

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	7
<i>Hardware</i>	8
<i>Functions</i>	13
<i>Traffic Processing</i>	13
<i>Traffic Load Balancing</i>	14
<i>Understanding NAT & Load Balancing</i>	16
<i>FortiSwitch Concepts</i>	18
FortiGate Architecture	19
<i>Hardware</i>	19
<i>Functions</i>	20
<i>Traffic Processing</i>	20
Naming Scheme	21
FortiSwitch	21
Master FortiSwitch Chassis 15 Slot 1 Configuration Example.....	23
Slave FortiSwitch Chassis 15 Slot 2 Configuration Example	25
Slave FortiSwitch Chassis 16 Slot 1 Configuration Example	27
Slave FortiSwitch Chassis 16 Slot 2 Configuration Example	29
FortiSwitch Installation.....	31
<i>Method 1</i>	31
<i>Method 2</i>	32
FortiSwitch HA Synchronization	33
<i>Verification</i>	33
<i>Troubleshooting FortiSwitch HA</i>	34
Understanding Service Groups.....	39
<i>Managing Service Group Slots</i>	47
<i>Troubleshooting Service Groups</i>	48
<i>Installing a New FortiGate into an Existing Service Group</i>	52
FortiGate	54
ELBCv3 Installation.....	54
<i>Management Routing</i>	56
<i>Troubleshooting FortiGate Joins</i>	57
<i>Reducing Single Core CPU Usage</i>	58
FortiSwitch & FortiGate SNMP	59
Enable SNMP.....	59
<i>Query the FortiSwitch</i>	60
<i>Query the FortiGate</i>	61
<i>FortiSwitch Service Group Worker Blades Commonly Used OIDs</i>	62
<i>SNMP Interface Statistics</i>	63

Traps.....	64
FortiManager.....	66
FortiGate Management.....	66
<i>Install FortiGate Firewalls.....</i>	<i>66</i>
<i>Associating FortiGate Interfaces with Zones</i>	<i>72</i>
<i>Adding Policy Package</i>	<i>78</i>
<i>Deploy System Configuration and Firewall Policy Packages</i>	<i>83</i>
FortiGate Firmware Upgrade.....	86
FortiSwitch Management.....	90
<i>Add FortiSwitch.....</i>	<i>90</i>
Chassis Shelf Manager.....	95
<i>Add The Shelf Manager</i>	<i>95</i>
FortiAnalyzer	96
FortiGate Log Settings.....	96
<i>Logging to the Analyzer.....</i>	<i>97</i>

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 <http://docs.fortinet.com>.

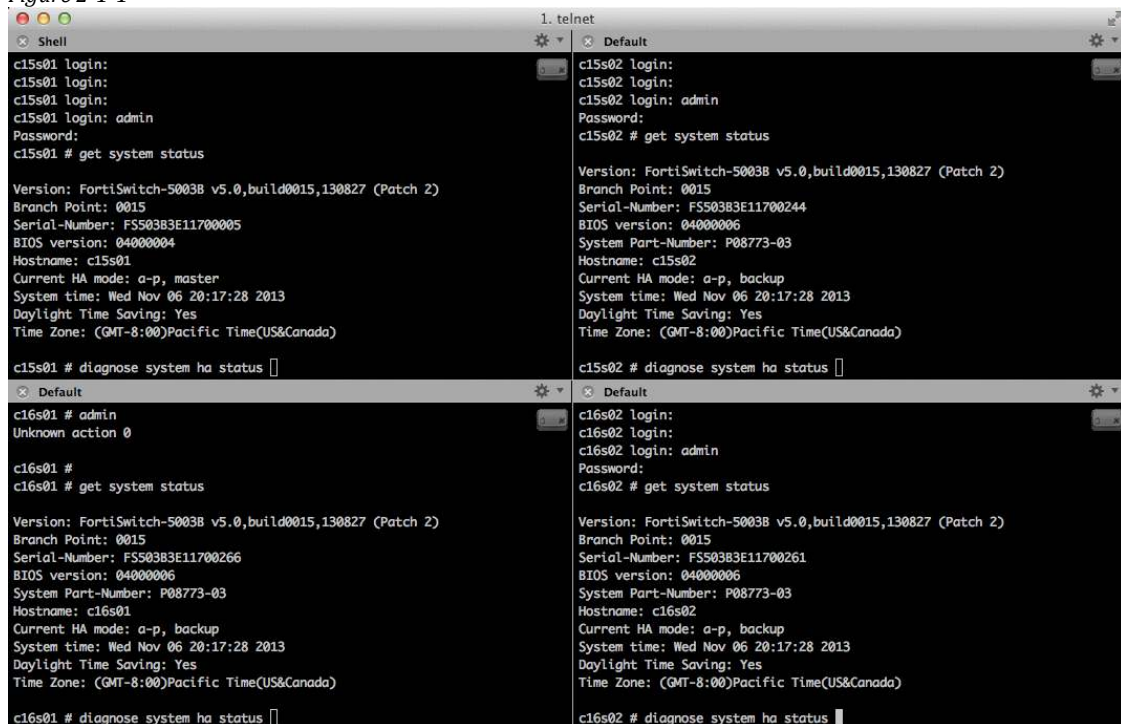
Intended Audience

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. telnet
Shell
c15s01 login:
c15s01 login:
c15s01 login:
c15s01 login: admin
Password:
c15s01 # get system status

Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)
Branch Point: 0015
Serial-Number: F550383E11700005
BIOS version: 04000004
Hostname: c15s01
Current HA mode: a-p, master
System time: Wed Nov 06 20:17:28 2013
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

c15s01 # diagnose system ha status

Default
c15s01 # admin
Unknown action 0

c15s01 #
c15s01 # get system status

Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)
Branch Point: 0015
Serial-Number: F550383E11700266
BIOS version: 04000006
System Part-Number: P08773-03
Hostname: c16s01
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&Canada)

c15s01 # diagnose system ha status

Default
c15s02 login:
c15s02 login:
c15s02 login: admin
Password:
c15s02 # get system status

Version: FortiSwitch-5003B v5.0,build0015,130827 (Patch 2)
Branch Point: 0015
Serial-Number: F550383E11700244
BIOS version: 04000006
System Part-Number: P08773-03
Hostname: c15s02
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&Canada)

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)
Branch Point: 0015
Serial-Number: F550383E11700261
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&Canada)

c16s02 # diagnose system ha status
```

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

Hardware

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

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

Figure 3-1-1



FG5140B

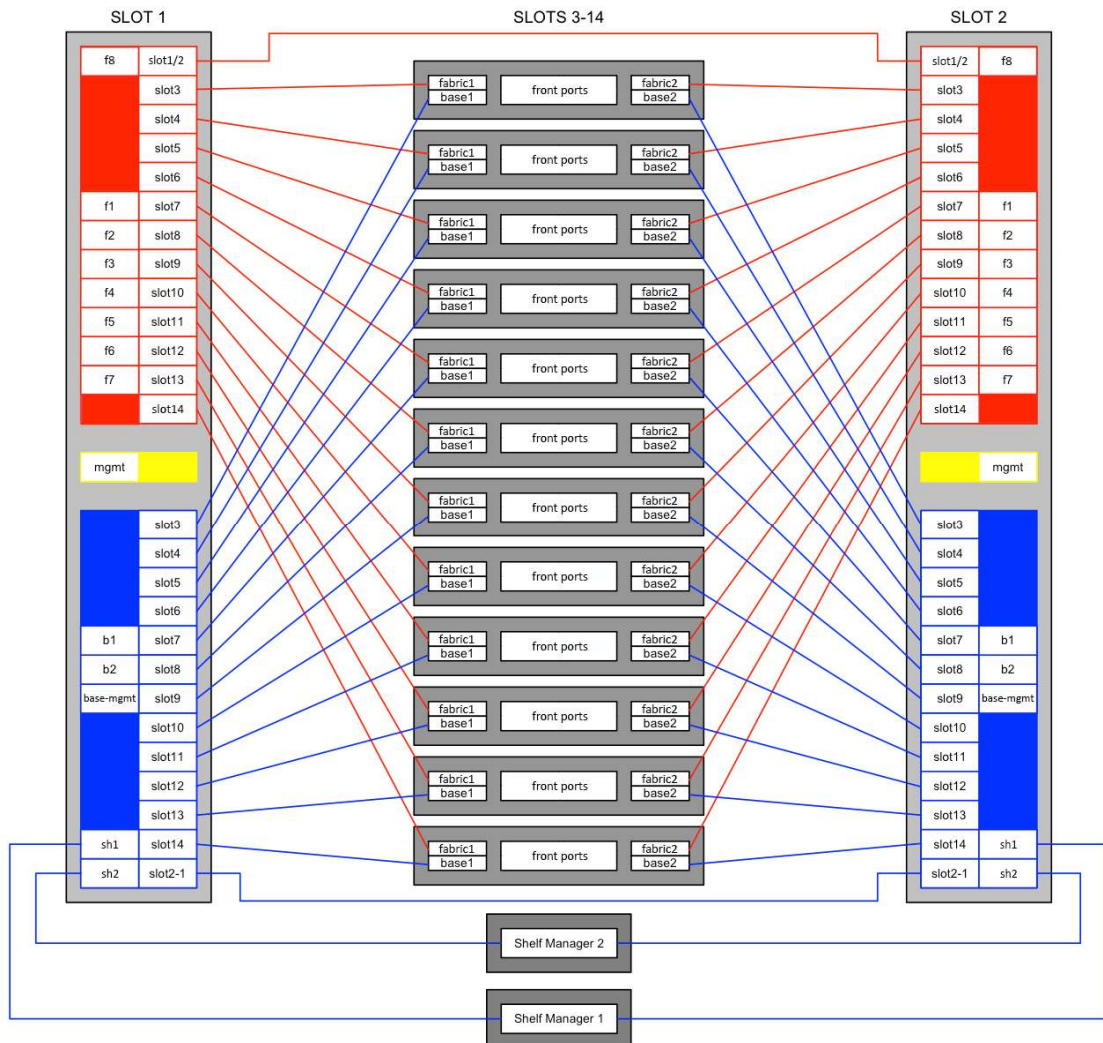
FG5060

- 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.

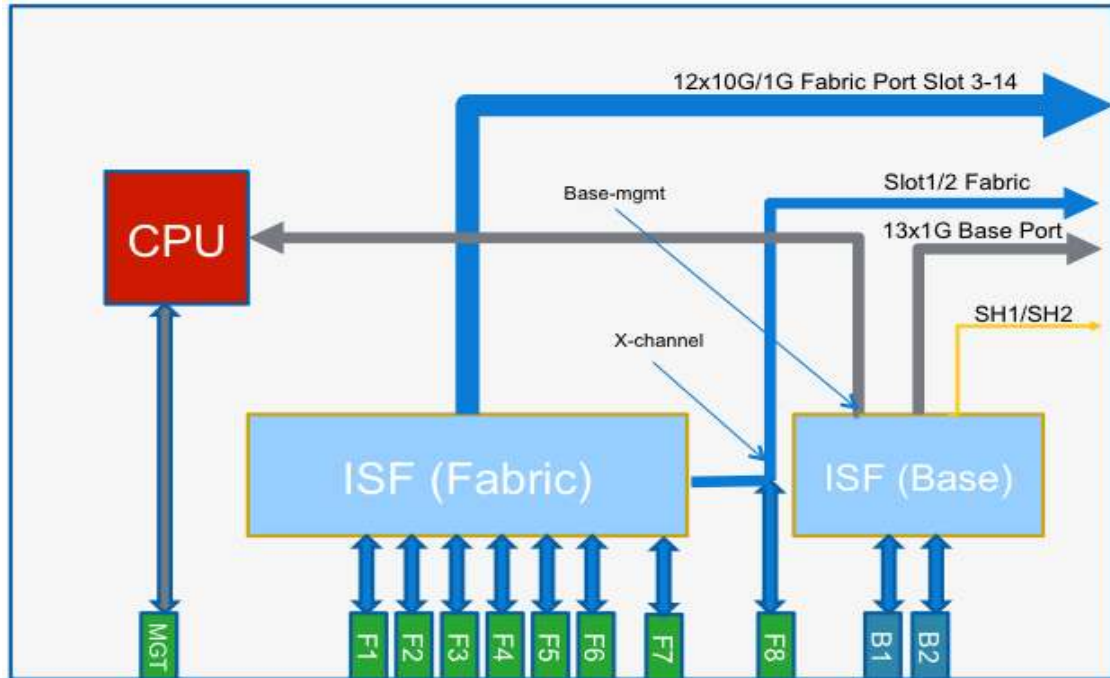
The diagram conceptualizes internal connectivity for an FG5140B chassis.

Figure 3-1-2



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

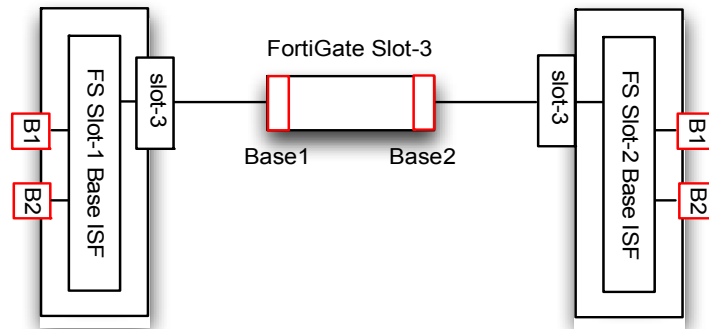
Figure 3-1-3



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

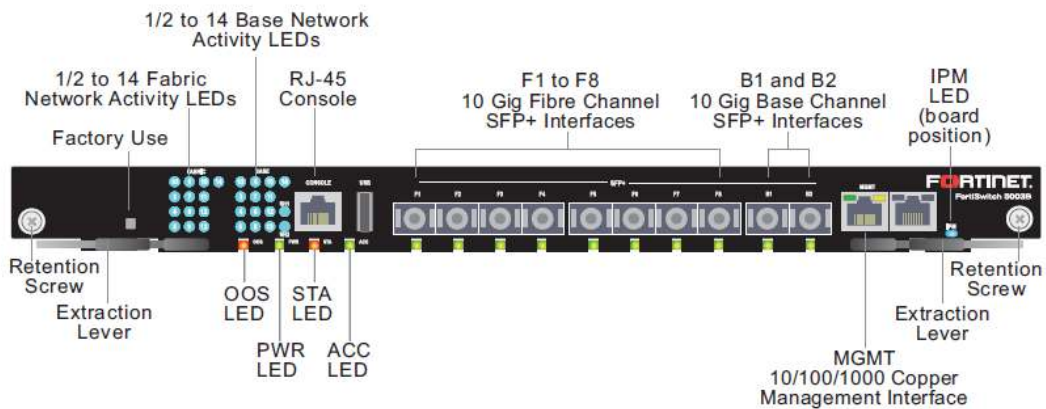
Each FortiGate contains a set of base interfaces. Base 1 connects to the FortiSwitch in slot-1 and base 2 connects to the FortiSwitch in slot-2 as depicted on page 9. Each FortiSwitch also contains a set of interfaces named B1 and B2. Do not be confused by the naming scheme on the FortiSwitch. Both B1 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



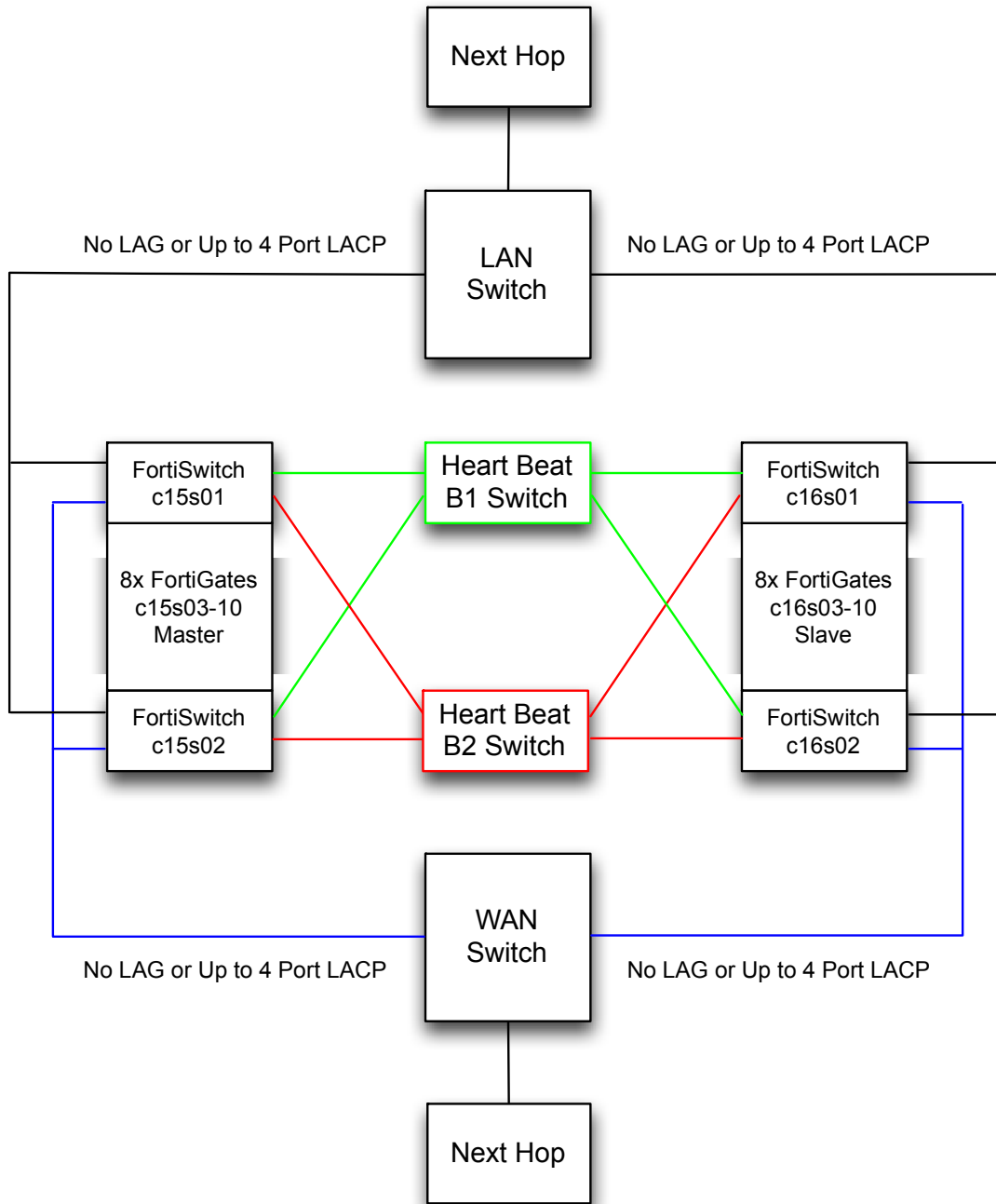
FS5003B External Interfaces

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.

Figure 3-1-6



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 active-passive 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.
- Health 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 non-management 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.

Traffic Load Balancing

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 its 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.

Figure 3-1-7

The screenshot shows the FortiSwitch 5003B web interface. The 'Traffic Monitor' tab is active, displaying the 'Service Group #1 Traffic Calculator' and a 'Group Membership' table.

Service Group #1 Traffic Calculator

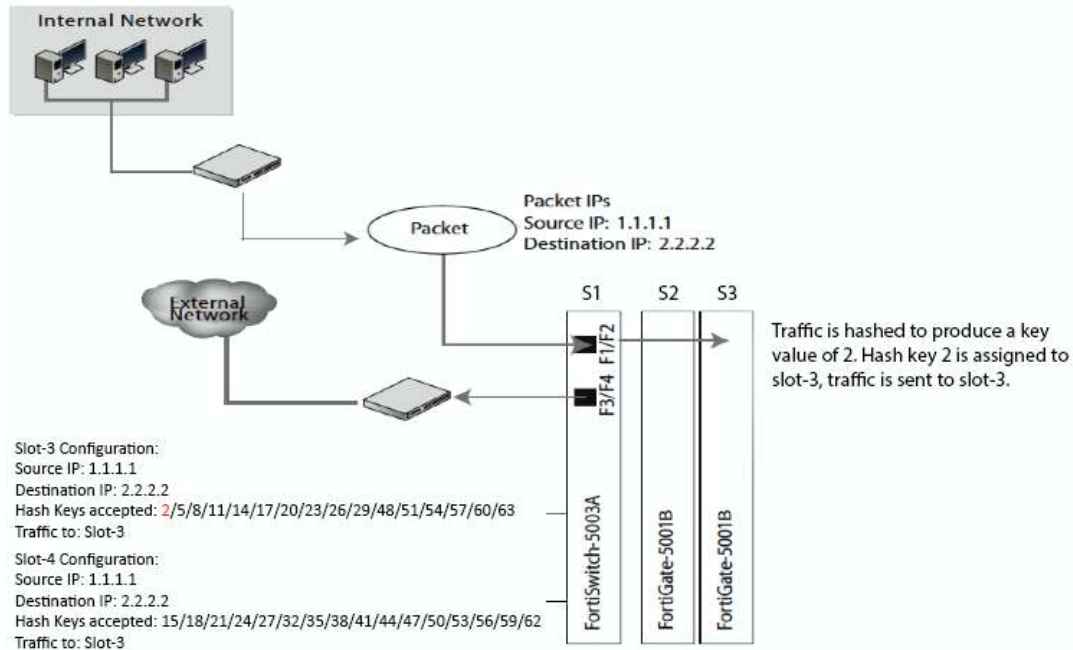
Load Balancing Algorithm: Hash IP Least 6-Bits
Direction: Internal (F1/F2) -> External (F3/F4)
Src IP: 1.1.1.1
Dst IP: 2.2.2.2
Apply

Hash Key: 2
Traffic To: Slot #3

Group Membership

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	🟢
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	🟢
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	🟢
Slot #6	Active	5	0/1/3/4/6/7/9/10/12/13/30/33/36/39/42/45	304,773,190	2,007,166,526	🟢

Figure 3-1-8



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 FortiSwitch.

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

