2 (Un	mapped)	Physical	Manual	0.0.0.0/0		
	-		elbc-base-	ctrl (Unmapped)		Manual	10.101.11.3/255.255.255.0		

000			1	FortiManager: I	MG-VM64	HA(Gr	oup-ID:1	1)						Mar N
FortiManager: FMG-VM64 HA(G	×	Please log	in	× +						_				
A 3 172.30.71.92/index.htm?act	ion=login#							$\sum_{i=1}^{N_{a}} \forall \ \textbf{C}$	🙁 🕈 jessica her	rin facebo	ok	۹ 🜗		3-) 🖸
E FortiManager VM64	1	Device Mar	nager Po	licy & Objects	FortiGua	rd Lo	og View	Drill Down	Event Manag	ement	Reports	Syster	n Settings	?
Device Manager										Search				
All FortiGate(2)		Device Name		Config Stat	us 🖗 P	olicy Pac	ckage Stal	tus	Connectivity	s	IP	6	Platfor	n
All Log Arrays(0)	EE ELBC			🔮 Pending					G-5KB3E1170040 G-5KB3E1170031 G-5KB3E1170037	7 (Master) 5 (Slave) 3 (Slave)	10.100	23.222	FortiGate	5001B
				E	dit Zone N	1ap				(Slave) Slave)				
		Zone:external								Slave)				
	Mer	Available Interfa	ce		-	Interfac	ce Membe	r		Systen	n ≱ Zon	e & Inte	rface [C	ustomize]
	Гн	internal mesh.root				extern	nal				Sea	arch		
	Virtual D	npu0-vlink0									Access			
		npus-viinki npui-viinki ssi.root Block intra-zone traffic			G									
								Арр	ly Cancel					
	elbc-mgmt	🐨 external												
		😨 internal												
			base-mgm	t (Unmapped)	** Red	undant	Manual	10.	101.10.3/255.255	.255.0	нттр, нт	TTPS, SSH	I, PING, SN	1P, TELNET,
			base1 (Uni	mapped)	🔄 Phy	sical	Manual	0.0	.0.0/0					
			base2 (Uni	mapped)	Phy	sical	Manual	0.0	.0.0/0					
Provisioning Templates			elbc-base-	ctrl (Unmapped)	S VLA	N	Manual	10.	101.11.3/255.255	.255.0				
×														

FortiManager: FMG-VM64 HA	(G × 💷	Please log	in	× +						
( 3 172.30.71.92/index.htm	n?action=login#					, H ≞	C (8	<ul> <li>jessica herrin facebo</li> </ul>	iok Q 🛛	
EF FortiManager VI	M64	Device Mar	ager Polic	cy & Objects	FortiGuard	.og View Drill	Down	Event Management	Reports Syste	m Settings 🔋
Device Manager								Search		
All FortiGate(2)	De	vice Name		Config Status	Policy P	ackage Status	5	Connectivity	IP	Platform
🖶 All Log Arrays(0)	<u>₽</u> 3 elbC			Pending			<ul> <li> <b>↑</b>             FG-5i      <li>             FG-5i         </li> </li></ul>	(B3E11700407 (Master) (B3E11700315 (Slave) (B3E11700411 (Slave) (B3E11700411 (Slave) (B3E11700636 (Slave) (B3E1270001 (Slave) (B3E12700041 (Slave)	10.100.23.222	FortiGate-5001B
	🎒 Menu 🔻							ELBC: Syster	m 👂 Zone & Inte	erface [Customize
	□ Hide Un	mapped Zo	nes 🤇	Create New	Colur	nn Settings			Search	
	Virtual Domain	Zone	Interface Me	mber	Туре	Addressing Mode	ing Mode IP/Netmask		Access	
	root	😨 external	external		Physical	Manual	0.0.0.0	/0		
		😨 internal	-							
			internal (Unr	mapped)	E Physical	Manual	0.0.0.0	/0		
			mesh.root (L	Inmapped)	🙌 WiFi SSID	Manual	0.0.0.0	/0		
			npu0-vlink0	(Unmapped)	🗵 Physical	Manual	0.0.0.0	/0		
			npu0-vlink1	(Unmapped)	토 Physical	Manual	0.0.0.0	/0		
			npu1-vlink0	(Unmapped)	Physical	Manual	0.0.0.0	/0		
			npu1-vlink1	(Unmapped)	🗷 Physical	Manual	0.0.0.0	/0		
			ssl.root (Unn	napped)	Tunnel	Manual	0.0.0.0	/0		
	elbc-mgmt	🐨 external								
		🐨 internal								
			base-mgmt (	(Unmapped)	* Redundant	Manual	10.101	.10.3/255.255.255.0	HTTP, HTTPS, SS	H, PING, SNMP, TELNE
			base1 (Unma	apped)	Physical	Manual	0.0.0.0	/0		
			base2 (Unma	apped)	Physical	Manual	0.0.0.0	/0		
			elbc-base-ctr	rl (Unmapped)	S VLAN	Manual	10.101	11.3/255.255.255.0		
Provisioning Templates			elbc-ctrl/1 (U	Jnmapped)	Physical	Manual	0.0.0.0	/0		



				NW NW			Search		1	
All FortiGate(2)	De	vice Name	+	Config Status	Policy Pa	ckage Status	Connectivity	IP	Platform	
🖶 All Log Arrays(0)	₽8 ELBC			Pending			<ul> <li> <b>P</b> FG-5KB3E11700407 (Master)             <b>P</b> FG-5KB3E11700315 (Slave)          </li> <li> <b>P</b> FG-5KB3E11700417 (Slave)         </li> <li> <b>P</b> FG-5KB3E11700411 (Slave)         </li> <li> <b>P</b> FG-5KB3E11700636 (Slave)         </li> <li> <b>P</b> FG-5KB3E12700001 (Slave)         </li> </ul>	10.100.23.222	FortiGate-5001B	
	😂 Menu 🔻						ELBC: System	n 👂 Zone & Inte	rface [Customize]	
	Hide Un	mapped Zo	ines	Create New *	Colun	nn Settings		Search		
	Virtual Domain	Zone	Interface M	ember	Туре	Addressing Mode	IP/Netmask	Access		
	root	😨 external	external		Physical	Manual	0.0.0/0			
		😨 internal	internal		Physical	Manual	0.0.0.0/0			
			mesh.root (	Unmapped)	(1) WiFi SSID	Manual	0.0.0/0			
			npu0-vlink0	(Unmapped)	Physical	Manual	0.0.0/0			
			npu0-vlink1	(Unmapped)	E Physical	Manual	0.0.0/0			
			npu1-vlink0	(Unmapped)	Physical	Manual	0.0.0/0			
			npu1-vlink1	(Unmapped)	Physical	Manual	0.0.0.0/0			
			ssl.root (Un	imapped)	Tunnel	Manual	0.0.0/0			
	elbc-mgmt	😨 external								
		😨 internal								
			base-mgmt	(Unmapped)	** Redundant	Manual	10.101.10.3/255.255.255.0	HTTP, HTTPS, SSI	H, PING, SNMP, TELNET	
			base1 (Unn	napped)	🔄 Physical	Manual	0.0.0/0			
			base2 (Unn	napped)	Physical	Manual	0.0.0/0			
			elbc-base-c	tri (Unmapped)	🗐 VLAN	Manual	10.101.11.3/255.255.255.0			
			elbc-ctrl/1	(Unmapped)	🔄 Physical	Manual	0.0.0/0			
Provisioning Templates			elbc-ctrl/2	(Unmapped)	Physical	Manual	0.0.0.0/0			

Once complete click on the interface Member name to add IP addresses.