```
c15s01 # diagnose switch fabric-channel pfm-load-balance list
Entry[0]: input-interface:internal-1(0) hash-on:destination
calendar(len 64)[5 5 2 5 5 2 5 5 2 5 5 2 5 5 2 3
4 2 3 4 2 3 4 2 3 4 2 3 4 2 5 4
3 5 4 3 5 4 3 5 4 3 5 4 3 5 4 3
2 4 3 2 4 3 2 4 3 2 4 3 2 4 3 2]
Calendar Legend: 2=slot-3, 3=slot-4
4=slot-5, 5=slot-6

Entry[1]: input-interface:external-1(1) hash-on:source
calendar(len 64)[5 5 2 5 5 2 5 5 2 5 5 2 5 5 2 3
4 2 3 4 2 3 4 2 3 4 2 3 4 2 5 4
3 5 4 3 5 4 3 5 4 3 5 4 3 5 4 3
2 4 3 2 4 3 2 4 3 2 4 3 2 4 3 2]
Calendar Legend: 2=slot-3, 3=slot-4
4=slot-5, 5=slot-6
```

When a slot fails such as slot-6, only its calendar entry is remapped to existing 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.

```

c15s01 # diagnose switch fabric-channel fm-load-balance list
Entry[0]: input-interface:internal-1(0) hash-on:destination
calendar(len 64)[3 2 2 3 2 2 3 2 2 3 2 2 2 2 2 3
4 2 3 4 2 3 4 2 3 4 2 3 4 2 4 4
3 4 4 3 4 4 3 4 4 3 4 4 3 3 4 3
2 4 3 2 4 3 2 4 3 2 4 3 2 4 3 2]
Calendar Legend: 2=slot-3, 3=slot-4
4=slot-5,
Entry[1]: input-interface:external-1(1) hash-on:source
calendar(len 64)[3 2 2 3 2 2 3 2 2 3 2 2 2 2 2 3
4 2 3 4 2 3 4 2 3 4 2 3 4 2 4 4
3 4 4 3 4 4 3 4 4 3 4 4 3 3 4 3
2 4 3 2 4 3 2 4 3 2 4 3 2 4 3 2]
Calendar Legend: 2=slot-3, 3=slot-4
4=slot-5,

```

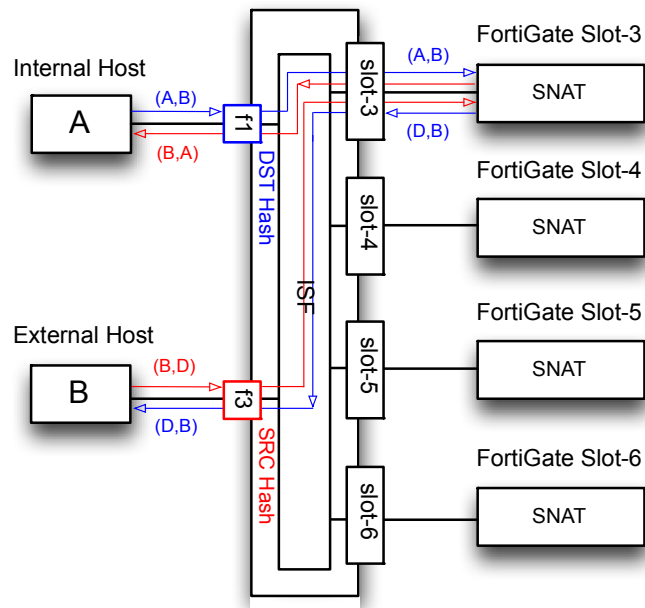
Understanding NAT & Load Balancing

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.

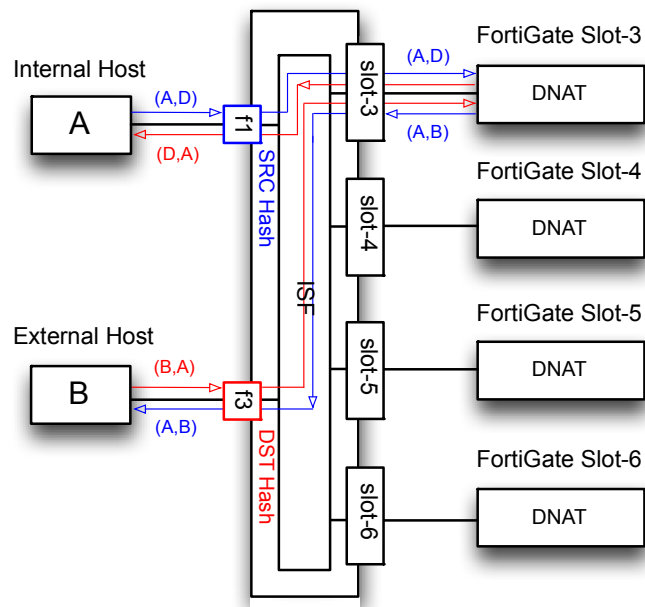
- SNAT is used when the FortiGate translates all internal source traffic to a different IP address. With this mode the FortiSwitch will hash based upon the destination IP address on the internal interface and source IP address on the external interface.

Figure 3-1-9 SNAT, Single LAG Port Shown on FS Per Direction
FS5003B



- 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
FS5003B

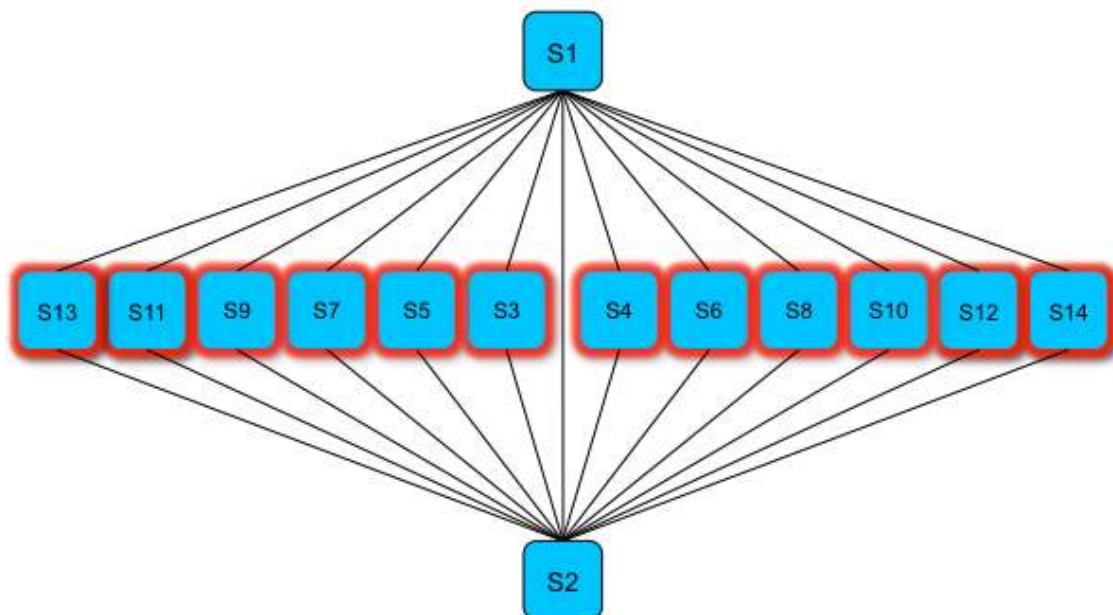


- NONAT is used when translations do not occur on either side.

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.

Figure 3-1-11



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

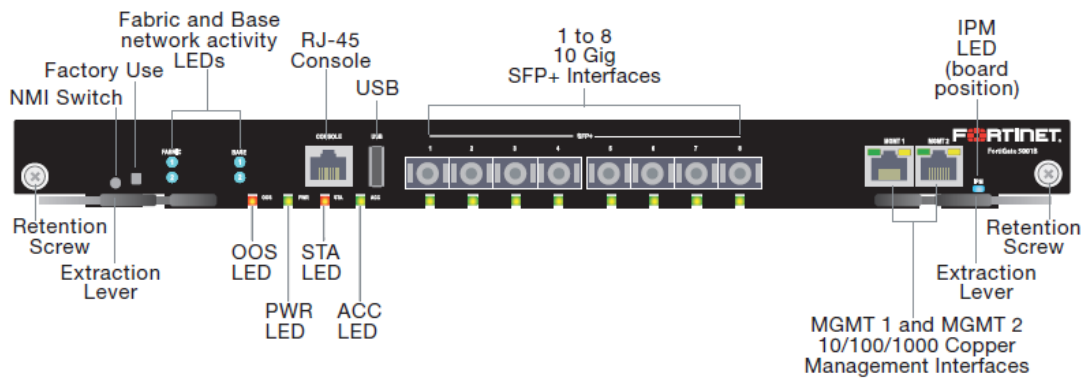
The 5000 Series FortiGates can be installed into a FG5140B or FG5060 chassis. Some older chassis versions are also supported.

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

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

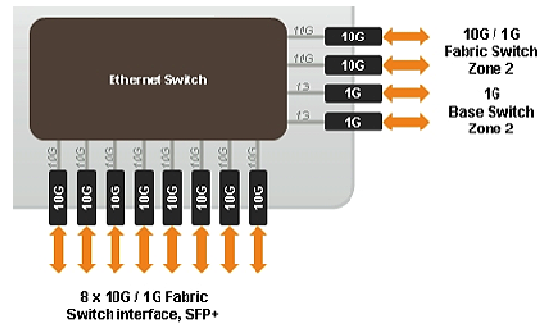
FG5001B External Interfaces

Figure 3-2-1



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.

Master FortiSwitch Chassis 15 Slot 1 Configuration Example

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/eVNgL2jOJcYbGoB3P1UAvrnOZ4u1sr4VEejirW3XRDHif1f40
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
7vXgU5glGwe4iT9Lor/eVNGL2jOJcYbGoB3P1UAvrnOZ4u1sr4VEejirW3XRDHIf1f40
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
7vXgU5glGwe4iT9Lor/eVNgl2jNlNk+fOzMa7WJry7nTqhz9AI8B0iR8bH/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
7vXgU5glGwe4iT9Lor/eVNgl2jNlNk+fOzMa7WJry7nTqhz9AI8B0iR8bH/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

```

FortiSwitch Installation

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 5th octet of the mac address by one. For example service group 2's MAC address would be 00:09:0f:43:9e: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.

FortiSwitch HA Synchronization

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
```

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 fswbfd 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 ffff 0009 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 than 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
```

Understanding Service Groups

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 5-3-1 Basic

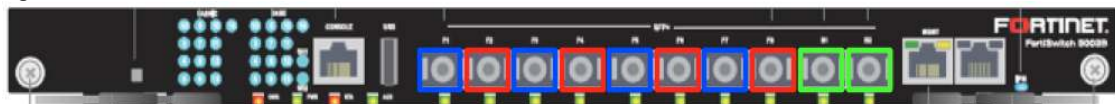


Figure 5-3-2 Two-Port LAG

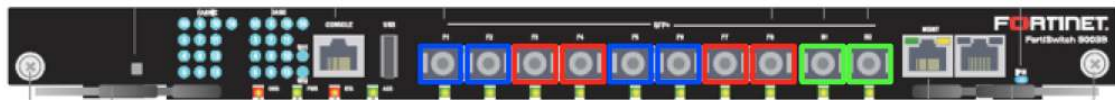
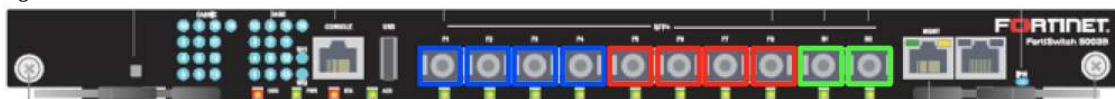


Figure 5-3-3 Four-Port LAG



- 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

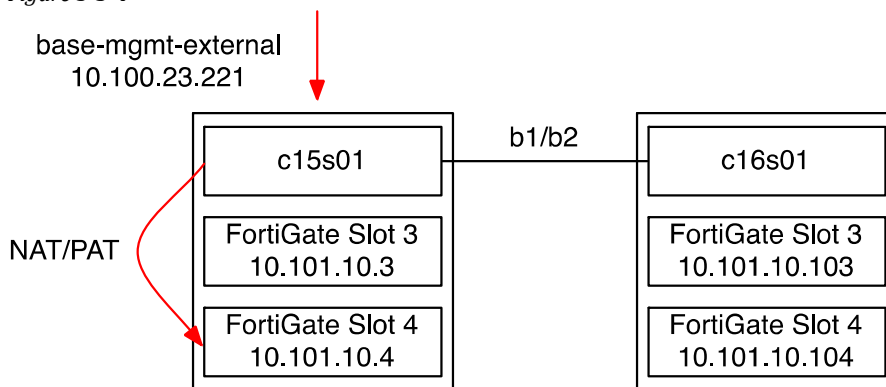
Scenario A			
c15s01b1	u	c16s01b1	u
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	YES		
Scenario B			
c15s01b1	d	c16s01b1	u
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	YES		
Scenario C			
c15s01b1	u	c16s01b1	u
c15s01b2	d	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	YES		
Scenario D			
c15s01b1	u	c16s01b1	d
c15s01b2	u	c16s01b2	u
c15s02b1	u	c16s02b1	u
c15s02b2	u	c16s02b2	u
Conf Sync	YES		
Scenario E			
c15s01b1	u	c16s01b1	d
c15s01b2	u	c16s01b2	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.

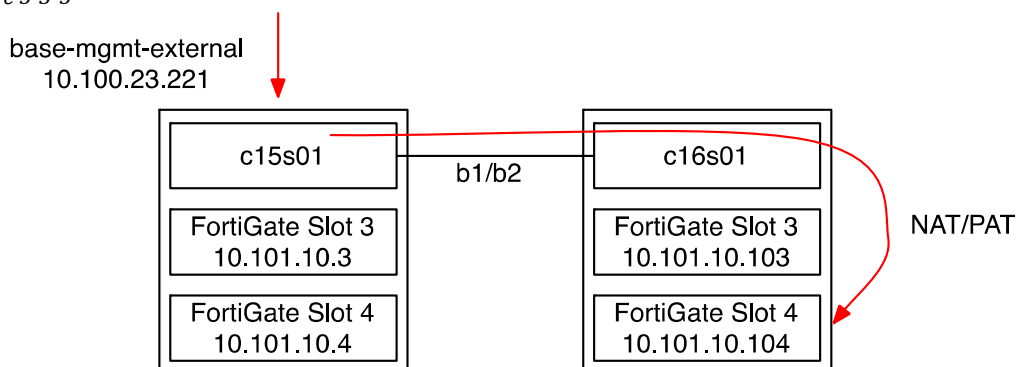
The diagram below depicts a management connection to slot-4 using IP address 10.101.23.221 via HTTP port 8004. The connection is PAT to 10.101.10.4 to access slot-4.

Figure 5-3-4



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.

Figure 5-3-5



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
```

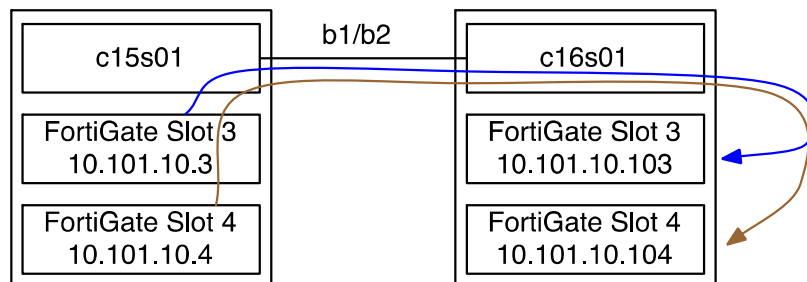
If a response does not occur, verify the FS and external switch VLAN configuration.

- 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.

Figure 5-3-6



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 Service Group Slots

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: Management: 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: Management: 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 inter-chassis 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: Management: Good Data: Failed
Status Message:"Waiting for data heartbeat."

- In the FortiGate that is showing “Waiting for data heartbeat,” 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 following 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
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 its locked position. Push the lever in towards the board. Please refer to the hardware installation guide found at <http://kb.fortinet.com> 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 (chlb) process is used to synchronize with the ELBC Master. Once chlb 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
  0 ff:ff:ff:ff:ff:ff N/A
  1 ff:ff:ff:ff:ff:ff N/A
  2 ff:ff:ff:ff:ff:ff N/A
  3 00:09:0f:ff:44:75 FG-5KB3E11700407 ←MAC of Base1 MGMT
  4 00:09:0f:43:96:39 FG-5KB3E11700636
  5 00:09:0f:ff:44:cd FG-5KB3E11700411
  6 00:09:0f:4d:97:42 FG-5KB3E12700041
  7 ff:ff:ff:ff:ff:ff N/A
  8 ff:ff:ff:ff:ff:ff N/A
  9 ff:ff:ff:ff:ff:ff N/A
  10 ff:ff:ff:ff:ff:ff N/A
  11 ff:ff:ff:ff:ff:ff ,m-N/A
  12 ff:ff:ff:ff:ff:ff N/A
  13 ff:ff:ff:ff:ff:ff N/A
  14 ff:ff:ff:ff:ff:ff N/A
  15 ff: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
  Slot Swdev MAC Serial-Number
  0 ff:ff:ff:ff:ff:ff N/A
  1 ff:ff:ff:ff:ff:ff N/A
  2 ff:ff:ff:ff:ff:ff N/A
  3 00:09:0f:ff:44:75 FG-5KB3E11700407
  4 00:09:0f:43:96:39 FG-5KB3E11700636
  5 00:09:0f:ff:44:cd FG-5KB3E11700411
  6 00:09:0f:4d:97:42 FG-5KB3E12700041
  7 ff:ff:ff:ff:ff:ff N/A
  8 ff:ff:ff:ff:ff:ff N/A
  9 ff:ff:ff:ff:ff:ff N/A
  10 ff:ff:ff:ff:ff:ff N/A
  11 ff:ff:ff:ff:ff:ff N/A
  12 ff:ff:ff:ff:ff:ff N/A
  13 ff:ff:ff:ff:ff:ff N/A
  14 ff:ff:ff:ff:ff:ff N/A
  15 ff: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
```

- 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
```


Troubleshooting FortiGate Joins

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
```

Reducing Single Core CPU Usage

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 <http://support.fortinet.com>.

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 FortiSwitch'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

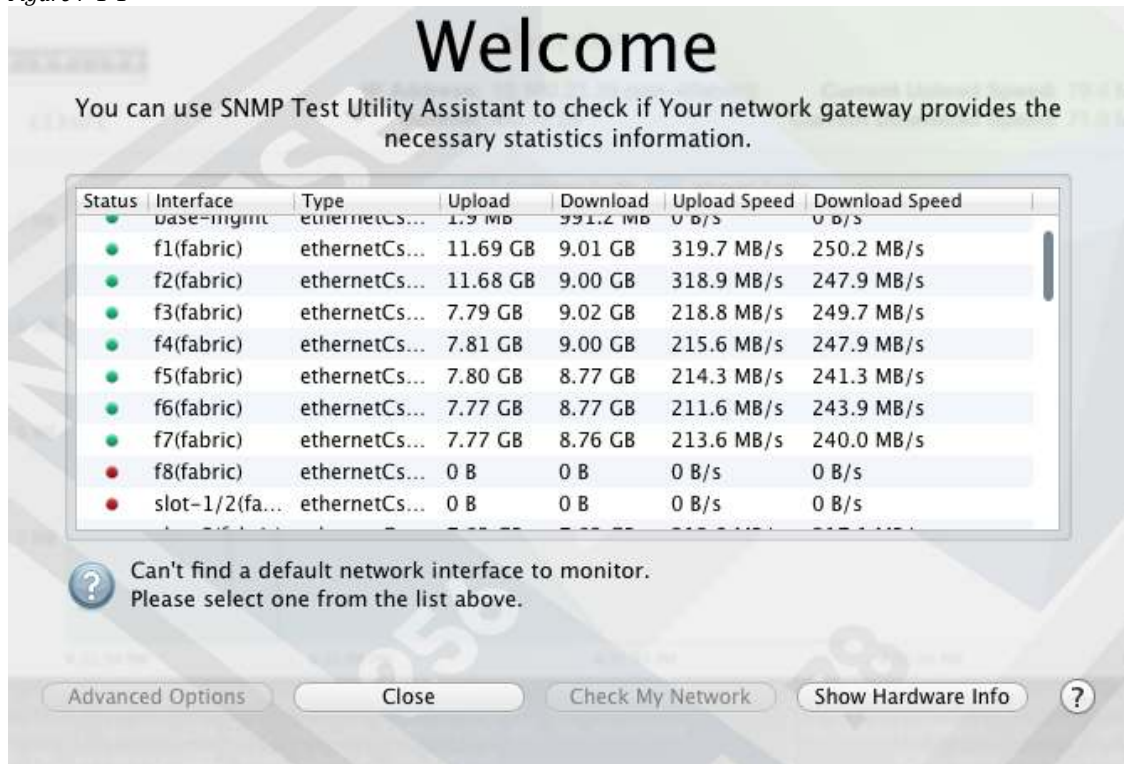
```
snmpwalk -v 2c -c fortinet 10.100.23.222:16101 .1.3.6.1.4.1.12356.106.14.2.1.1.12
```

SNMP Interface Statistics

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.

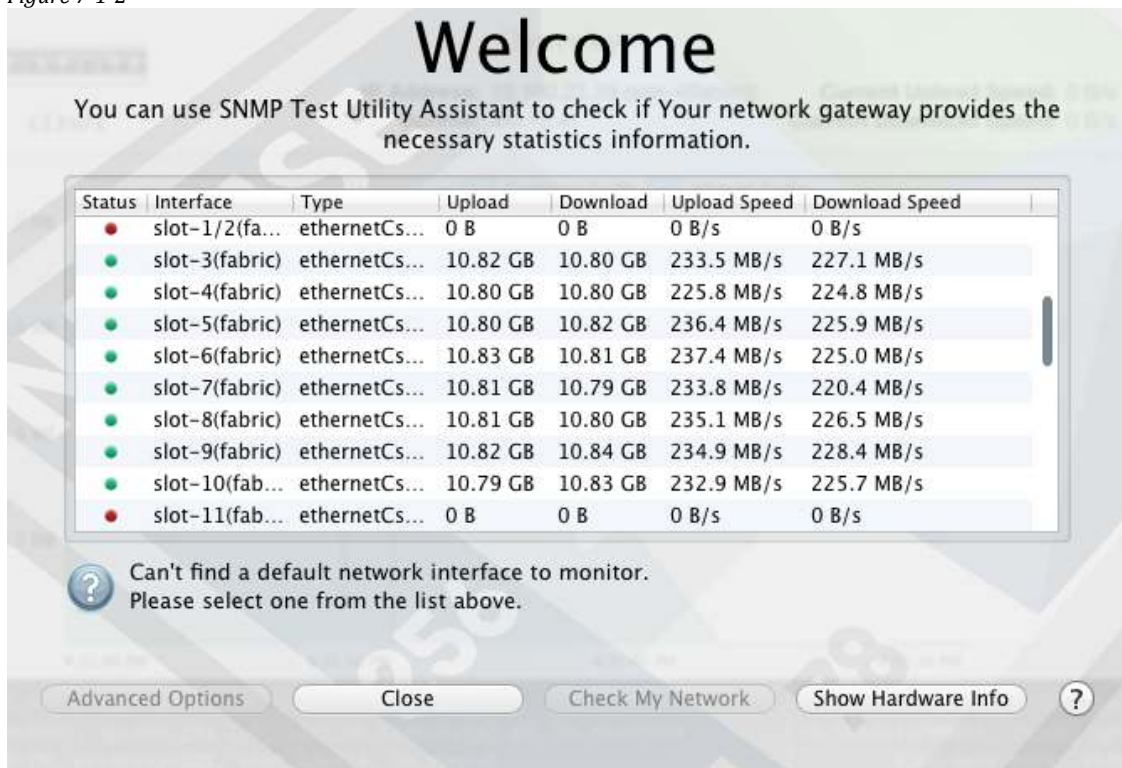
Traffic distribution is shown for the front ports of the master FS5003B. F1 and F2 is receiving more traffic than F3-F7 as expected with an uneven number of ports. Overall the distribution of traffic is under maximum capacity and flowing nicely.

Figure 7-1-1



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

Figure 7-1-2



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 be 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 <http://docs.fortinet.com>.

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.