FortiManager: FMG-VM64 HA(	G × 🚺	Please log	in	× (+ )						
( 3 172.30.71.92/index.htm	n?action=login#					슈포	C 🔋 🙁 🕈 jessica herrin facel	ook		3-) 🖸
E FortiManager VI	<b>//64</b>	Device Mar	iager F	Policy & Objects F	ortiGuard I	.og View Drill I	Down Event Management	Reports	System Settings	?
Device Manager							Search			
- 📾 All FortiGate(2)	De	evice Name		- TConfig Status	Policy Pa	ckage Status	Connectivity	IP	Platform	n
All Log Arrays(0)	<u>R</u> ₫ ELBC			C Pending			<ul> <li></li></ul>	10.100.	.23.222 FortiGate-	5001B
	🍪 Menu <del>-</del>						ELBC: Syst	em 🕨 Zon	e & Interface [Co	ustomize
	Hide Un	mapped Zo	nes	🔾 Create New 🔻	Colur	nn Settings		Sea	arch	
	Virtual Domain	Zone	Interface	Member	Туре	Addressing Mode	IP/Netmask	Access		
	root	😨 external	al external		👿 Physical	Manual	1.0.0.1/255.255.255.0	PING		
		😨 internal	internal	2	🗵 Physical	Manual	2.0.0.1/255.255.255.0	PING		
			mesh.roo	t (Unmapped)	(1) WiFi SSID	Manual	0.0.0.0/0			
			npu0-vlin	k0 (Unmapped)	Physical	Manual	0.0.0.0/0			
			npu0-vlin	k1 (Unmapped)	E Physical	Manual	0.0.0/0			
			npu1-vlin	k0 (Unmapped)	Physical	Manual	0.0.0/0			
			npu1-vlin	k1 (Unmapped)	Physical	Manual	0.0.0/0			
			ssl.root (	Unmapped)	Tunnel	Manual	0.0.0.0/0			
	elbc-mgmt	😨 external								
		😨 internal								
			base-mgr	mt (Unmapped)	*** Redundant	Manual	10.101.10.3/255.255.255.0	нттр, нт	TTPS, SSH, PING, SNM	1P, TELNI
			base1 (U	nmapped)	E Physical	Manual	0.0.0/0			
			base2 (U	nmapped)	Physical	Manual	0.0.0/0			
			elbc-base	-ctrl (Unmapped)	🧐 VLAN	Manual	10.101.11.3/255.255.255.0			
			elbc-ctrl/	1 (Unmapped)	Physical	Manual	0.0.0/0			
Provisioning Templates			elbc-ctrl/	2 (Unmapped)	Physical	Manual	0.0.0/0			

Static routes can be added by clicking on **Menu** and selecting **Router**.

By default there are no firewall policy packages associated with a newly installed ELBC cluster. The default policy package is not assigned to any device or VDOM and should be left alone in favor of a more specific Policy Package Name.

Create a new Policy Package and deploy firewall policies.

Fiaure 8-1-21										
000				FortiManager: F	MG-VM64 HA(Grou	up-ID:1)				Mar No.
FortiManager: FMG	-VM64 HA(G	. × 609	Please login	× (+ )						
172.30.71.92	/index.htm?a	ction=login					😫 🛪 jessica herrin fa	acebook		-
E FortiMana	ager VM6	64	Device Manager	Policy & Objects	FortiGuard Log	View Drill Down	Event Manageme	nt Reports	System Settings	? 🐺
Display Options	Revisions									
Policy Package	_	Policy							OSection View 💿	Global View
🖹 📾 Policy Package		Seq.#	Source Interface	Destination Interface	Source Destination	Schedule Service	Authentication	Action Profile	Log NAT Cor	mments
∟ <u>≣</u> default	Polic ····································	y Package Install Re-install Create New Installation Targ Delete Export Policy Check y Folder Create New Rename	get		Local Do	main Polic	ies			
Objects	1	Delete	D	elete Colur	nn Settings			Sea	-ch	1.00
Zone	2	Name		- Туре		Descriptio	n			
a ﷺ Firewall Objects a G Security Profiles a G User & Device		No records fo	sund.							
172.30.71.92/index.htm?	action=login#									

<b>9</b> 00				FortiManager: FMG-VM64 HA(Group-ID	:1)							12 <sup>71</sup>
FortiManager: FMG-VM64 HA(G 3		Pleas	se login	×    +	0 - C	N T ins	sica herri	n faceboo	× 0			
EII FortiManager VM64	in-iogin	Device	Manager	Policy & Objects FortiGuard Log View	Drill Down	Even	it Managei	ment	Reports	System	Settings	?
Display Options Revisions Policy Package	Policy	_				_	_	_		Sectio	n View 🤆	Global View
Cobjects Co	Seq. # Create Name No records fou	Sc Ne	Name E	LEC olicy Package Target Group All_FortiCarrier Device Device Cont elbe-mgmt	Apply Can	cei	ntication	Action	Searc	Log J	NAT C	mments
×	1								_			

Figure 8-1-23					
FortiManager: EMG-VM64 HA/G	2 475 Please login	FortiManager: FMG-V	M64 HA(Group-ID:1)		μ <sup>2</sup>
(172.30.71.92/index.htm?actio	on=login		<u> </u>	8 r jessica herrin facebook	
The FortiManager VM64					
=== FOI timaliager vino4	Device Manage	r Policy & Objects Forti	iGuard Log View Drill Down	Event Management Rep	orts System Settings 🔋 🖺
Display Options - Parisions					
Policy Package	Policy				OSection View 💽 Global View
Policy Package	Seq.# Source Interfac	Destination Interface Source	ce Destination Schedule Servic	e Authentication Action I	Profile Log NAT Comments
default		100			
		L	ocal Domain Polic	ies	
					1
Objects	Create New	Delete Column Set	ttings		Search
Firewall Objects	No records found.	- 1996	beachpic		
🗉 🌠 Security Profiles					
E 🛃 User & Device					
×					•
Figure 8-1-24					
FortiManager: EMC=VM64 HA/G	Y Please login	FortiManager: FMG-V	M64 HA(Group-ID:1)		2
172.30.71.92/index.htm?actic			्र⊤ a)	R iessica herrin facebook	
	-login		H · · ·	Jessica nenni nacebook	
FortiManager VM64	Device Manage	r Policy & Objects Forti	Guard Log View Drill Down	Event Management Rep	orts System Settings 🔋 👺
<b>.</b>		_			
Display Options Revisions	1				0
Policy Package	Policy See # Source Interfai	Destination Interface Sour	ce Destination Schedule Servic	e Authentication Action	Profile Log NAT Comments
-ELBC					rione big fun connents
default	Create New	Policy	ocal Domain Bolic	ioc	
		Identity Policy	ocal Domain Polic	les	
					~
Objects	O Create New	Delete 🔲 Column Set	ttings		Search
Zone	Name	Туре	Descriptio	n	
Firewall Objects      Security Profiles	No records found.				
E Second Promes					
173 20 71 02 () 1		1-2-1			
www.ise.regi-bin/module/snaredobjm	anager/policy_new/539/PolicyTabl	e:br30ia=223#			

Add firewall policies to the ELBC Policy Package.