Figure 8-1-1

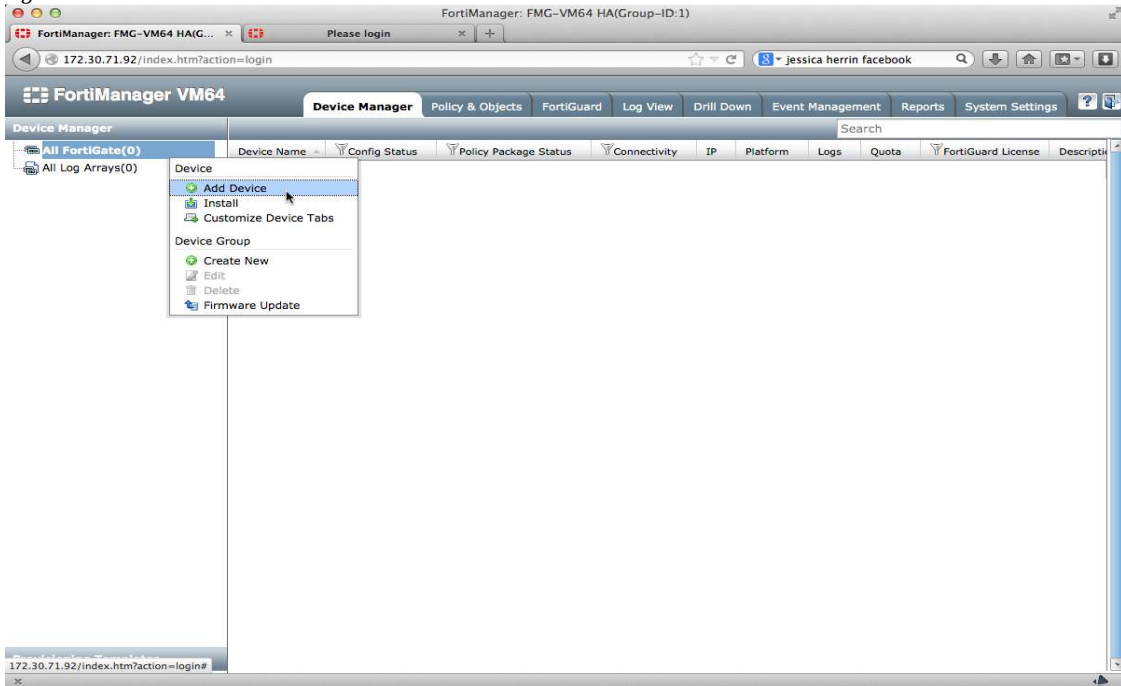


Figure 8-1-2

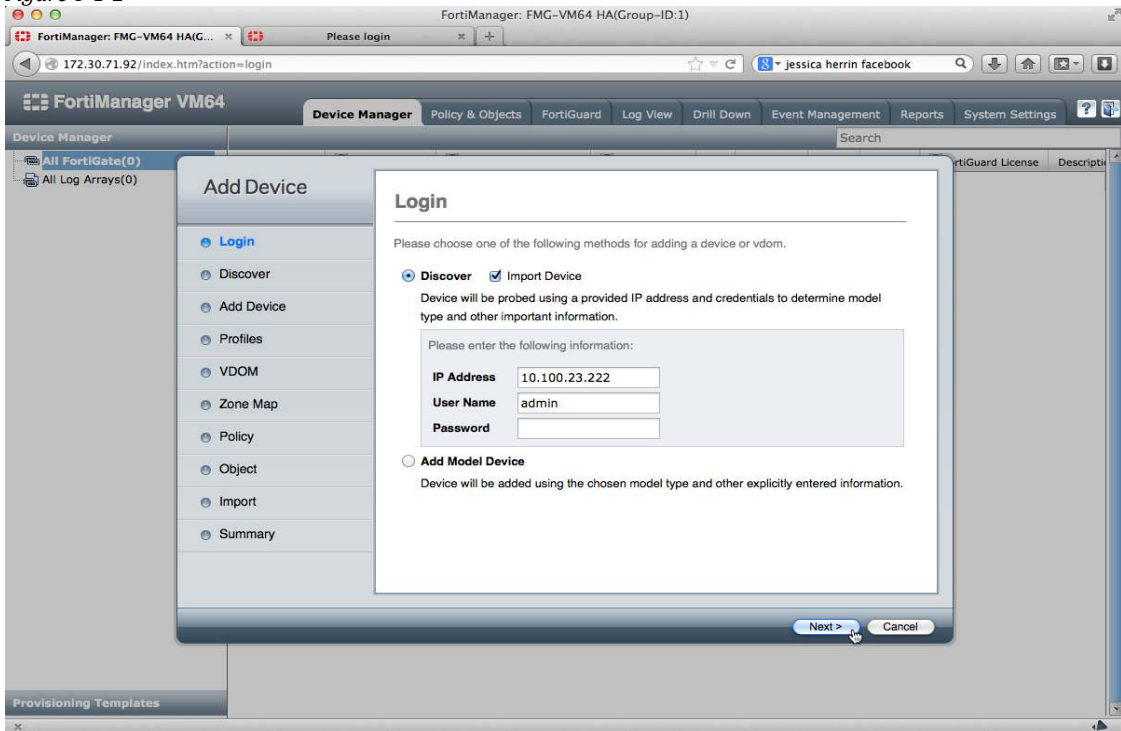


Figure 8-1-3

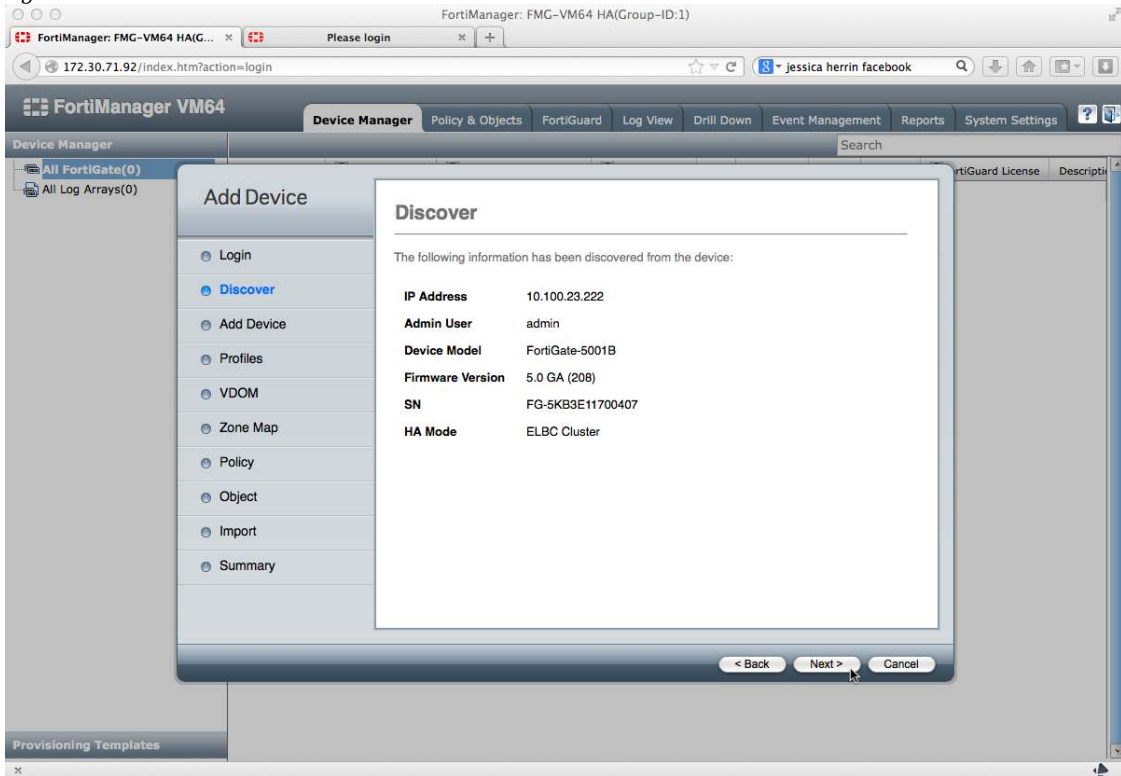


Figure 8-1-4

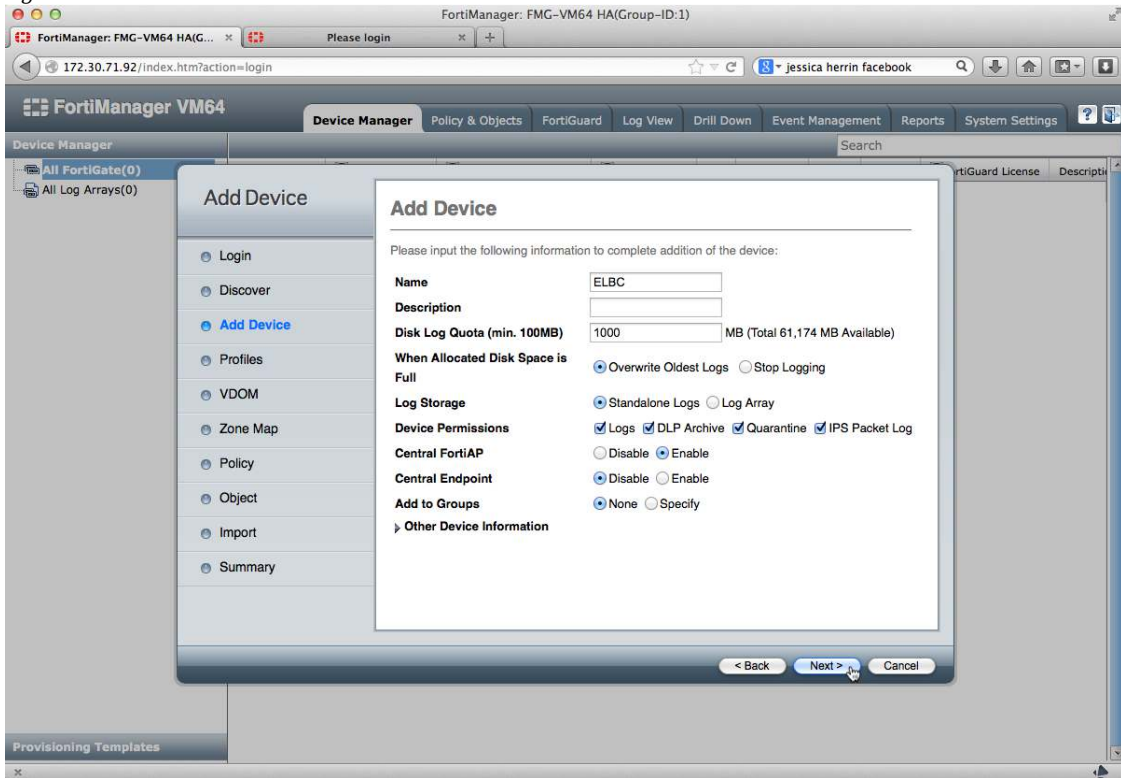


Figure 8-1-5

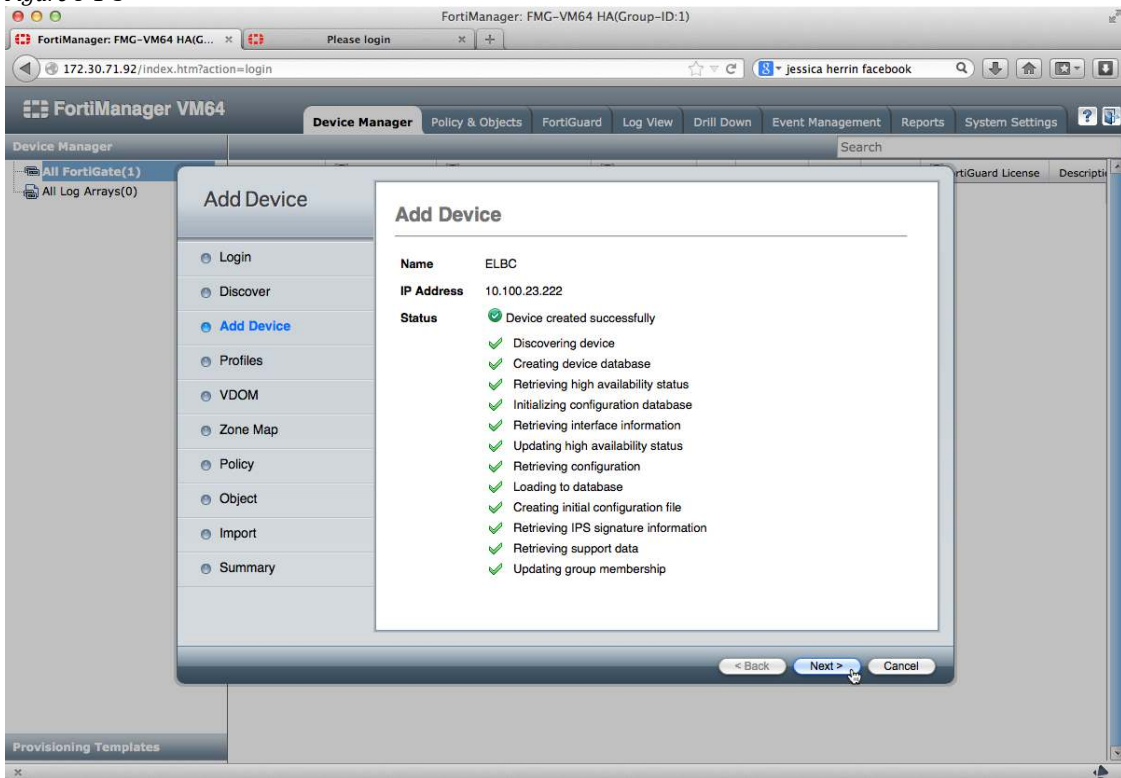


Figure 8-1-6

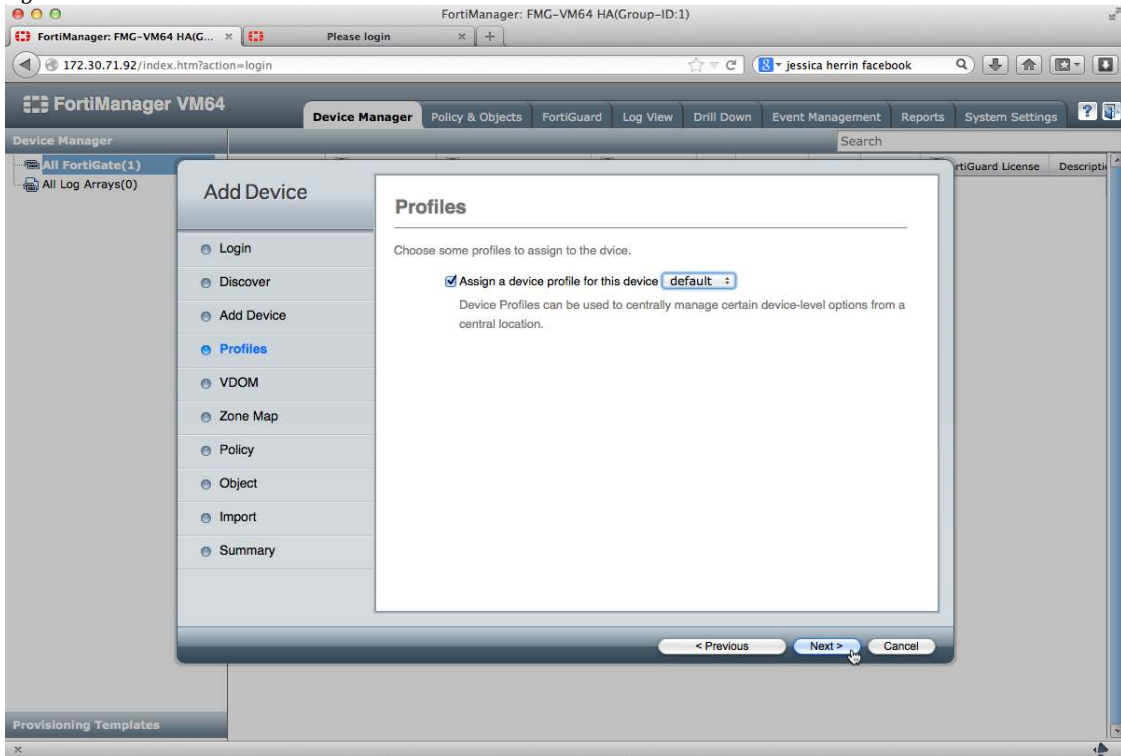


Figure 8-1-7

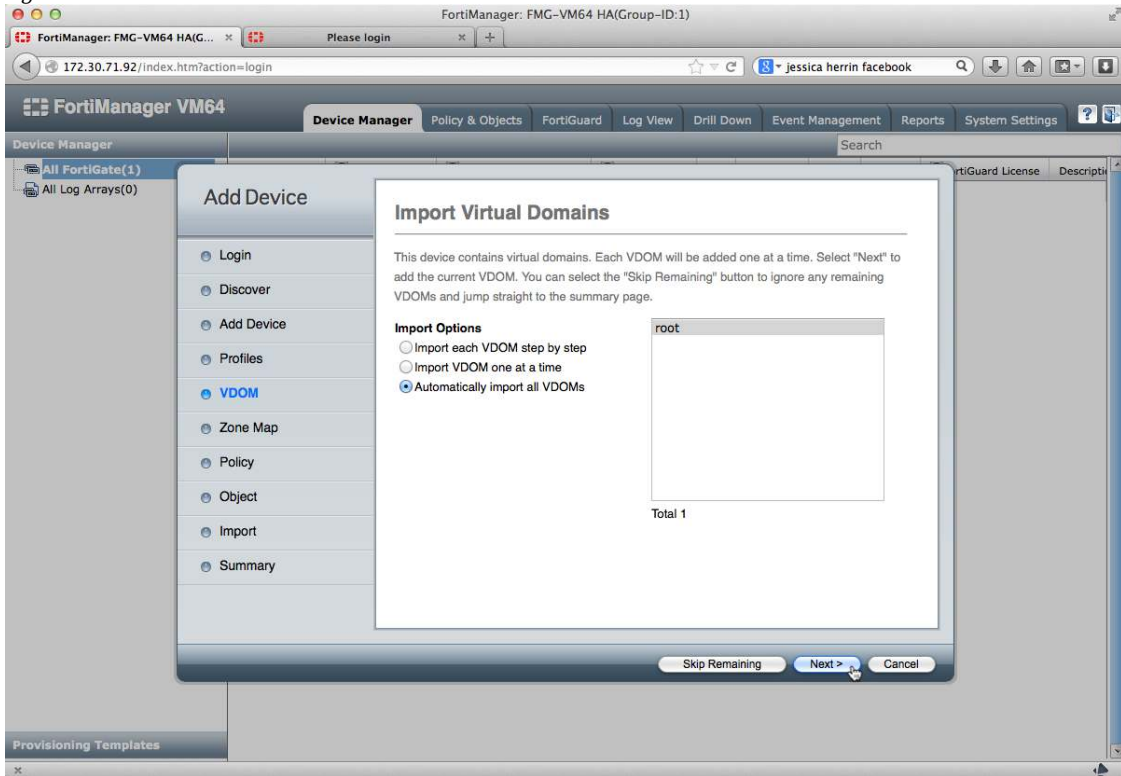


Figure 8-1-8

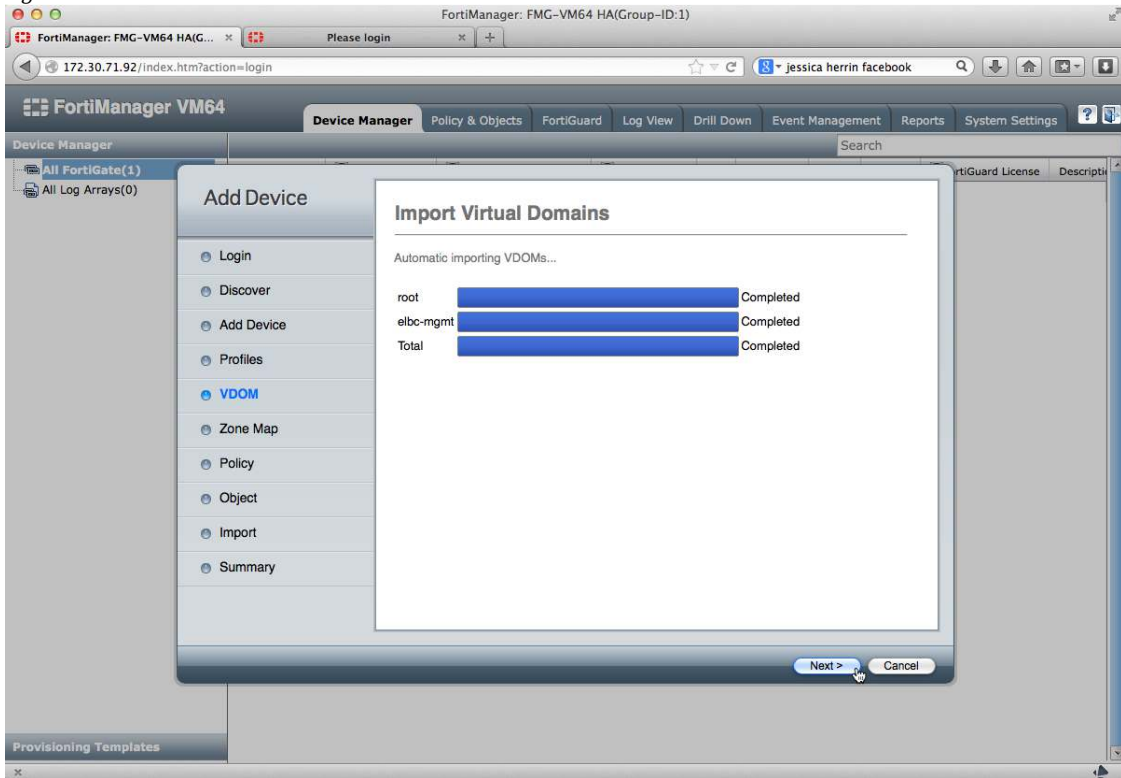