FortiManager: FMG-VM64 HA(G.	X Elease logic	FortiManager	:: FMG-VM64 HA(G	roup-ID:1)		ť.
172 30 71 92/index htm?activ	on=login#				a 🔞 🔹 jessica herrin fa	rehook Q L A D I
	on togina			Ed.		
FortiManager VM64	Device Manag	ger Policy & Objects	s FortiGuard L	og View Drill D	own Event Managemei	nt Reports System Settings <table-cell> 😱</table-cell>
Display Options Revisions	1					
Policy Package	Policy					Section View  Global View
ELBC	Seq. # Source Inter	race Destination Internac	ce source Destina	tion schedule se	arvice Authentication A	Letton Prome Log NAT Comments
default	Create New	Policy				
	8	Identity Policy	Local D	omain Po	licies	
		_				
Objects	Create New	Delete Col	umn Settings	Interface	Details	Search
Firewall Objects	SSLVPN_TUNNEL_ADDR1	8	Address	any	IP Range:10.212.134.2	00-10.212.134.210
🛃 Address	🖪 all		Address	any	IP/Mask:0.0.0.0/0.0.0.0	I
Service	6 SSLVPN_TUNNEL_IPv6_A	DDR1	IPv6 Address		fdff:ffff::1/120	
Schedule     Traffic Shaper	is all		IPv6 Address		::/0	
Cirtual IP						
E G Security Profiles						
Web Filter Profile						
Application Sensor						
IPS Sensor						
172 30 71 92/cgi-bin/module/charedobim	anager/policy_new/539/PolicyTa	able?nk.co.id=539#				
×						4.
Figure 8-1-26						
000		FortiManager	: FMG-VM64 HA(G	roup-ID:1)		e <sup>r</sup>
FortiManager: FMG-VM64 HA(G	× Please login	FortiManager n × +	:: FMG-VM64 HA(G	roup-ID:1)		2
FortiManager: FMG-VM64 HA(G      T72.30.71.92/index.htm?action	× Please login#	FortiManager n × +	:: FMGVM64 HA(G	roup-ID:1) $\langle \stackrel{\wedge}{_{ - }} = 0$	C) 🔞 yiessica herrin fa	 cebook Q) ♣ ♠  · []
Control C	× (;;) Please login on=login#	FortiManager n × +	:: FMG-VM64 HA(G	roup-ID:1) 후 (	। 😰 🕈 jessica herrin fa	دوbook ۹ ای ا
FortiManager: FMG-VM64 HA(G     G 9 172.30.71.92/index.htm?actik     FortiManager VM64	× (;;) Please login on=login# Device Manaq	FortiManager n × + ger Policy & Objects	:: FMG-VM64 HA(G s FortiGuard L	roup-ID:1) 슈 호 ( og View Drill D	ී 🛞 ་ jessica herrin fa own Event Managemei	cebook Q 🛃 🍙 💽 🔹 🖬
FortiManager: FMG-VM64 HA(G     T72:30.71.92/index.htm?actil     FortiManager VM64	× <b>(t)</b> Please login on=login# Device Mana	FortiManager n × + ger Policy & Objects Cr	:: FMG-VM64 HA(G s FortiGuard L reate New Policy	roup-ID:1) 슈 호 ( og View Drill D	연 🔞 🛪 jessica herrin fa own 👌 Event Managemen	cebook Q 🛃 🍙 💽 - 🖬
<ul> <li>FortiManager: FMG-VM64 HA(G</li> <li>T72.30.71.92/index htm?actil</li> <li>FortiManager VM64</li> <li>Display Options Revisions</li> </ul>	× ( <b>5.)</b> Please login on=login# Device Manag	FortiManager n × + ger Policy & Objects Cr	: FMG-VM64 HA(G S FortiGuard L reate New Policy	roup-ID:1) 나너 또 og View Drill D	연 😢 🛪 jessica herrin fa own 👌 Event Managemer	cebook Q 🛃 🍙 💽 - 🖬
Control Contro Control Control Control Control Control Control Control Control Co	× ( <b>5:)</b> Please login on=login# Device Manag	FortiManager n × + per Policy & Objects Cr	: FMG-VM64 HA(G S FortiGuard L reate New Policy	roup-ID:1) 슈너 호 ( og View ) Drill D	연 😢 🛪 jessica herrin fa own 👌 Event Managemer	cebook Q 💽 🏫 💽 🔹 🖬 nt Reports System Settings 🖓 😨
Continuanager: FMG-VM64 HA(G      TotiManager: FMG-VM64 HA(G      TotiManager: FMG-VM64      TotiManager: VM64      Diaplav Octions: Revisions      Policy Package      Policy	× (::: Please login on=login# Device Manag Policy Type	FortiManager n × + Policy & Objects Cr OFirewall VPN	s FortiGuard L	roup-ID:1) 슈국 코 ( og View Drill D	ී 😢 ་ jessica herrin fa own Event Managemei	cebook Q I I I I I I I I I I I I I I I I I I
Continuanager: FMG-VM64 HA(G      TotiManager: FMG-VM64 HA(G      TotiManager: FMG-VM64      TotiManager: VM64      Display Options: Revisions      Policy Package      Policy Package      Genuit	× (*** Please login on=login# Device Manag Policy Type Policy Subtype	FortiManager n × + Policy & Objects Cr • Firewall VPN • Address User Ic	s FortiGuard L FortiGuard L reate New Policy dentity ODevice Id	roup-ID:1)	경 🔞 ་ jessica herrin fa own 👌 Event Managemer	cebook Q 💽 👚 💽 - 💽 nt Reports System Settings 🖓 💽 Section View Oslobal View Profile Log NAT Comments
FortiManager: FMC-VM64 HA(G      FortiManager: FMC-VM64 HA(G      T2:30.71.92/index.htm?actif      FortiManager VM64      FortiManager VM64      FortiManager VM64      FortiManager	× E: Please login on=login# Device Manag Policy Type Policy Subtype Incoming Interface	FortiManager n × + Policy & Objects Cr OFirewall VPN OAddress User Ic Minternal	s FortiGuard L FortiGuard L reate New Policy dentity ODevice Id	roup-ID:1)	경 🔞 👻 jessica herrin fa own Event Managemer	cebook Q I Reports System Settings 2 I X Section View Global View Profile Log NAT Comments 4
FortiManager: FMC-VM64 HA(G      FortiManager: FMC-VM64 HA(G      T2:30.71.92/index.htm?actii      FortiManager VM64      FortiManager VM64      FortiManager VM64      FortiManager      Folicy Package      Folicy Package      ELBC      default	× (5.) Please login on=login# Device Manac Policy Type Policy Subtype Incoming Interface Source Address	FortiManager n × + Policy & Objects Cr • Firewall VPN • Address User Ic § Internal * all	s FortiGuard L FortiGuard L reate New Policy dentity ODevice Id	roup-ID:1)	경 🔞 * jessica herrin fa own Event Managemer	cebook Q R C - C nt Reports System Settings 2 C X Section View Global View Profile Log NAT Comments 2
FortiManager: FMC-VM64 HA(G      FortiManager: FMC-VM64 HA(G      T2:30.71.92/index.htm?activ      FortiManager VM64      Fort	× E Please login on=login# Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface	FortiManager n × + ger Policy & Objects Cr • Firewall VPN • Address User Ic % Internal * all % external	s Fort/Guard L Fort/Guard L reate New Policy dentity Opevice Id	roup-ID:1)	경 🔞 ་ jessica herrin fa own Event Managemen	cebook Q R T Comments
FortiManager: FMC-VM64 HA(G      FortiManager: FMC-VM64 HA(G      T2:30.71.92/index.htm?activ      FortiManager VM64      FortiManager VM64      FortiManager VM64      FortiManager VM64      FortiAnage      Fort	<ul> <li>Please login</li> <li>Device Manage</li> <li>Policy Type</li> <li>Policy Subtype</li> <li>Incoming Interface</li> <li>Source Address</li> <li>Outgoing Interface</li> <li>Destination Address</li> </ul>	FortiManager n × + ger Policy & Objects Co Officewall VPN OAddress User Ic Sinternal all Signet external Signet Policy & Objects Pricewall VPN Other Signet Sig	s FortiGuard L FortiGuard L reate New Policy dentity Opevice Id	entity	경 🔞 ་ jessica herrin fa own Event Managemer	cebook Q R T Comments
FortiManager: FMC-VM64 HA(G      FortiManager: FMC-VM64 HA(G      T2.30.71.92/index.htm?activ      FortiManager VM64      Display Dotions Revisions      Policy Package      Policy Package      ELBC     default	<ul> <li>Please login</li> <li>Device Manage</li> <li>Policy Type</li> <li>Policy Subtype</li> <li>Incoming Interface</li> <li>Source Address</li> <li>Outgoing Interface</li> <li>Destination Address</li> </ul>	FortiManager n × + ger Policy & Objects Co Officewall VPN Oddress User Ic Market Solution Market Solution Co Officewall VPN Oddress User Ic Market Solution Co Officewall VPN Co Officewall VPN Oddress VPN Co Officewall VPN Co Offic	FMG-VM64 HA(G	entity	경 🔞 🛛 jessica herrin fa own Event Managemer	cebook Q R T Comments