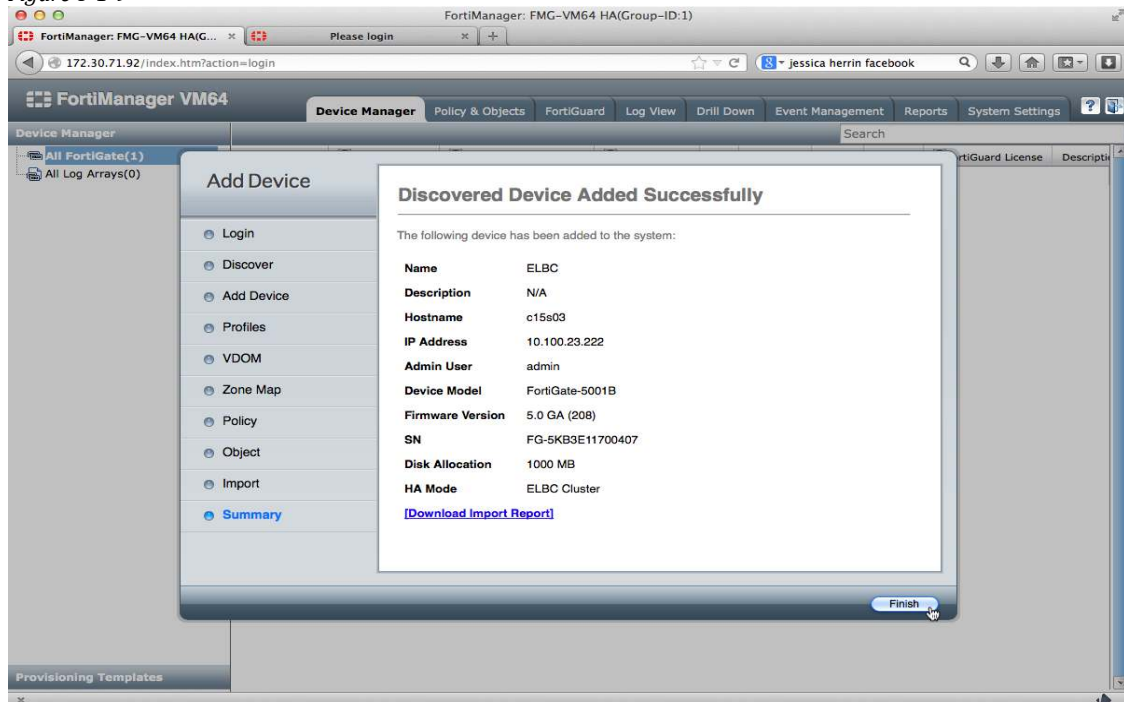
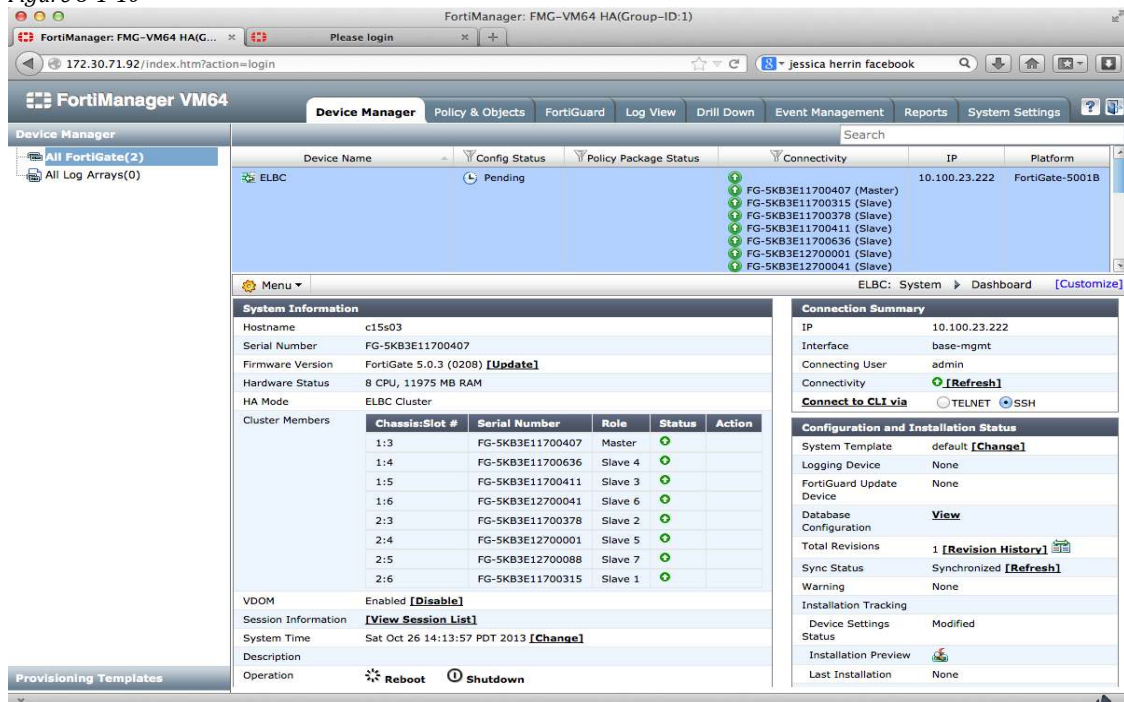


Figure 8-1-9



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.

Figure 8-1-10



Associating FortiGate Interfaces with Zones

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

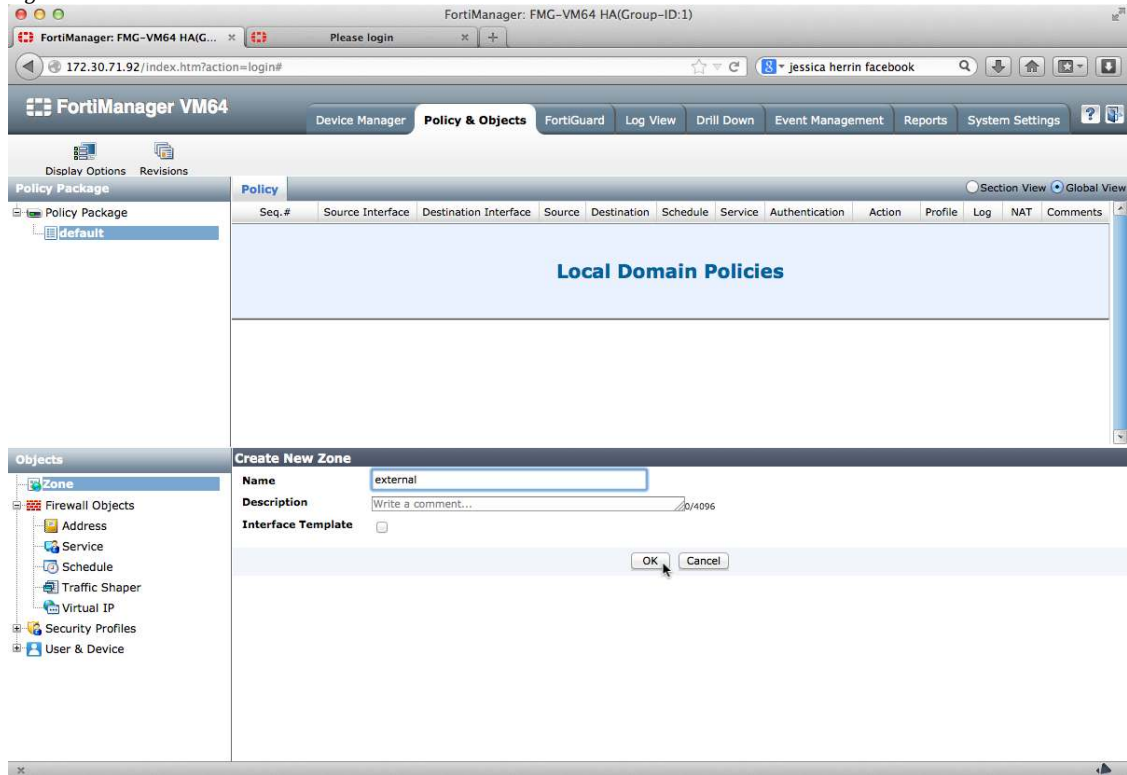


Figure 8-1-12

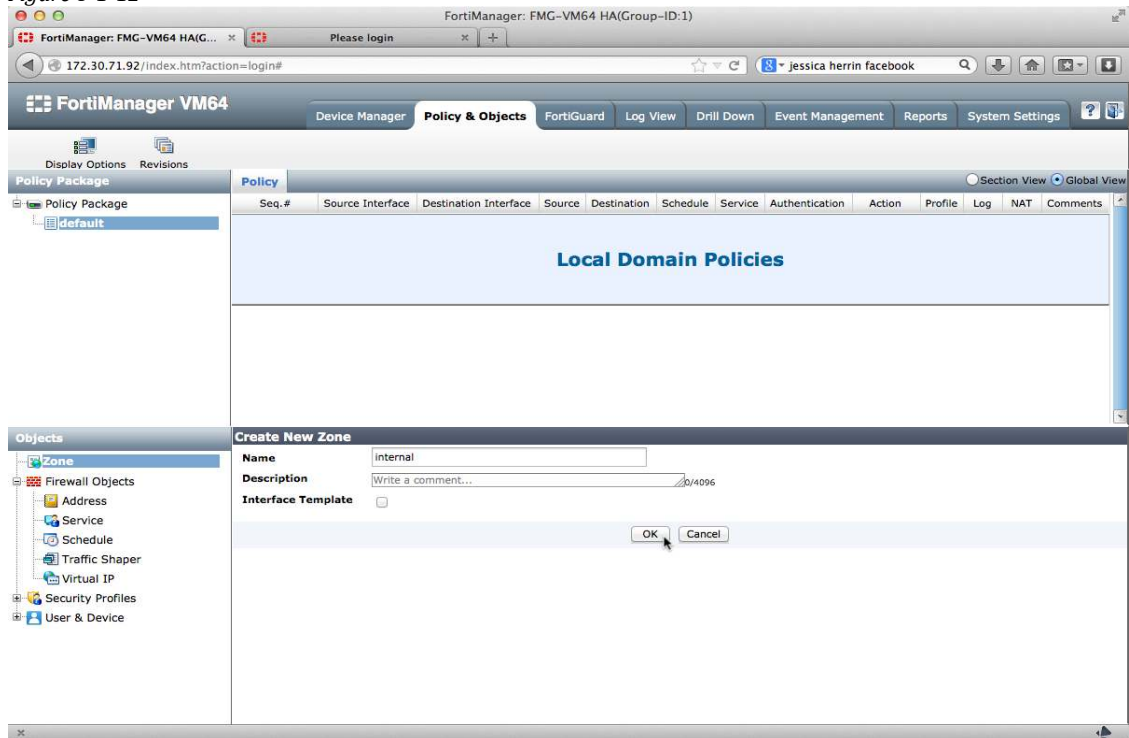
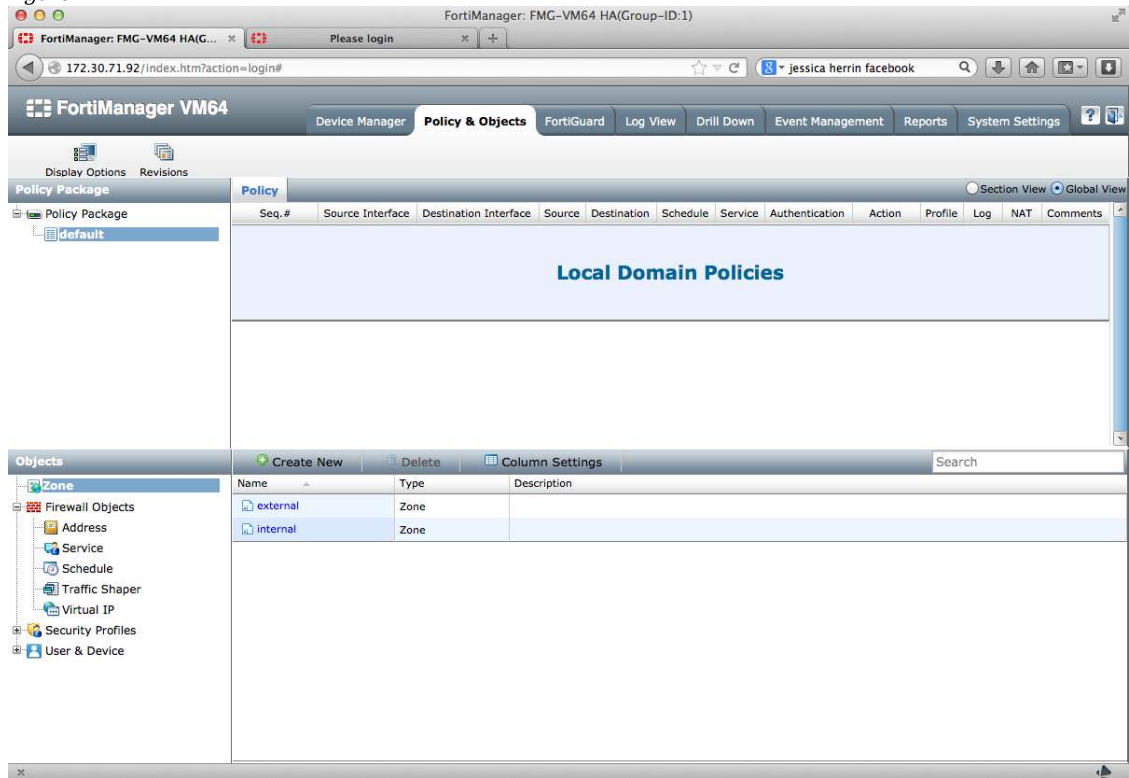


Figure 8-1-13



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

Figure 8-1-14

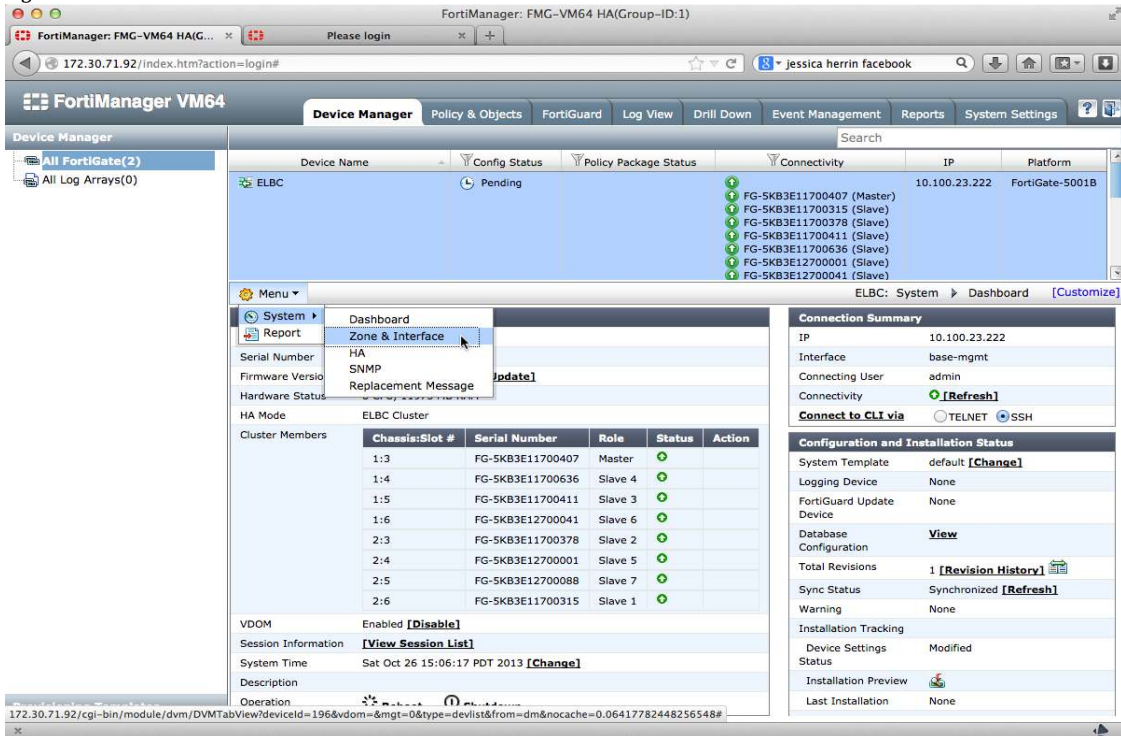


Figure 8-1-15

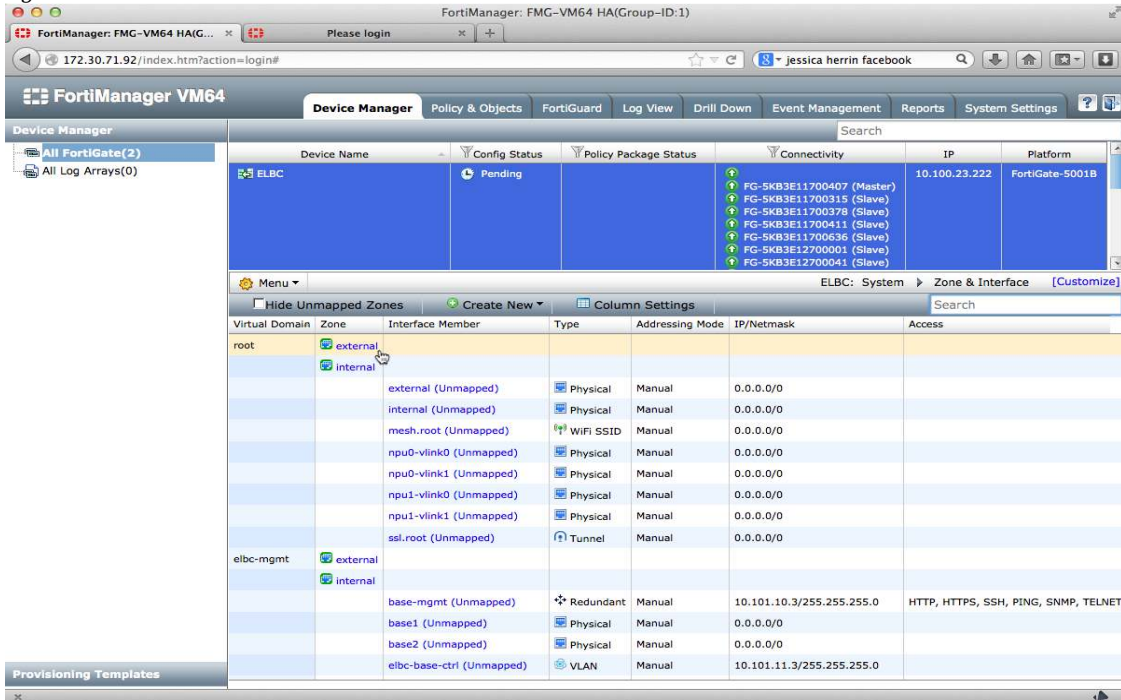


Figure 8-1-18

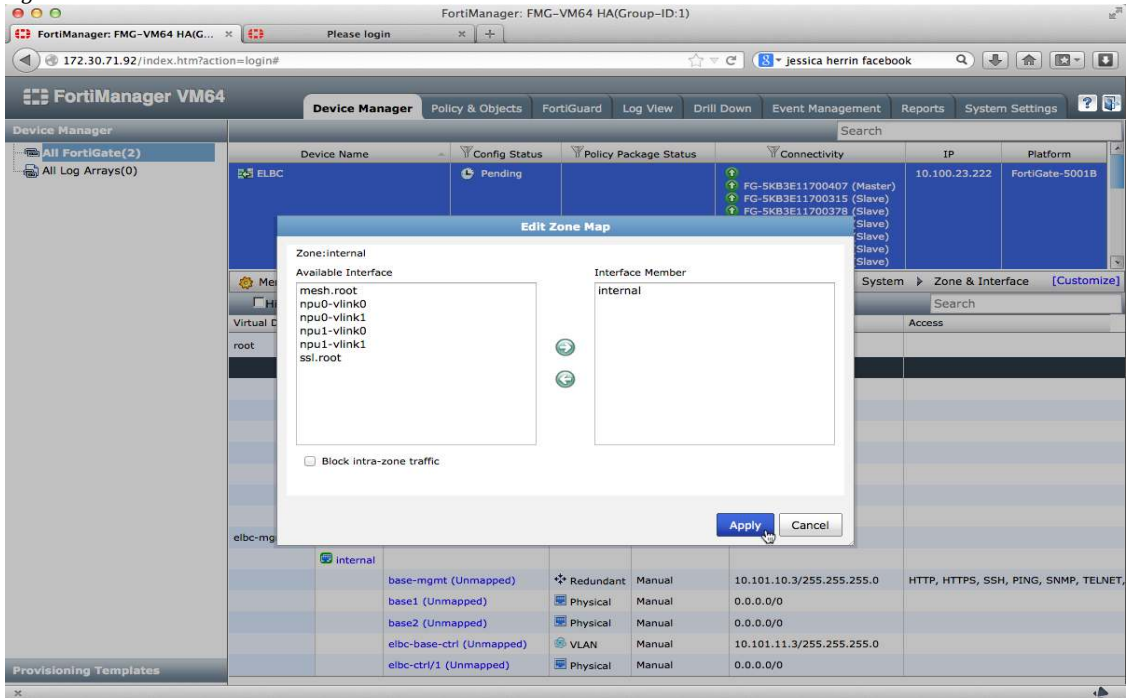
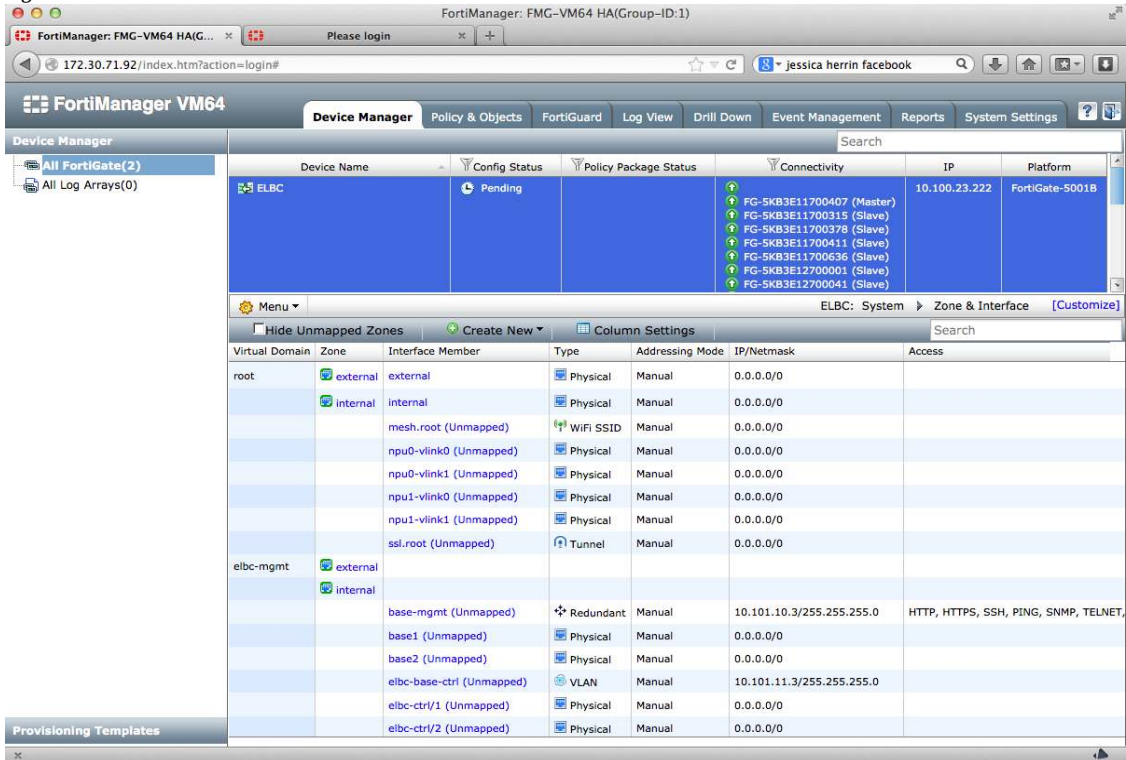


Figure 8-1-19



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

Figure 8-1-20

The screenshot shows the FortiManager VM64 interface. The top navigation bar includes 'Device Manager', 'Policy & Objects', 'FortiGuard', 'Log View', 'Drill Down', 'Event Management', 'Reports', and 'System Settings'. The left sidebar shows 'All FortiGate(2)' and 'All Log Arrays(0)'. The main content area displays the configuration for device 'ELBC', which is in a 'Pending' state. Below this, a table shows the configuration for the 'root' virtual domain, including interface members and their properties.

Virtual Domain	Zone	Interface Member	Type	Addressing Mode	IP/Netmask	Access
root	external	external	Physical	Manual	1.0.0.1/255.255.255.0	PING
	internal	internal	Physical	Manual	2.0.0.1/255.255.255.0	PING
		mesh.root (Unmapped)	WiFi SSID	Manual	0.0.0.0/0	
		npu0-vlink0 (Unmapped)	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 (Unmapped)	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, SSH, PING, SNMP, TELNET,
		base1 (Unmapped)	Physical	Manual	0.0.0.0/0	
		base2 (Unmapped)	Physical	Manual	0.0.0.0/0	
		elbc-base-ctrl (Unmapped)	VLAN	Manual	10.101.11.3/255.255.255.0	
	elbc-ctrl/1 (Unmapped)	Physical	Manual	0.0.0.0/0		
	elbc-ctrl/2 (Unmapped)	Physical	Manual	0.0.0.0/0		

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

Adding Policy Package

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.

Figure 8-1-21

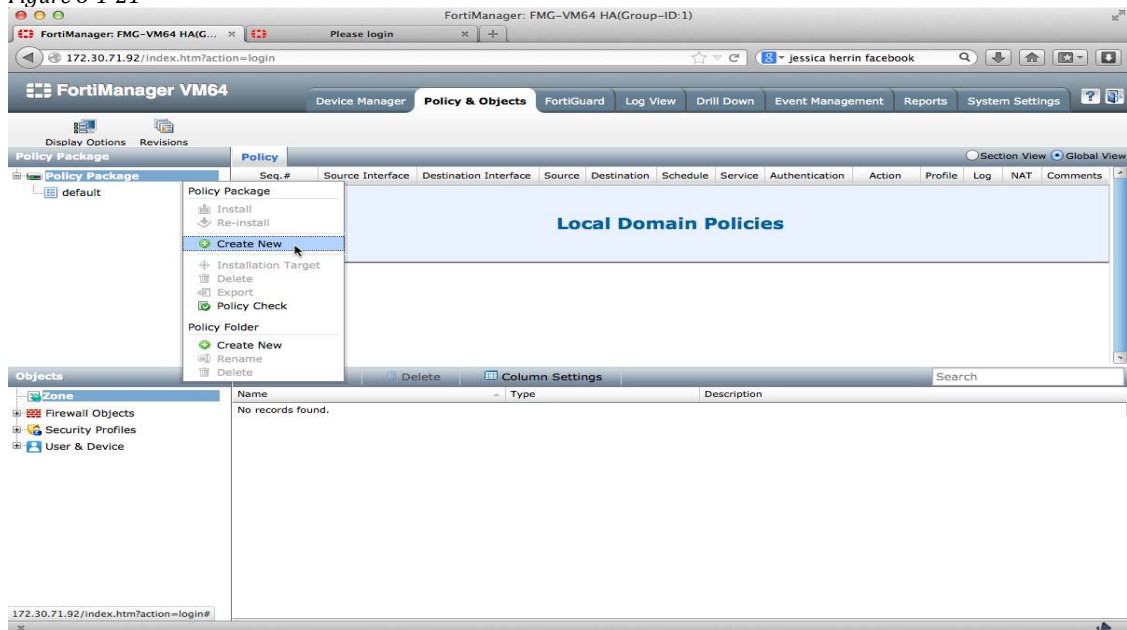


Figure 8-1-22

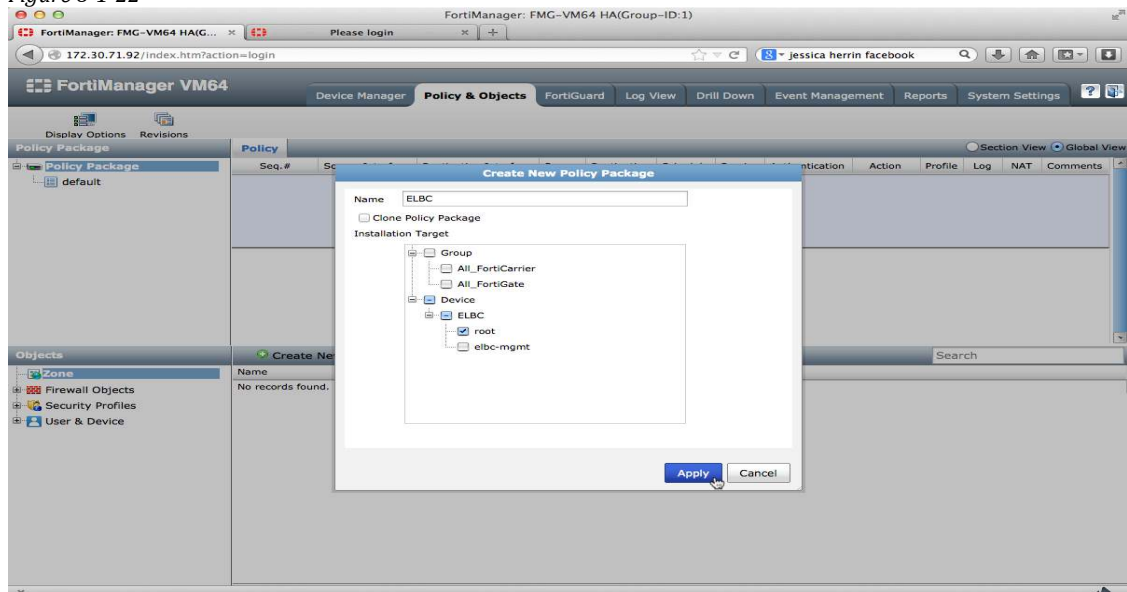


Figure 8-1-23

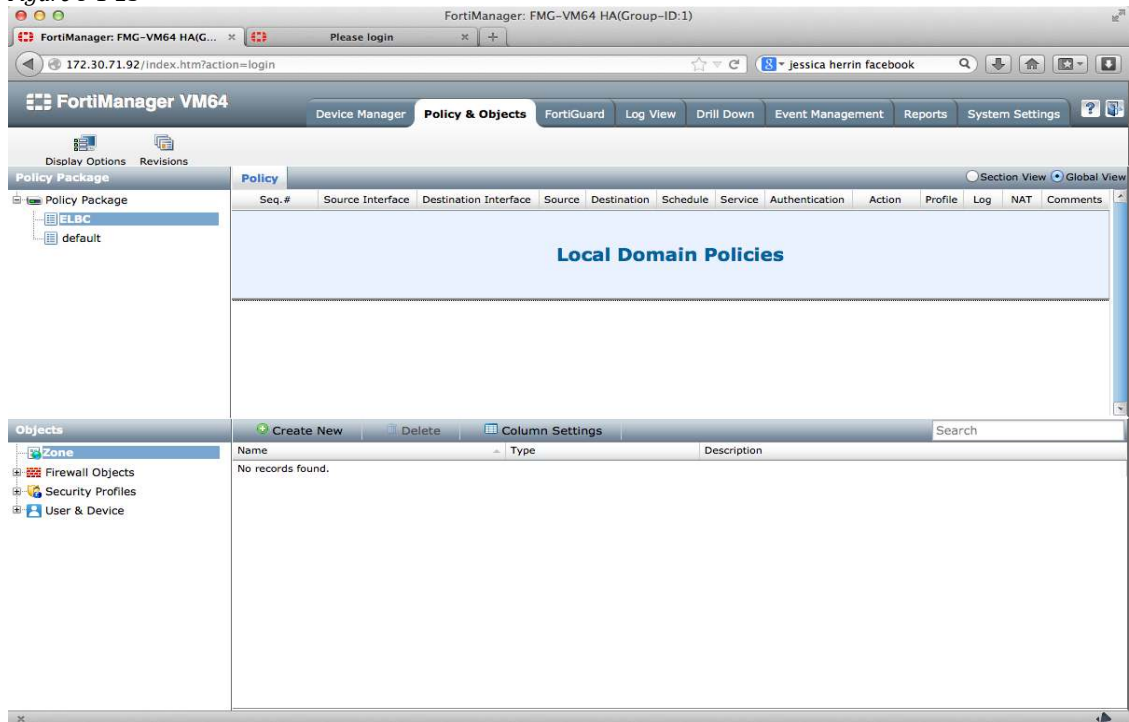
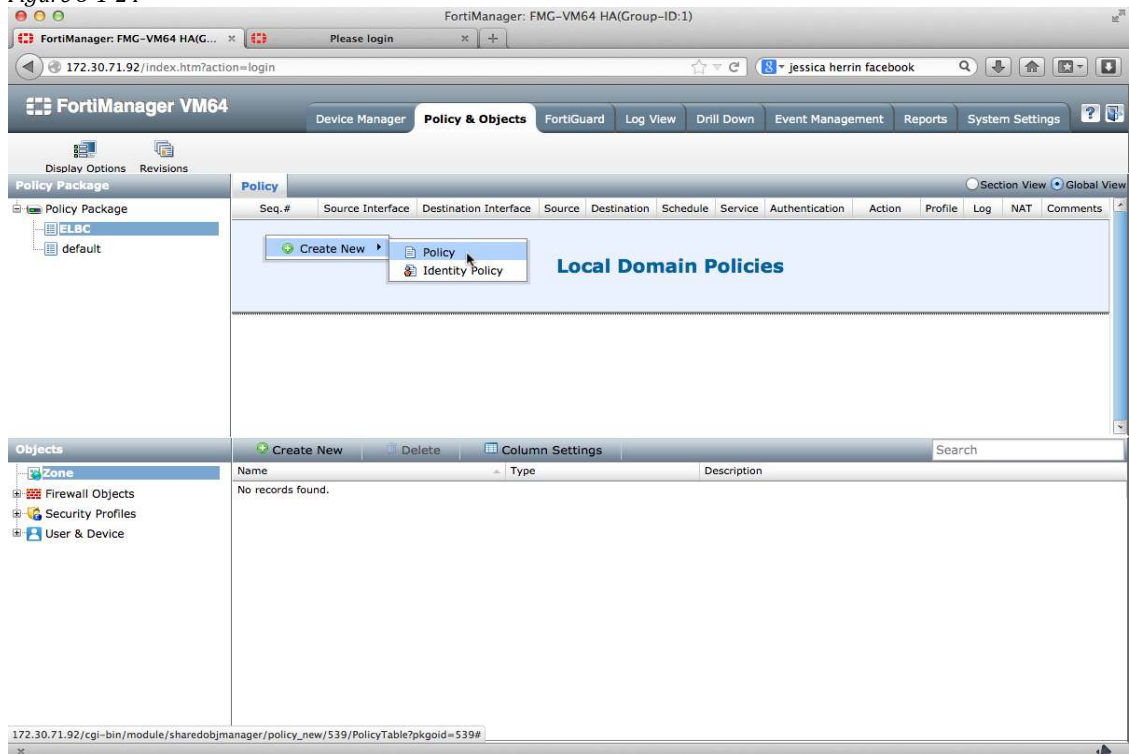


Figure 8-1-24



Add firewall policies to the ELBC Policy Package.