FortiManager: FMC-VM64 HA(G     T2.30.71.92/index.htm?activ     FortiManager VM64     Display Octions Revisions     Policy Package     Policy Package     ELBC     default	<ul> <li>Please login</li> <li>Device Manage</li> <li>Policy Type</li> <li>Policy Subtype</li> <li>Incoming Interface</li> <li>Source Address</li> <li>Outgoing Interface</li> <li>Destination Address</li> <li>Schedule</li> </ul>	FortiManager n × + ger Policy & Objects Co OFirewall VPN OAdress User IC Minternal all External all all all all all all all	FMG-VM64 HA(G	entity	경 🔞 💌 jessica herrin fa own Event Managemet	cebook Q R T Comments
FortiManager: FMC-VM64 HA(G     T2.30.71.92/index.htm?activ     FortiManager VM64     FortiManager VM6	<ul> <li>Please login</li> <li>Device Manage</li> <li>Policy Type</li> <li>Policy Subtype</li> <li>Incoming Interface</li> <li>Source Address</li> <li>Outgoing Interface</li> <li>Destination Address</li> <li>Schedule</li> <li>Service</li> </ul>	FortiManager n × + Ger Policy & Objects Co Original VPN Original VPN Original VPN Address User Ic Sector all sector a	s FortIGuard L reate New Policy dentity ODevice Id	entity	ී 💽 🛛 jessica herrin fa own Event Managemei	cebook Q R T Comments
Control Contro Control Control Control Control Control Control Control Control Co	× Clear Please login on=login# Device Manage Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface Destination Address Schedule Service Action	FortiManager n × + Policy & Objects Cr • Firewall VPN • Address User Ic is internal * all * alcept	s FortiGuard L reate New Policy dentity Opevice Id	entity	ී 😢 ་ jessica herrin fa own Event Managemei	cebook Q Profile Log NAT Comments
FortiManager FMG-VM64 HA(G     T72:30:71:92/index.htm?actid     T72:30:71:92/index.htm?actid     FortiManager VM64     Forti	× Clear Please login on=login# Device Manage Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface Destination Address Schedule Service Action	FortiManager n × + Policy & Objects Cr • Firewall VPN • Address User Ic Minternal * all * all * all * all * always © ACCEPT	s FortiGuard L s FortiGuard L dentity ODevice Id	entity	3 😢 – jessica herrin fa	cebook Q Profile Log NAT Comments Search
FortiManager FMG-VM64 HA(G      T72:30:71:92/index.htm?actil      FortiManager VM64      FortiManager VM64      FortiManager VM64      FortiManager VM64      FortiPackage      Folicy Package      Fo	× Clear Please login on=login# Device Manage Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface Destination Address Schedule Service Action	FortiManager n × + Policy & Objects Cr Offrewall VPN OAddress User Ic Minternal * all # all # always Cr Address User Ic Address Ic Address User Ic Address Ic A	s FortiGuard L s FortiGuard L reate New Policy dentity ODevice Id	entity	3 😢 – jessica herrin fa	cebook Q P P P Content Comments
Cobjects Cobject Co	Yease login     Device Manage     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT	FortiManager n × + Policy & Objects Cr Offirewall VPN O Address User Ic Minternal * all * all * always ALL O ACCEPT	s Fort/Guard L s Fort/Guard L reate New Policy dentity ODevice Id	entity	경 (원 ~ jessica herrin fa own ) Event Managemer	cebook Q P P C
Cobjects Co	Yease login     Device Manage     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options	FortiManager n × + ger Policy & Objects Cr • Firewall VPN • Address User Ic Signternal * all * accept	s Fort/Guard L s Fort/Guard L reate New Policy dentity ODevice Id	roup-ID:1)	김 (원 - jessica herrin fa own ) Event Managemer	cebook Q P P P C
Cobjects Co		FortiManager n × + ger Policy & Objects Co • Firewall VPN • Address User Ic is internal • all • all • all • always is ALL • ACCEPT	s Fort/Guard L s Fort/Guard L reate New Policy dentity ODevice Id	roup-ID:1)	김 (원 - jessica herrin fa own) Event Managemer	cebook Q P Profile Log NAT Comments
Constant Series     C	Yease login     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     No Log     O Security Ever     Log All Sessions	FortiManager n × + ger Policy & Objects Co Officewall VPN OAddress User Ic Signternal 2 all 2 all 2 all 2 ALL 2 ACCEPT mts	s FortiGuard L reate New Policy dentity ODevice Id	roup-ID:1)	2 😢 🕶 jessica herrin fa	cebook Q R C C C C C C C C C C C C C C C C C C
Cobjects Co	Pelase login     Device Manage     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     O Security Eve     Log All Sessions     Enable Web Cache	FortiManager n × + ger Policy & Objects Co Officewall OVPN OAddress OUser Ic Ministremal all all ALL ACCEPT ALL ACCEPT	s FortiGuard L reate New Policy dentity ODevice Id	roup-ID:1)	2 😢 🕶 jessica herrin fa	cebook Q R C - C
FortiManager: FMC-VM64 HA(G      FortiManager: FMC-VM64 HA(G      T2.30.71.92/index.htm?activ      FortiManager: VM64      Bisplay Options Revisions     Policy Package      Policy Package      Policy Package      ELBC      default      Displate Options     ELBC      Gostende      Gostende      Traffic Shaper      Virtual IP      Security Profiles      Motivinus Profile      Security Profiles      Motivinus Profile      Security Profile       Security Profile      Security Profile       Securi	Yease login     Device Manage     Policy Type     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     Olog Sourity Evec     Log All Sessions     Enable Web Cache     Enable Web Cache	FortiManager n × + ger Policy & Objects Co O Firewall O VPN O Address O User Ic Market S O User Ic S external all all ALL ACCEPT nts	s FortiGuard L reate New Policy dentity ODevice Id	roup-ID:1)	3 🔞 🖲 jessica herrin fa	cebook Q R T Comments
Sorreal Objects      Sorr	Yease login     Device Manage     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     Ola Sessions     Enable Web Cache     Enable WAN Optime	FortiManager n × + ger Policy & Objects Co O Firewall VPN O Address User Ic Minternal all E all all Address Address Market Address Ad	s FortIGuard L reate New Policy dentity ODevice Id	entity	C Residence (Service)	cebook
Service     S	Yease login     Device Manage     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     Olog Security Ever     Olog All Sessions     Enable Web Cache     Enable WAN Optim	FortiManager n × + ger Policy & Objects Co © Firewall VPN © Address User Ic % Internal * all * alcept	s Fort/Guard L reate New Policy dentity Oevice Id	entity	C R Cancel	cebook
SortiManager: FMG-VM64 HA(G      T72:30.71.92/index.htm?actid      T72:30.71.92/index.htm?actid      FortiManager VM64      Sortice      Policy Package      P	Yease login     Device Manage     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     Cog Security Ever     Log All Sessions     Enable Web Cache     Enable Web Cache	FortiManager n × + ger Policy & Objects Co Prirewall VPN Address User Ic Minternal all Address User Ic Address User Ic Address Australia Address Address Address Australia Address Address Ad	S FortiGuard L s FortiGuard L dentity ODevice Id	roup-ID:1)	Cance	cebook
<ul> <li>FortiManager: FMG-VM64 HA(G</li> <li>FortiManager: FMG-VM64 HA(G</li> <li>T2:30.71.92/index.htm?actif</li> <li>FortiManager VM64</li> <li>FortiManager</li> <li>Policy Package</li> <li< td=""><td>Policy Type     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     Clog Security Ever     Log All Sessions     Enable Web Cache     Enable WAN Optim</td><td>FortiManager n × +</td><td>s FortiGuard L s FortiGuard L dentity ODevice Id</td><td>roup-ID:1)</td><td>Cancel</td><td>cebook</td></li<></ul>	Policy Type     Policy Type     Policy Subtype     Incoming Interface     Source Address     Outgoing Interface     Destination Address     Schedule     Service     Action     NAT     Logging Options     No Log     Clog Security Ever     Log All Sessions     Enable Web Cache     Enable WAN Optim	FortiManager n × +	s FortiGuard L s FortiGuard L dentity ODevice Id	roup-ID:1)	Cancel	cebook

(172.30.71.92/index.htm?action=lo	gin#				ਊ ≞ G (	🙁 🕆 jessica herrin face	book	۹. 🖡 🍙	
EF FortiManager VM64	Device Manager	Policy & Objects	FortiGuard	.og View	Drill Down	Event Management	Reports	System Settin	gs ? (
Display Options Revisions Policy Package  Policy Package  Characteristic Constraints  Colored and the second seco	Policy Type Policy Subtype Incoming Interface Source Address Outgoing Interface Destination Address Schedule Service Action		Identity O Device	Identity	] 0 ] 0 ] 0 ] 0 ] 0		Action	OSection View Profile Log 2	Global V     NAT Con     S
Cone     N     Service     Service     Service     Service     Service     Sochedule     Traffic Shaper     Security Profiles     Security Profile     Web Filter Profile     Application Sensor     Sensor     Sensor     Susser Sensor     Susser Sensor	NAT Logging Options No Log Log Security Event Log All Sessions Enable Web Cache Enable WAN Optimiz	s				OK Cancel	10.212.134	.210	

(1) FortiManager FMG-VM64 HAC * *     (2) T2:30.71.92/index.htm?action=login#   FortiManager VM64 Device Manager Policy & Objects Policy & Objects Policy Bodiager Policy & Objects Policy Policy & Objects Policy Policy Policy Section View Office Policy Policy Policy Section View Office Sectin	000			FortiManager: F	MG-VM64	HA(Group	-ID:1)							M
	FortiManager: FMG-VM64 HA(G	×	Please login	× ) + )										
Circle Manager VM64       Device Manager       Policy & Objects       Fort/Guard       Log View       Drill Down       Event Management       Reports       System Settings         Dicalv Actions       Revisions         Policy Package       Source Interface       Destination       Schedule       Service       Authentication       Action       Profile       Log NAT       Image: Source Interface       Authentication       Action       Profile       Log NAT       Image: Source Interface       Source Interface       Source Interface       Source Interface       Image: Source Interface       Source Interface <t< th=""><th>( 3 3 172.30.71.92/index.htm?ac</th><th>tion=login#</th><th></th><th></th><th></th><th></th><th> ⊽ C</th><th>🙁 🕈 jess</th><th>ica herrin facebo</th><th>ook '</th><th>۹) 🖡</th><th></th><th>-</th><th></th></t<>	( 3 3 172.30.71.92/index.htm?ac	tion=login#					⊽ C	🙁 🕈 jess	ica herrin facebo	ook '	۹) 🖡		-	
Objects Policy Policy Source Destination Schedule Service Authentication Action Profile Log NAT   I Sinternal Secternal * all *	E FortiManager VM6	4	Device Manager	Policy & Objects	FortiGua	rd Log Vi	iew Drill Dov	wn Event	Management	Reports	System	Settir	igs	?
Seq.#       Source Interface       Destination Interface       Source Destination       Schedule       Service       Authentication       Action       Profile       Log       NAT         I       Binternal       Binternal       Binternal       # all       # all       # all       # always       BALL       Accept       Image: Comparison of the comparis	Display Options Revisions Policy Package	Policy									Osectio	on View	Glot	al Vie
Dijects Create New * Delete El Column Settings Search   Source Objects Create New * Delete Delete   Source Search Search   Source Search Search   Source Search Search   Source Search Search	Policy Package	Seq.#	Source Interface	Destination Interface	Source	Destination	Schedule	Service	Authentication	Action	Profile	Log	NAT	Cor
Qefault       2 Sectornal       internal       * all       * all <td>- ELBC</td> <td>1</td> <td>😕 internal</td> <td>🗏 external</td> <td>* all</td> <td>* all</td> <td>* always</td> <td>🔀 ALL</td> <td></td> <td>S Accept</td> <td></td> <td>9</td> <td>Θ</td> <td></td>	- ELBC	1	😕 internal	🗏 external	* all	* all	* always	🔀 ALL		S Accept		9	Θ	
Objects       Create New *       Delete       Column Settings       Search         Source       Name       Type       Interface       Details         Firewall Objects       66 SSLVPN_TUNNEL_ADDR1       Address       any       IP Range:10.212.134.200-10.212.134.200         Address       asy       IP/Mask:0.0.0/0.0.0.0       asy       IP/Mask:0.0.0/0.0.0.0         Service       65 SSLVPN_TUNNEL_IPV6_ADDR1       IPv6 Address       fdff:fff::1/120         Scaurity Profiles       asi       IPv6 Address       ::/0         Virtual IP       Security Profiles       ::/0       ::/0         Application Sensor       IPS Sensor       ::/0       ::/0	default	2	🔀 external	5 internal	* all	* all	* always	ALL		S Accept		0	0	
Name       Type       Interface       Details         Image: Dispects       Image: Dispects       Image: Dispects       Image: Dispect Dispects         Image: Dispect Dispects       Image: Dispect	Objects	O Creat	te New 🔹 🗍 De	elete 🔲 Colun	nn Setting	S				Sea	ch			
Image: StyPe_TUNNEL_ADDR1       Address       any       IP Range: 10.212.134.200-10.212.134.200         Image: Address       any       IP Range: 10.212.134.200-10.212.134.200       IP Range: 10.212.134.200-10.212.134.200         Image: 10.212.134.200-10.212.134.200-10.212.134.200       Image: 10.212.134.200-10.212.134.200       Image: 10.212.134.200-10.212.134.200         Image: 10.212.134.200-10.212.134.200       Image: 10.212.134.200-10.212.134.200       Image: 10.212.134.200-10.212.134.200         Image: 10.212.134.200       Image: 10.212.134.200       Image: 10.212.134.200       Image: 10.212.134.200         Image: 10.212.134.200       Image: 10.212.134.200       Image: 10.212.134.200       Image: 10.212.134.200         Image: 10.212.134.200       Image: 10.212.134.200       Image: 10.212.134.200       Image: 10.212.134.200         Image: 10.212.134.200       Image: 10.212.134	- 🛐 Zone	Name			Туре	I	interface	Details						
Address       any       IP/Mask:0.0.0/0.0.0.0         Address       any       IP/Mask:0.0.0/0.0.0.0         Schedule       IB SSLVPN_TUNNEL_IPV6_ADDR1       IPv6 Address       Idfr:ffff:::1/120         Traffic Shaper       IB SSLVPN_TUNNEL_IPV6_ADDR1       IPv6 Address       :/0         Virtual IP       Scurity Profiles       :/0       :/0         Application Sensor       IPS Sensor       :/0       :/0         User & Device       IPS Sensor       :/0       :/0	🗄 🧱 Firewall Objects	SSLVPN_	TUNNEL_ADDR1		Address	a	any	IP Range:1	0.212.134.200-1	0.212.134.2	10			
Image: Service       Image	Address	🗐 all			Address	а	any	IP/Mask:0.0	0.0.0/0.0.0.0					
	Cabadula	6 SSLVPN_	TUNNEL_IPV6_ADDR:	1	IPv6 Addre	SS		fdff:ffff::1/	120					
Virtual IP  AtVVirus Profile  AtVVirus Profile  Application Sensor  IPS Sensor  User & Device	Traffic Shaper	6 all			IPv6 Addre	ss		::/0						
Image: Security Profiles         Image: Security Profile	Cirtual IP													
Image: Second	= 🌀 Security Profiles													
Web Filter Profile	AntiVirus Profile													
User & Device	Web Filter Profile													
User & Device	Application Sensor													
	IPS Sensor													
	IPS Sensor     Jose & Device													

# **Deploy System Configuration and Firewall Policy Packages**

Once configurations are completed, install all changes through **Device Manager**.