Figure 8-1-25

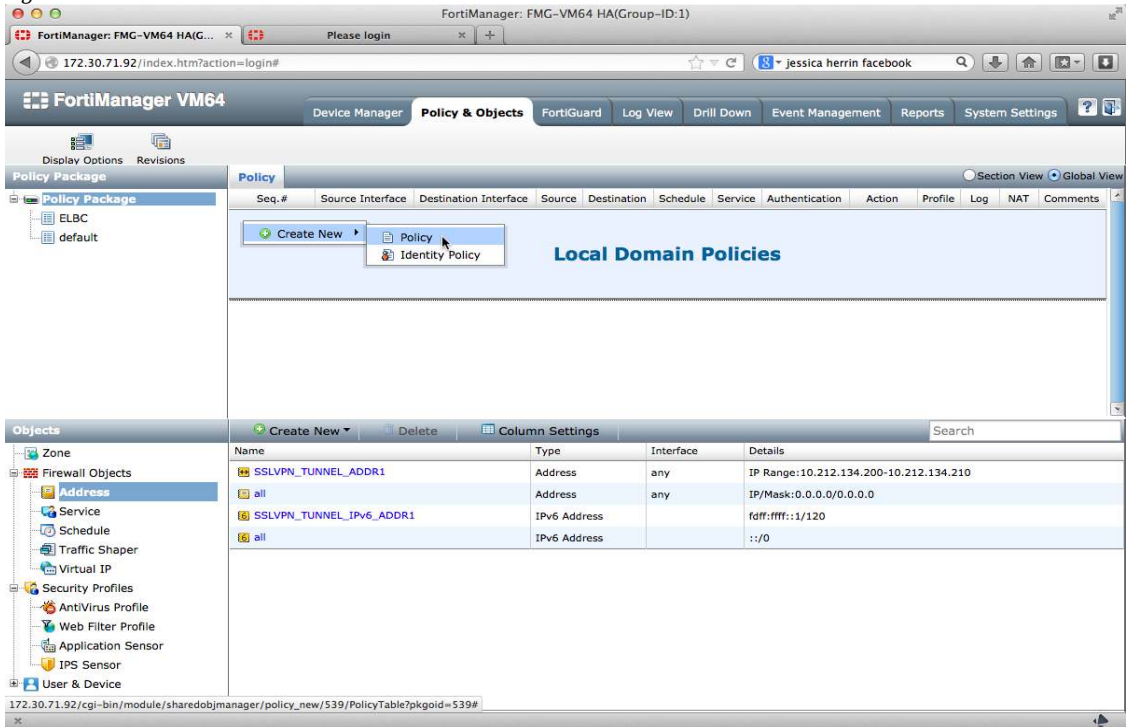


Figure 8-1-26

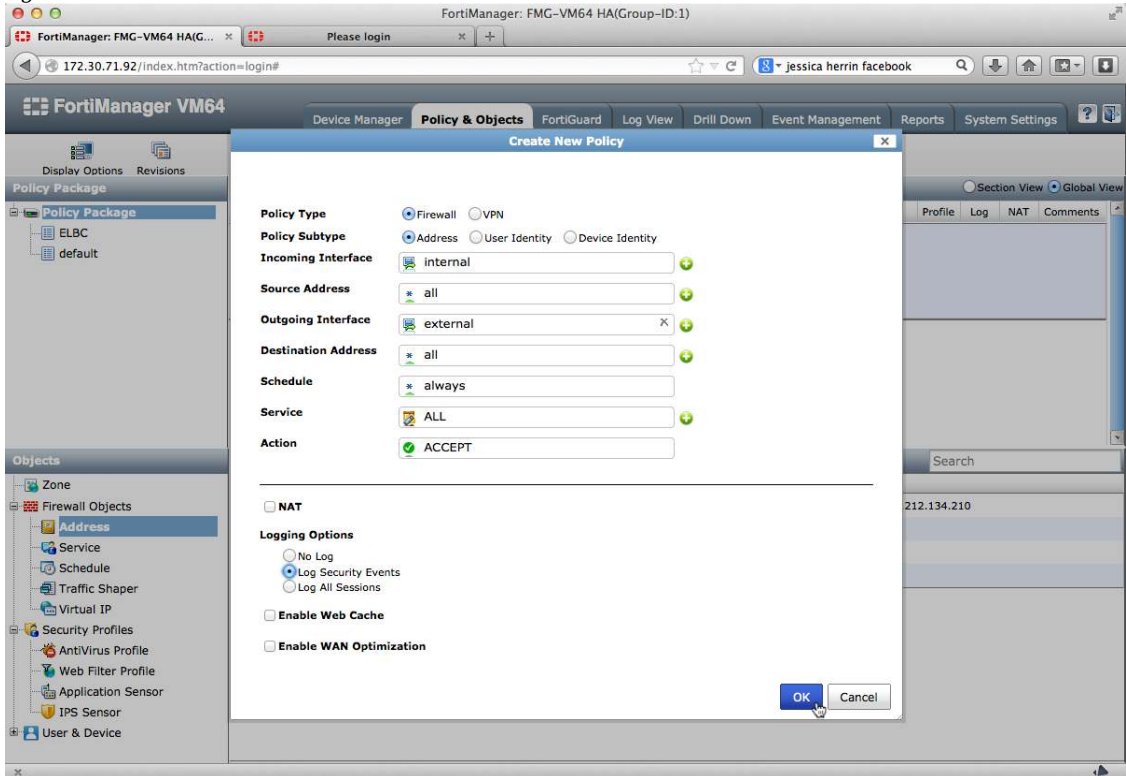


Figure 8-1-27

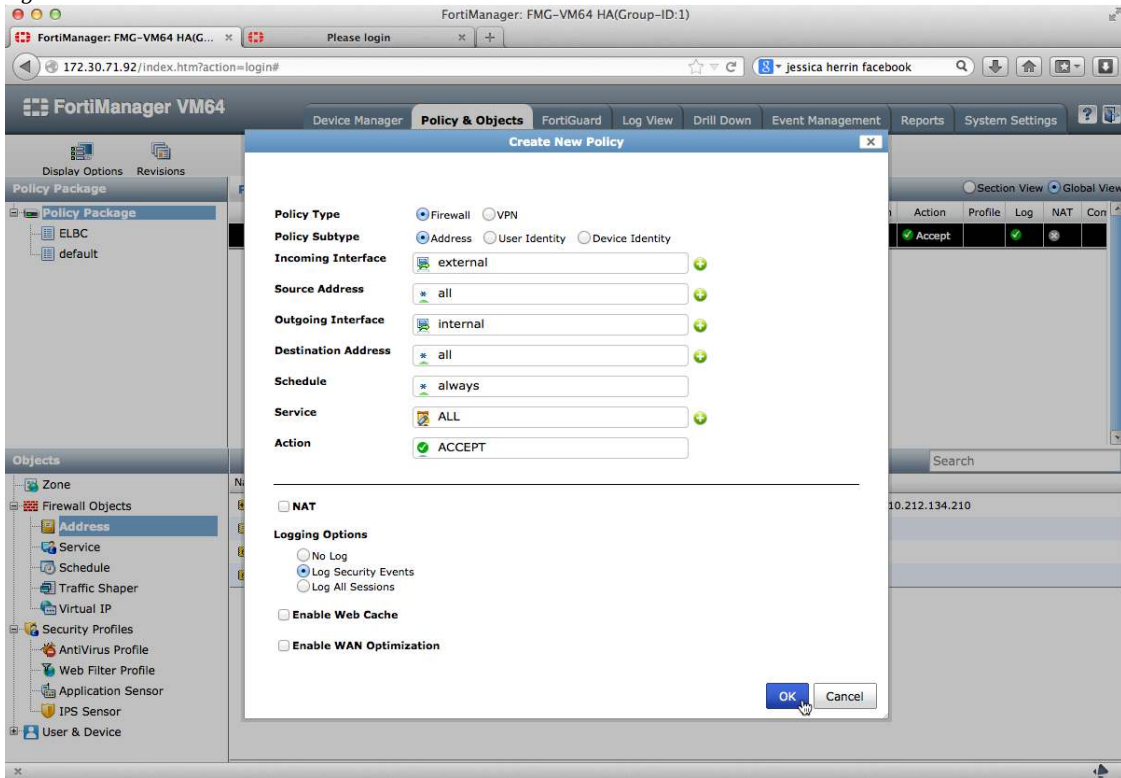
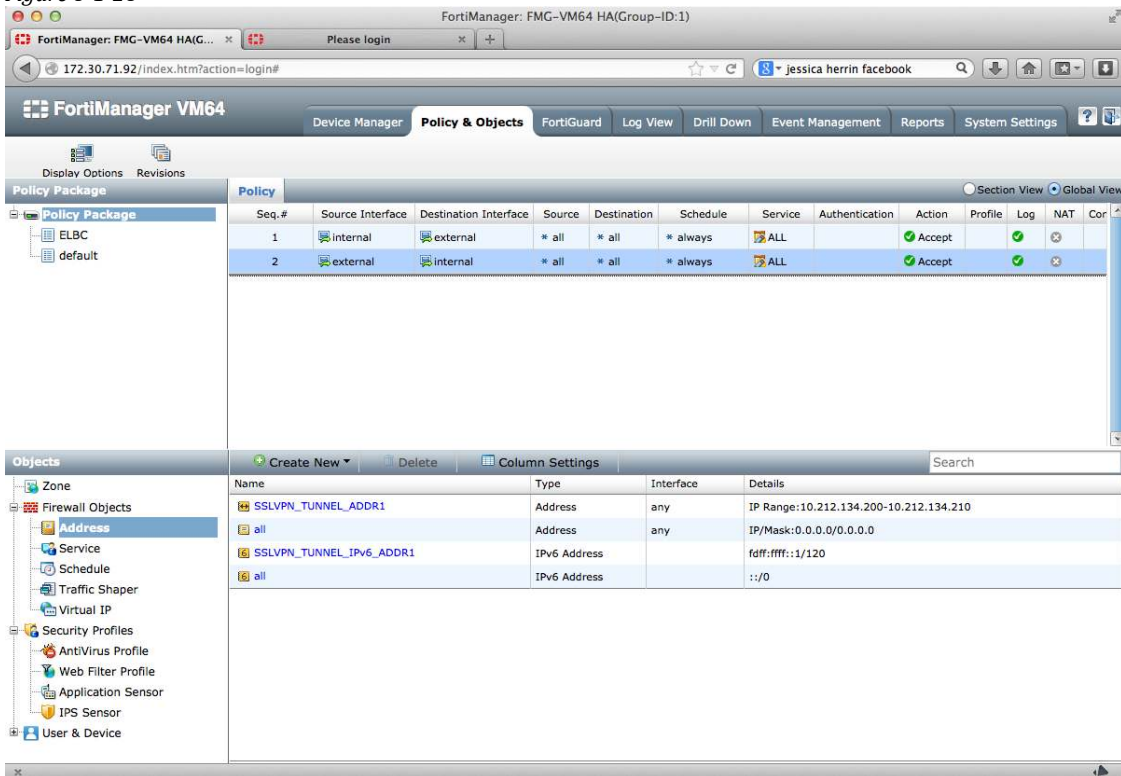