Figure 8-1-29				Frankling and FMC	VACA HAIC	- (D.1)				
East Manager FMC V	MEANAC	v dtb Blaze	e legis	Fortimanager: FMG-	VM04 HA(Grou	ip-iD:1)				
Continentager. PMG-V	MO4 HA(G	· lass riea:	se login	~ [ +						
( 172.30.71.92/ir	ndex.htm?actio	on=login#					- ₹ ( <mark>8</mark>	<ul> <li>jessica herrin facebook</li> </ul>	a) 📳	
=== FortiManac	er VM64			~				x	~	
		Device	Manager	Policy & Objects For	tiGuard Log	View D	rill Down	Event Management R	eports Syster	n Settings 🛛 🤨
Device Manager								Search		
All FortiGate(2)		Device Na	me	- Config Status	Policy Packa	age Status	8	Connectivity	IP	Platform
All Log Arrays(0)	Device			( Pending			0		10.100.23.222	FortiGate-5001B
	O Add D	evice					G FG-5k	(B3E11700407 (Master)		
	install	N					FG-5K	(B3E11700378 (Slave)		
	and Custor	mize Device Tabs					G FG-5K	(B3E11700411 (Slave)		
	Device Gro	up					G FG-5K	(B3E12700001 (Slave)		
	Create	e New					G FG-5k	(B3E12700041 (Slave)		
	Edit						ILD FG-5K	ELBC: SV	stem 🕨 Dasht	oard [Custom
	1 Eirmw	are Undate								
			1					Connection Summa	ry	
		Flostname Carial Number	C15503	00407				1P Tatasfasa	10.100.23.22	2
		Eirmware Version	FG-5KB3E117	3 (0208) [lindate]				Connection User	admin	
		Hardware Statue	8 CPU 11975	MB PAM				Connectivity	Q [Refrech]	
		HA Mode	ELBC Cluster					Connect to CLI via	TELNET	SSH
		Cluster Members	Chassis:Slo	ot # Serial Number	Role	Status	Action	Configuration and 1	Installation Stat	
			1:3	FG-5KB3E11700	407 Master	0		System Template	default [Char	ael
			1:4	FG-5KB3E11700	636 Slave 4	0		Logging Device	None	
			1:5	FG-5KB3E11700	411 Slave 3	0		FortiGuard Update	None	
			1:6	FG-5KB3E12700	041 Slave 6	0		Device		
			2:3	FG-5KB3E11700	378 Slave 2	0		Database	View	
			2:4	FG-5KB3E12700	001 Slave 5	0		Total Revisions		
			2:5	FG-5KB3E12700	088 Slave 7	0		Concerned and the	1 [Revision ]	listory]
			2:6	FG-5KB3E11700	315 Slave 1	0		Sync Status	Synchronized	[Refresh]
		VDOM	Enabled [Disa	ble]				Installation Tracking	None	
		Session Information	[View Sessio	n List]				Device Settings	Modified	
		System Time	Sat Oct 26 16	:11:22 PDT 2013 [Char	nge]			Status	riounled	
		Description						Installation Preview	<u>s</u>	
72.30.71.92/index.htm?act	tion=login#	Operation	34	<b>∩</b>				Last Installation	None	





Figure 8-1-32

FortiManager: FMG-VM6	4 HA(G × 🔃 Plea	FortiManager: FMG-VM64 HA	(Group-ID:1)		
172.30.71.92/index	x.htm?action=login#		', ∼ C'	Service a servin facebook	<u> </u>
E FortiManager	VM64 Device	e Manager Policy & Objects FortiGuard	Log View Drill Dow	n Event Management R	eports System Settings 🕐 🕻
Device Manager				Search	
All FortiGate(2)	Install	Validation	1. 200		IP 1 10.100.23.222 Fort (er)
	What to Install	Installation Preparation			e) e)
	Device Selection	Zone Validation			Dashboard [Costomiz
	Validation	Ready to Install			00.23.222 -mgmt
	Install	Device Name	VDOM Name Stat	us	n
		ELBC	root 🖸	Preview	ELNET SSH
			11.5		ion Status ilt <u>[Change]</u>
					-
					evision History]
					odified
	Description		<	Back Next > Canc	
	Operation	Reboot O Shutdown		Last Installation	Revision-2 (2013-10-26
Provisioning Templates	License Informatio	n		Scheduled	None

000		FortiManager: FMG-VM64 H	A(Group-ID:1)		M <sub>20</sub>
FortiManager: FMG-VM64	HA(G × 🚺 Please	login × +			
( 172.30.71.92/index.	htm?action=login#		∰ ₹ C	🙁 🛪 jessica herrin facebook	۹ 🛃 🍙 💽 - 🚺
1": FortiManagor				s	
t=5 i oi timanagei	Device	Manager Policy & Objects FortiGuard	Log View Drill Down	Event Management Report	s System Settings ? 🕼
Device Manager				Search	
All Log Arrays(0)	Install  What to Install  Device Selection  Validation  Install  Description Operation	Installation Installing settings to devices. Total:1/1, Success:1, Error:0, Warning ( Index Name - Status I ELBC Install and save fin	I 100% History Ished status=OK	Finish Installation Preview Last Installation N	Platform 23.222 FortiGate-5001B 23.222 FortiGate-5001B Dashboard [Customize] D.23.222 -mgmt n efresh] ELNET • SSH in Status it [Change] fed fed
Provisioning Templates	License Information			Scheduled N	one
×					



To upgrade the FortiGate through the FortiManager ensure that the required OS has been downloaded into the FortiManager. Then go to **Device Manager**, **System Information** and update the Firmware.



000		Fort	iManager: FMC	G-VM64 HA	(Group-ID:1)							M <sub>21</sub>
FortiManager: FMG-VM64 HA(G	× Please login	ж	https:	//10.100.23	222/login ×	: [+]				_		
(172.30.71.92/index.htm?acti	on=login				r.	7 7 C (	🙁 🕆 jessica he	rrin facebo	ook (	ء 💽		
E FortiManager VM64	Device Manag	er Policy	& Objects F	ortiGuard	Log View C	Drill Down	Event Mana	gement	Reports	System Se	ttings 📑	? 📳
Device Manager								Search				
All FortiGate(2)	Device Name	~ 7	Config Status	Policy	Package Status		Connectivity		IP		Platform	*
a Ali Log Arrays(0) → ELBC		e	Synchronized			<ul> <li>FG-</li> <li>FG-</li></ul>	5KB3E1170040 5KB3E1170031 5KB3E1170037 5KB3E1170041 5KB3E1170063 5KB3E1270000 5KB3E1270000 5KB3E1270008	7 (Master) 5 (Slave) 8 (Slave) 1 (Slave) 5 (Slave) 1 (Slave) 1 (Slave) 8 (Slave)	10.100.2	3.222 For	iGate-5001E	3
	root [NAT]	6	Not Modified	C ELBC						VD	мс	
		ement) 👩	Not Modified	63						VD	ом	*
	🍪 Menu 🔻							ELBC:	System 🕨	Dashboar	d [Custo	mize]
	<b>Device Firmware Inform</b>	ation										
	Current Firmware											
	Partition	Active		F	irmware		Sta	atus				
	1	0		FortiGat	e 5.0.3 (0208)		Run	ning				
	Available Upgrades											
	Firmware		Release D	Date		Upgrade		1				
	5.00-00228-228		13-08-0	09	[Upgrade No	w] [Schedu	ule Upgrade]					
	Upgrade History											
				Records				>>	1			
			1	Return								
172.30.71.92/col-bin/module/firmwarem	ng/FMCFwmDevice?deviceId=196#											
× Find: Q 5001	) (Next   Previous ) ( High	light all ) 🛛	Match case									
*												

FortiManager: FMG-VM64 HA(G 3	× Please login	× https://	(10.100.23.222/login )			
(A) @ 172 20 71 02 linday have				^   T		
1/2.30./1.92/index.htm/actio	on=login		1	☆ ▽ C' 🚺 🛛 Jessica he	rrin facebook Q	🛃 🍙 💽 🖬
The Contillionagor VM64		and the second states of		and the second second		
E_F FORUMANAGER VM04	Device Manag	er Policy & Objects Fo				ystem Settings 🛛 😮 💽
					Search	
All FortiGate(2)	Device Name	Config Status	Policy Package Status	Connectivity	IP	Platform
⊣ 🖶 Ali Log Arrays(0)	ELBC  Are yo  root [NAT]  A ethernom [NA]  Menu +  Device Firmware  Current Firmware	Synchronized to sure you want to continue to the sure you want to continue to	upgrade firmware on the sel	CK	(Master) (Slave) (Slave) (Slave) (Slave) (Slave) (Slave) (Slave) (Slave) (Slave) (Slave)	22 FortiGate-50018 VDOM vDOM ashboard [Customize]
	Partition	Active	Firmware	Sta	tus	
	1	0	FortiGate 5.0.3 (0208)	Run	ning	
	Available Upgrades					
	Firmware	Release Da	ite	Upgrade		
	5.00-00228-228	13-08-09	Upgrade No	w] [Schedule Upgrade]		
	upgrade History		Decords		1551	
			Records			
			Keturn			
Provisioning Templates						
× Find: (Q, 5001	(Next   Previous) (O High	light all 🔰 🗹 Match case				

000		FortiManager: FM0	G-VM64 HA(Group-ID:1	)		2 <sup>2</sup>
FortiManager: FMG-VM64 HA	(G × 🔃 Please login	× https:	//10.100.23.222/login	× +		
( ) @ 172.30.71.92/index.htm	n?action=login			☆ ▽ C ) (입 ▼ jessica herrin facel	oook Q	
E FortiManager VI	M64 Device Manager	Policy & Objects F	FortiGuard Log View	Drill Down Event Management	Reports Syst	em Settings 🕐 🔐
Device Manager				Search	Alcologination possible co	
All FortiGate(2)	Device Name	Config Status	Policy Package Statu	s TConnectivity	IP	Platform
🖶 Ali Log Arrays(0)	没 ELBC	Synchronized		<ul> <li>○</li> <li>○</li></ul>	10.100.23.222	FortiGate-5001B
	(NAT)	Not Modified	C ELBC			VDOM
	A elbc-mamt (NAT) (Management	) 🔊 Not Modified	0			VDOM
	Partition Active Firmw 1 PartiGate 5. Available Upgrades	ware 0.3 (0208) FortiGa	Statu te5.00 00228 scheduled at	is 2013-10-26 22:32:17 <u><b>Cancel</b></u>		
	Firmware	Polease	Date	Inorade		
	5.00-00228-228	13-08	-09 4	Accepted		
	Upgrade History			15		
	#	Re	ecords	>>		
		Re	turn			
Provisioning Templates						
× Find: Q 5001	Next Previous O Highlight all	Match case				
×		and the second second				

The Firmware is downloaded to the Master FortiGate and verified for integrity.

• To minimize upgrade interruptions, all FortiGates in the slave chassis is upgrade first then rebooted. Once the reboot process completes a message will appear on the Master FortiGate indicating that a master/slave chassis switch over can now occur.

All members of the slave chassis are ready for traffic. You may switch over the master chassis now.

 To demote the master chassis determine which FortiSwitch is master as shown below.

```
15s01 # diagnose system ha status
mode: a-p
minimize chassis failover: 1
c15s01(FS503B3E11700005), Master(priority=0), uptime=113317.85, chassis=1(1)
c15s02(FS503B3E11700244), Slave(priority=1), uptime=14641.00, chassis=1(1)
c16s02(FS503B3E11700261), Slave(priority=2), uptime=9805.33, chassis=2(1)
c16s01(FS503B3E11700266), Slave(priority=3), uptime=9807.49, chassis=2(1)
```

• Enter the following command on the master FortiSwitch forcing the master chassis to become slave and a failover to occur. Replace the character "1" with "2" to specify chassis 2 if it is master.

```
c15s01 \ \text{\# diagnose system ha force-slave-state by-chassis 3 1}
```

delaying application of force by-chassis by 3 seconds New force setting is configured as: Apply at: system time(116398) delay remaining(3) Slave Chassis: 1 Slave SN: (Note: application time will be adjusted so that delay starts after configuration is confirmed.)

WARNING: Setting a forced HA state will override normal HA failover, including failover due to network connectivity and workblade loss. This can cause network

outages if the unit forced to master loses all connectivity or workers! DO NOT FORGET TO CLEAR THE FORCED STATE. Do you want to continue? (y/n)y

c15s03 login: Master chassis switchover is done. Time to upgrade myself now.

Firmware upgrade in progress... Done.

• Once all FortiGates have rebooted and synchronized, locate the master FortiSwitch and clear the force slave state. If the force slave state is not cleared, chassis 2 will always remain master and ignore all heath status of the chassis. Clearing can only be done on the current master FortiSwitch.

#### c15s01 # diagnose system ha status

c15s01(FS503B3E11700005), Slave(priority=3), uptime=1263.69, chassis=1(2) c16s02(FS503B3E11700261), Master(priority=0), uptime=11253.15, chassis=2(2) c16s01(FS503B3E11700266), Slave(priority=1), uptime=11255.03, chassis=2(2) c15s02(FS503B3E11700244), Slave(priority=2), uptime=16088.78, chassis=1(2)

#### c16s02 **# diagnose system ha force-slave-state clear** No delay passed, using default of 5

Warning: clearing these settings may cause a failover if there are units in a better state than the current master. Do you want to continue? (y/n)y The FortiManager does not manage the FortiSwitch, rather it is used as a repository for configurations and scripting.

### **Add FortiSwitch**

To add a FortiSwitch, right click **All FortiGate** to access the pop out menu and follow the figures below.







0 172.30.71.92/mde	x.numaction=login			H	S P Jessica Herrin Tacebook			
FortiManage	r VM64	Device Manager Policy & O	bjects FortiGuard Log Vie	ew Drill Down	Event Management Report	ts System Settings		
vice Manager	-	1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -			Search			
All FortiGate(2)	Add Device	Login				IP 10.100.23.222 Master) ilaye)		
	e Login	Please choose on	ne of the following methods for a	dding a device or v	dom.	ilave) ilave)		
	Discover	• Discover	Discover  Import Device					
	Add Device	Device will b	0.23.222					
	Profiles	Please ente	-mgmt					
	• VDOM	IP Addres	s 10.100.23.221			tefresh]		
	Sone Map	User Nam	e admin			ELNET SSH		
	Policy	Password	•••••			lt [Change]		
	<ul> <li>Object</li> </ul>	O Add Model I	Device					
	Import	Device will b	e added using the chosen mode	type and other ex	plicitly entered information.			
	Summary					Revision History]		
						hronized [Refresh]		
		_			Next > Cancel	odified		
	Description				Installation Preview	\$		
	Operation	Reboot O Shut	tdown		Last Installation	Revision-9 (2013-10-27		











Shelf Managers can be added to the FortiManager, it is useful to gather power statistics and be able to reboot individual slots from the Manager.

# Add The Shelf Manager

To add the Shelf Manager, chassis management must first be enabled through the FortiManager's CLI then refresh the WebUI browser.

config system admin setting set chassis-mgmt enable end

Right click **All FortiGate** to access the pop out menu.

# **FortiAnalyzer**

Each FortiGate logs directly to the FortiAnalyzer using it's own local resources and base-mgmt IP address. The FortiSwitch NAT's all FortiGates IP addresses to the base-mgmt-external-ip interface. All traffic received by the FortiAnalyzer will appear to have sourced from the same IP. As previously noted in the **FortiGate** section, a default route within the elbc-mgmt VDOM is required for external logging.

For additional FortiAnalyzer configuration information, please refer to <u>http://docs.fortinet.com</u>.

# FortiGate Log Settings

Logging can either be configured via the FortiManager or via the CLI. Once complete, the FortiGates will automatically attempt to register with the FortiAnalyzer.

c15s03 (global) # conf log fortianalyzer setting c15s03 (setting) # config log fortianalyzer setting set status enable set server 172.30.71.50 set upload-option realtime end

	M04 ( T (						
1) @ 172.30.71.50/inde	x.htm?action=login			$\sum_{i=1}^{N} \nabla \mathbf{C}_{i}$	🙁 🛪 jessica her	rin facebook	۹ 🔸 🍙 💽 - 🛛
FortiAnalyze	r VM64 Device	Manager Log View Dr	ill Down Event Manage	ement Repor	ts System Sett	ings	?
vice Manager						Search	
All FortiGate(0)	Device Name	<ul> <li>Logs</li> <li>IP</li> </ul>	Platform	Quota	Secure	Connection	Description
) All Log Arrays(0)	No records found.						
		U	nregistered Device				
	The following device(s) ar	e requesting to be registe	red on this FortiAnalyze	r. Please choo	se an action or o	lecide later.	
				Action			
	Name	Model	Connecting IP	🗹 Add	Delete	Later	
	FG-5KB3E11700407	FortiGate-5001B	10.100.23.222	Add	Oelete	OLater	
	FG-5KB3E11700636	FortiGate-5001B	10.100.23.222	Add	Oelete	OLater	
	FG-5KB3E11700411	FortiGate-5001B	10.100.23.222	• Add	Oelete	Later	
	FG-5KB3E12700041	FortiGate-5001B	10.100.23.222	Add	Oelete	OLater	
	FG-5KB3E11700378	FortiGate-5001B	10.100.23.222	Add	Oelete	Later	
	FG-5KB3E12700001	FortiGate-5001B	10.100.23.222	Add	Oelete	OLater	
	FG-5KB3E12700088	FortiGate-5001B	10.100.23.222	Add	Oelete	OLater	
	FG-5KB3E11700315	FortiGate-5001B	10.100.23.222	Add	Oelete	OLater	
					Apply	Decide Later	

Grant the FortiGates registration access to the FortiAnalyzer

Sixteen devices are show because there are eight FortiGates and each one has two VDOMs.

	~ .	
Figure	9-1	-2

172.30.71.50/index.htm?action	n=login				1	ी र <b>८</b> (	🕙 🛪 jessica her	rin facebook Q	
FortiAnalyzer VM64	De	vice Manager	Log View	Drill Down	Event Management	Reports	System Setti	Ings	
vice Manager							5	Search	
All FortiGate(16)	Device Name	Logs	IP		Platform	Quota		Secure Connection	Description
All Log Arrays(0)	💼 c15s03		10.100.2	3.222	ortiGate-5001B	ŕ		8	
	🝙 elbc-mgmt				/DOM			0	
	🝙 root	•		,	/DOM			0	
	🚍 c15s04	•	10.100.2	3.222	FortiGate-5001B	Ē		8	
	ige elbc-mgmt	•		,	/DOM			0	
	i root	•			/DOM			0	
	c15s05		10.100.2	3.222	ortiGate-5001B	1		0	
	elbc-mgmt				/DOM			0	
	💿 root			,	/DOM			0	
	c15s06		10.100.2	3.222	ortiGate-5001B	ř.		0	
	🝙 elbc-mgmt				/DOM			0	
	S root	•		,	/DOM			0	
	💼 c16s03	•	10.100.2	3.222	ortiGate-5001B	ř		0	
	🝙 elbc-mgmt				/DOM			0	
	🝙 root	•			/DOM			0	
	💼 c16s04	•	10.100.2	3.222	FortiGate-5001B	r.		8	
	elbc-mgmt	•		,	/DOM			0	
	🝙 root	•		,	/DOM			0	
	🚍 c16s05	•	10.100.2	3.222	ortiGate-5001B	(		0	
	i elbc-mgmt	•		,	/DOM			0	
	🝙 root	•			/DOM			0	
	🚍 c16s06	•	10.100.2	3.222	ortiGate-5001B	£		8	
	elbc-mgmt				/DOM			0	
	i root	•		,	/DOM			0	
l.	A Menu T								c15c02+

Create a Log Array so that logs from all FortiGates are put at a single place for faster access.



Figur	re 9-1-5								
000	0				FortiAnalyze	er: FAZVM64			R.
Jo	FortiAnalyzer: FAZVM64	+							
	172.30.71.50/index.htm?actio	on=login					ୁ ≂ <b>୯</b> (	<u>8</u> – jessica herrin facebook	۹ 🔮 🍙 💽 - 🚺
	FortiAnalyzer VM64						-	<u> </u>	
	r or thruldy 201 Third T		Device Manager	Log View	Drill Down	Event Management	Reports	System Settings	× .
Device	Manager			_	_		_	Search	
All	I FortiGate(16)	Name 🔺				Member			Quota(MB)
	ll Log Arrays(1)	ELBC	c15s03[elbc-mgmt], c15s c16s05[elbc-mgmt], c16s	04[elbc-mgn 06[elbc-mgn	nt], c15s05[elb nt]	c-mgmt], c15s06[elbc-n	ngmt], c16s0	3[elbc-mgmt], c16s04[elbc-mgmt],	
		🔕 Menu	•						ELBC: Report
× Find:	: Q 5001b	Next I	Previous ) (O Highlight	all ) 🗹 Mat	tch case Phras	se not found			
×									•

Verify that logs have been transmitted to the FortiAnalyzer.

Figure 9-	1-6
-----------	-----

000 F				FortiAnalyzer: FAZVM64				
FortiAnalyzer: FAZVM64	+							
3 3 172.30.71.50/index.htm?a	ction=log	in		ର୍ଦ୍ଧ ଟ C' ] ( <mark>ଃ</mark> + je	essica herrin facebook	۹ 🎝 🔝 🛽		
E FortiAnalyzer VM	64	Device Manager	Log View Drill Down Eve	nt Management Reports Syst	em Settinos	?		
Log View	Qus	usr=Jane msg=success*		reports System Strangs		e 🗟 🏼		
ELBC #		Date/Time	Level	Message		User		
	1	01:02:04		User Fortimanager_Access has entered the virtual domain elbc-momt	5	🔄 Fortimanager_/		
- System 2		01:01:27		Performance statistics				
	з	01:01:24		Performance statistics				
	4	01:01:23	MARCON CO.	Performance statistics				
	5	01:01:01		Performance statistics				
	6	01:01:01	and the second sec	Performance statistics				
	7	01:00:59		Performance statistics				
	8	01:00:58	(Contraction)	Performance statistics				
	9	00:59:56		Edit log.fortianalyzer.setting		🔁 admin		
	10	00:59:56		Edit log.fortianalyzer.setting		🔁 admin		
	11	00:59:56		Edit log.fortianalyzer.setting		🔁 admin		
	12	00:59:56		Edit log.fortianalyzer.setting		2 admin		
	13	00:59:56		Edit log.fortianalyzer.setting		🔁 admin		
	14	00:59:56		Edit log.fortianalyzer.setting		🔁 admin		
		50   Items per page << first < prev 1 2 next > last >> Go to page 1 of 2						
	Log	Log Details						
		ice ID FG-5KB3 FG-5KB3 FG VUSer For sage User For elbc-ma	vitch 3E11700407 ion timanager_Access has entered the mt	Date/Time Device Time Log ID virtual domain Reason	01:02:04 2013-10-28 00:59:10 32006 none	)		