Figure 8-1-28



Deploy System Configuration and Firewall Policy Packages

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

Figure 8-1-29

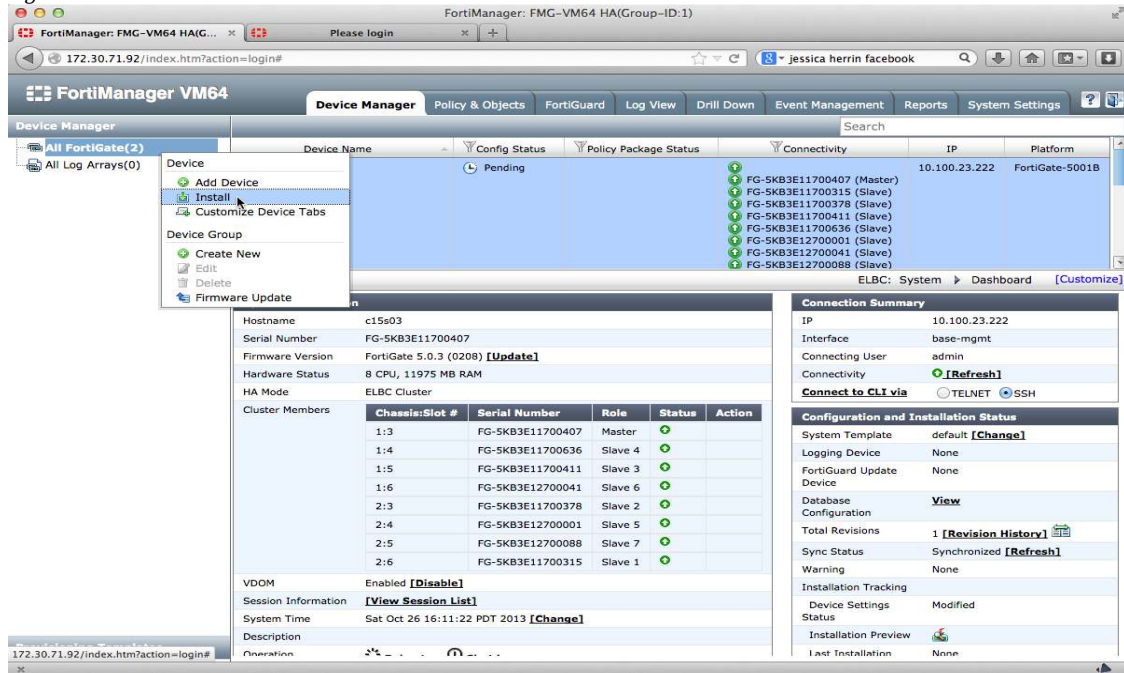


Figure 8-1-30

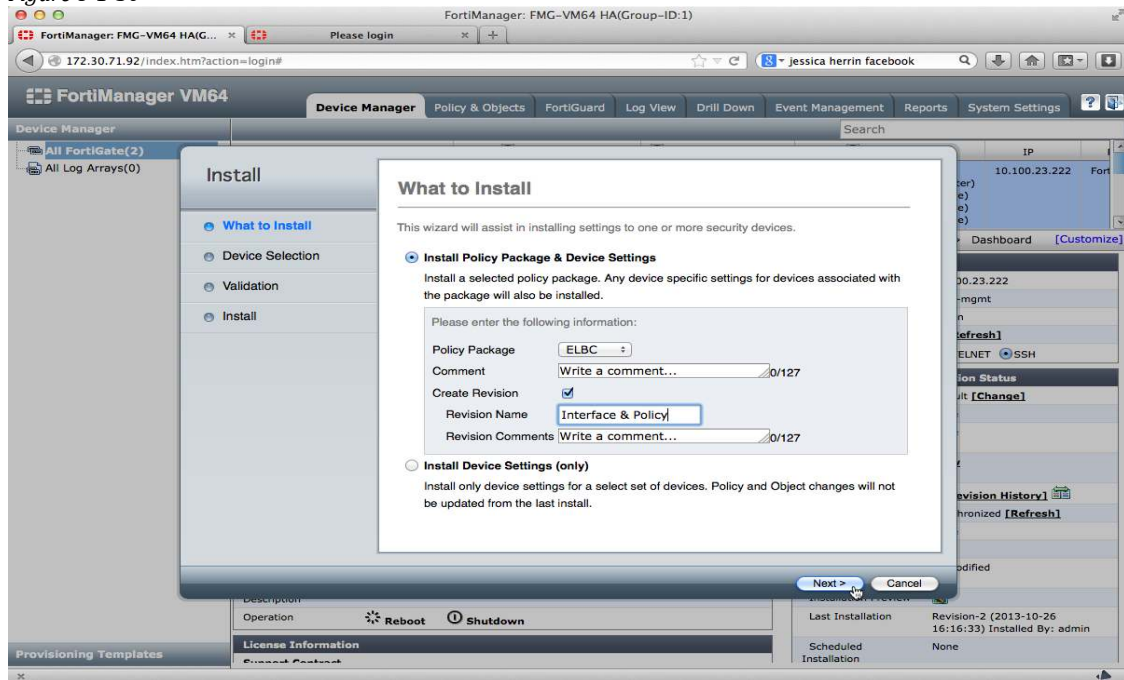


Figure 8-1-31

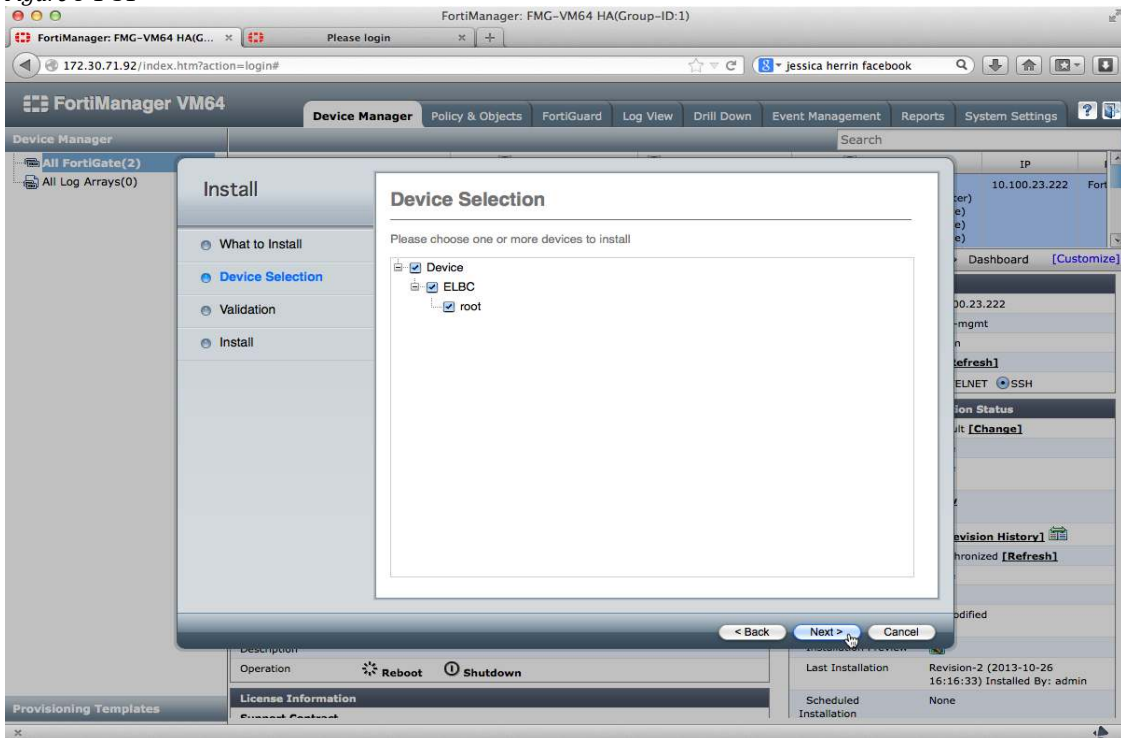


Figure 8-1-32

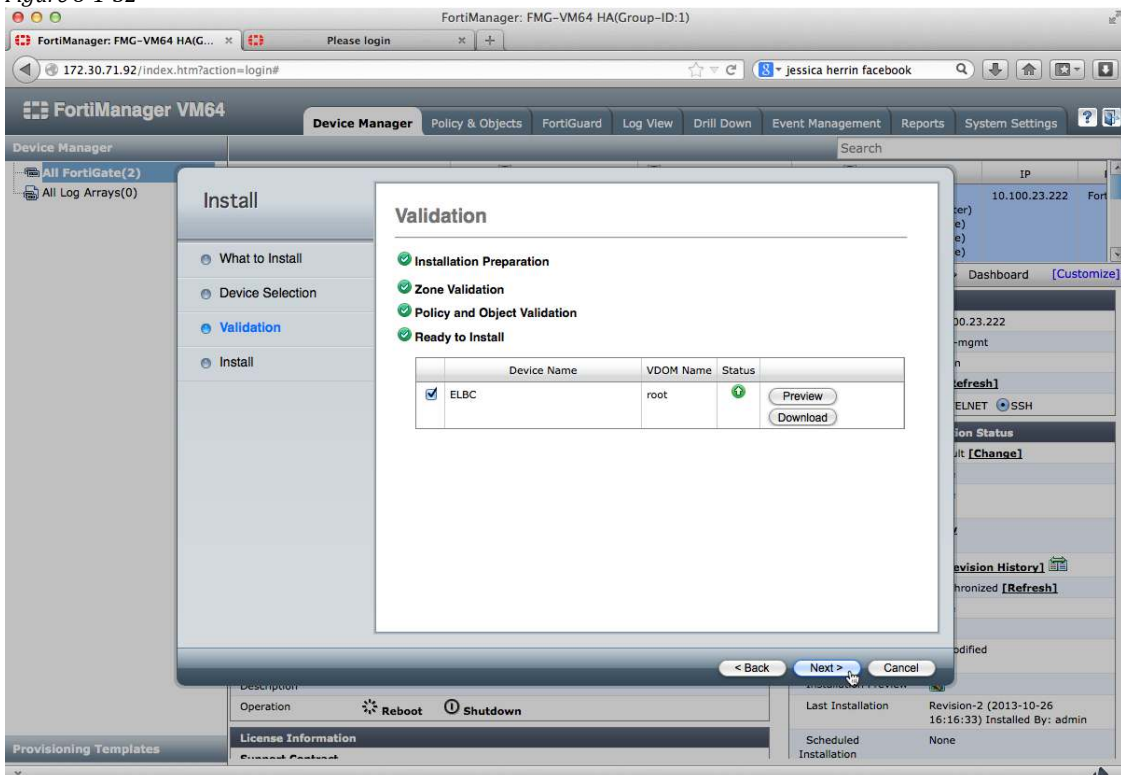


Figure 8-1-33

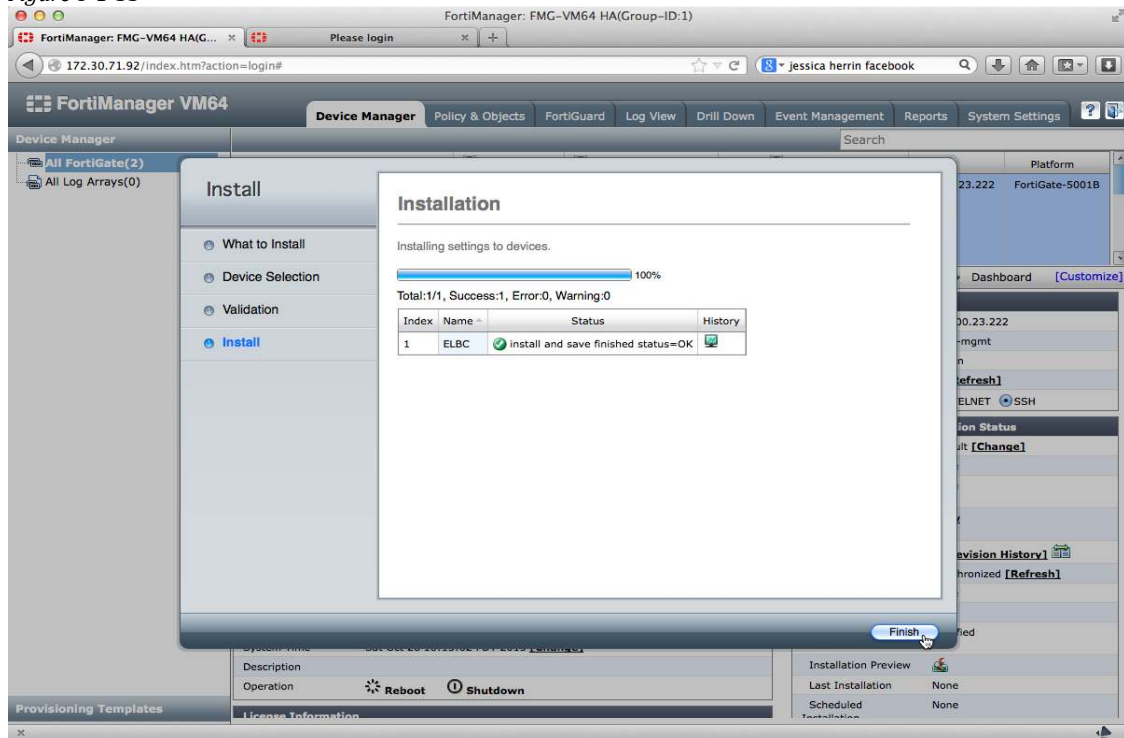
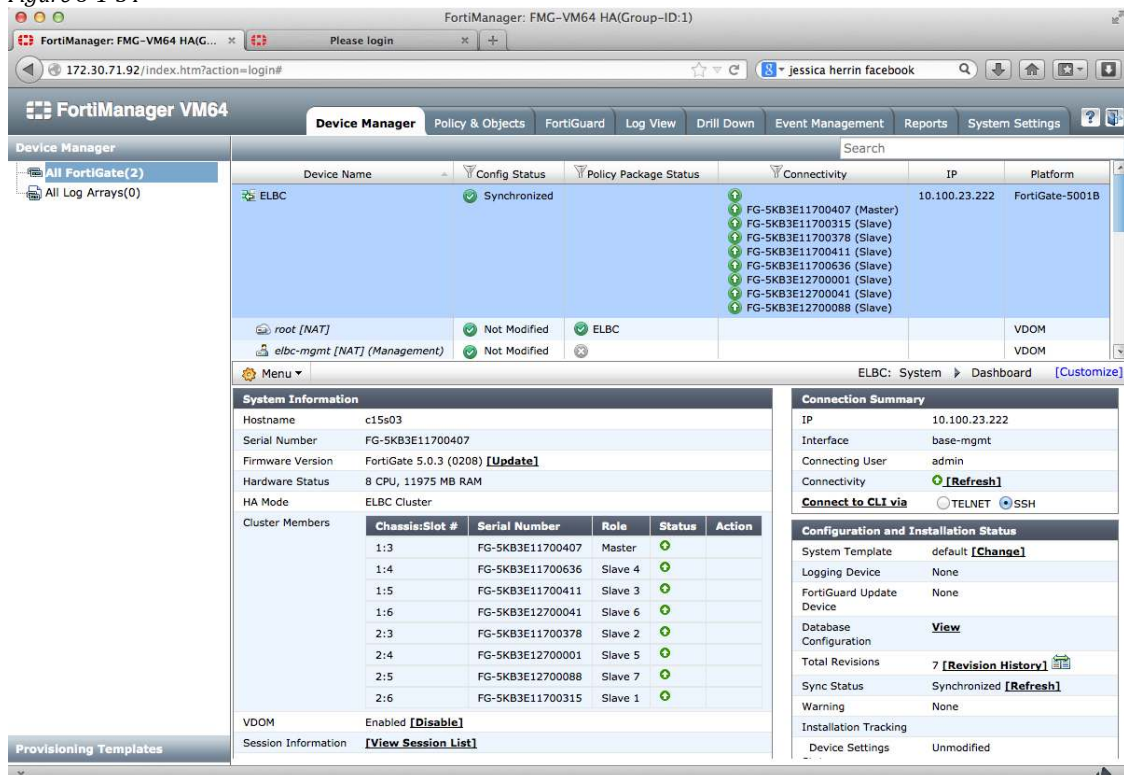


Figure 8-1-34



FortiGate Firmware Upgrade

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.

Figure 8-2-1

The screenshot shows the FortiManager VM64 interface. The 'Device Manager' tab is active, displaying a list of devices. The 'ELBC' device is selected, and its 'System Information' is shown. The 'Firmware Version' is 'FortiGate 5.0.3 (0208)' with an '[Update]' button next to it. The 'Hardware Status' is '8 CPU, 11975 MB RAM'. The 'HA Mode' is 'ELBC Cluster'. The 'Cluster Members' table is as follows:

Chassis:Slot #	Serial Number	Role	Status	Action
1:3	FG-5KB3E11700407	Master	✓	
1:4	FG-5KB3E11700636	Slave 4	✓	
1:5	FG-5KB3E11700411	Slave 3	✓	
1:6	FG-5KB3E12700041	Slave 6	✓	
2:3	FG-5KB3E11700378	Slave 2	✓	
2:4	FG-5KB3E12700001	Slave 5	✓	
2:5	FG-5KB3E12700088	Slave 7	✓	
2:6	FG-5KB3E11700315	Slave 1	✓	

The 'Connection Summary' shows IP: 10.100.23.222, Interface: base-mgmt, Connecting User: admin, and Connectivity: Synchronized. The 'Configuration and Installation Status' shows System Template: default, Logging Device: None, FortiGuard Update: None, and Database Configuration: View.

Figure 8-2-2

The screenshot shows the FortiManager VM64 interface. The 'Device Manager' tab is active, displaying a list of devices. The 'ELBC' device is selected, and its 'Device Firmware Information' is shown. The 'Current Firmware' table is as follows:

Partition	Active	Firmware	Status
1	✓	FortiGate 5.0.3 (0208)	Running

The 'Available Upgrades' table is as follows:

Firmware	Release Date	Upgrade
5.00-00228-228	13-08-09	[Upgrade Now] [Schedule Upgrade]

The 'Upgrade History' table is empty.

Figure 8-2-3

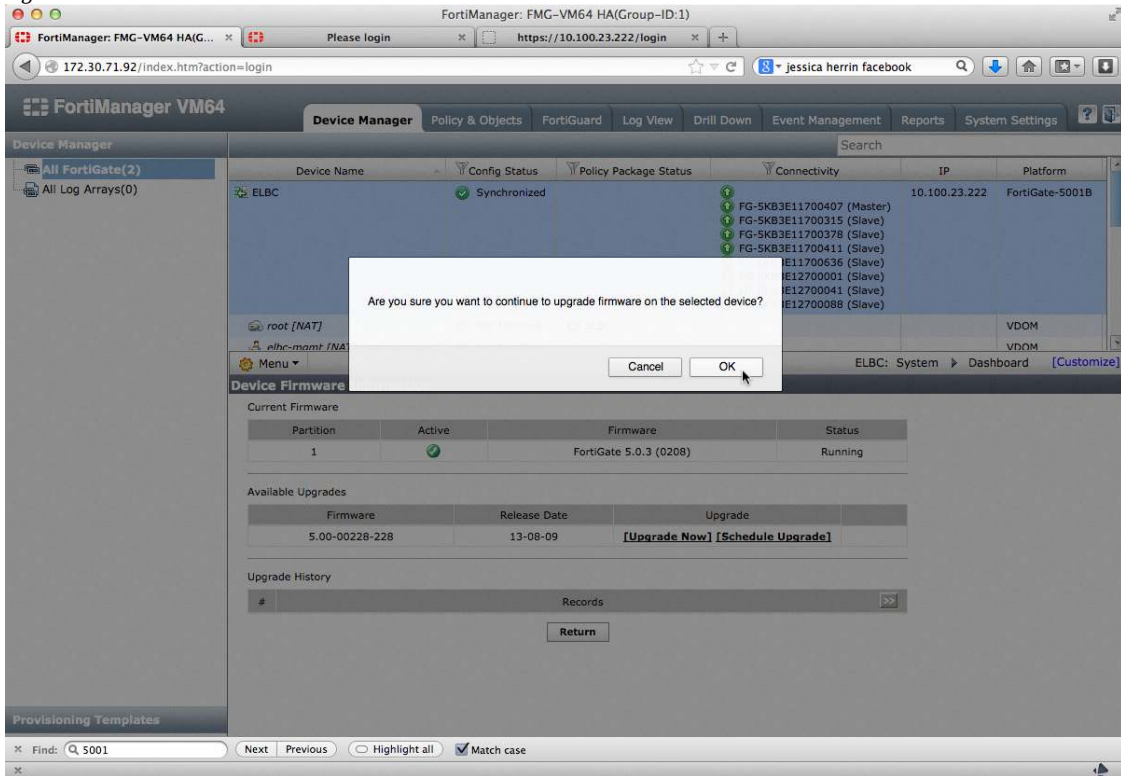
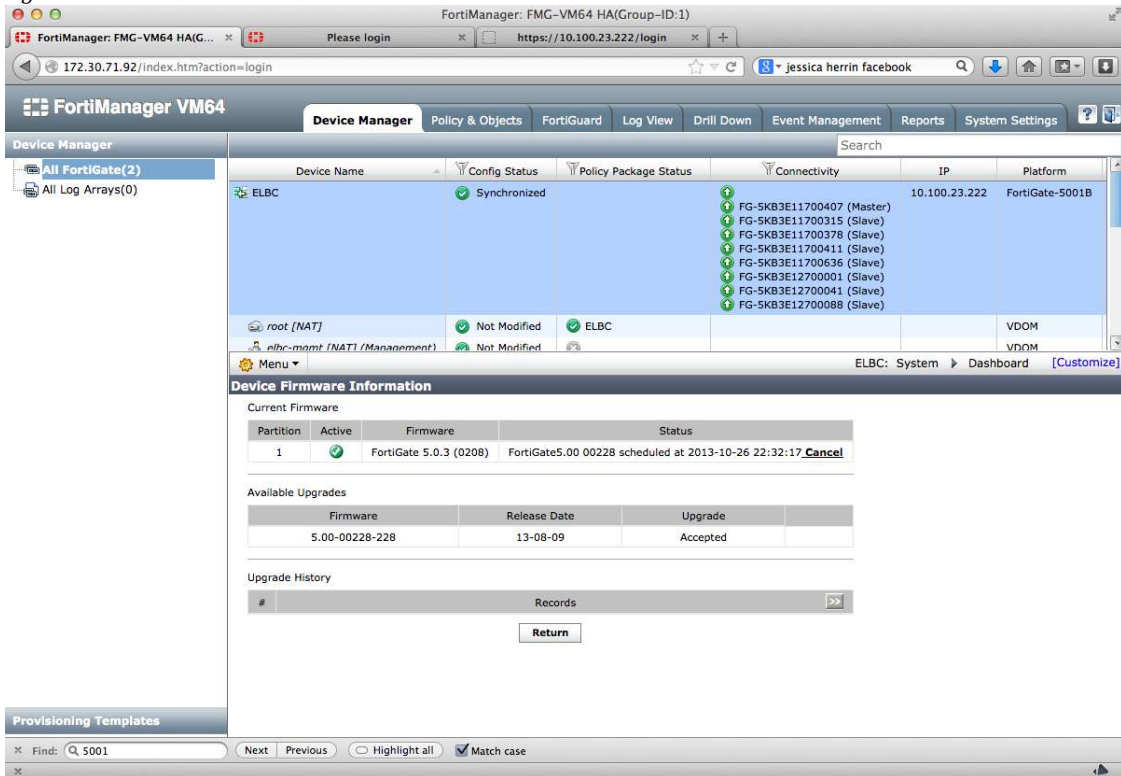


Figure 8-2-4



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.

```
c15s03 login: Update image: Check image OK
Update image: Checking new firmware integrity ... pass
Update image: Please wait for system to restart
Update image: completed
Send image to slave.
Wait for slave to upgrade.
.....
Image upgrade in progress. 19 minutes before aborting.
.....
Image upgrade in progress. 18 minutes before aborting.
.....
All members of the slave chassis are up.
.....
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 # 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 health 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

FortiSwitch Management

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.

Figure 8-3-1

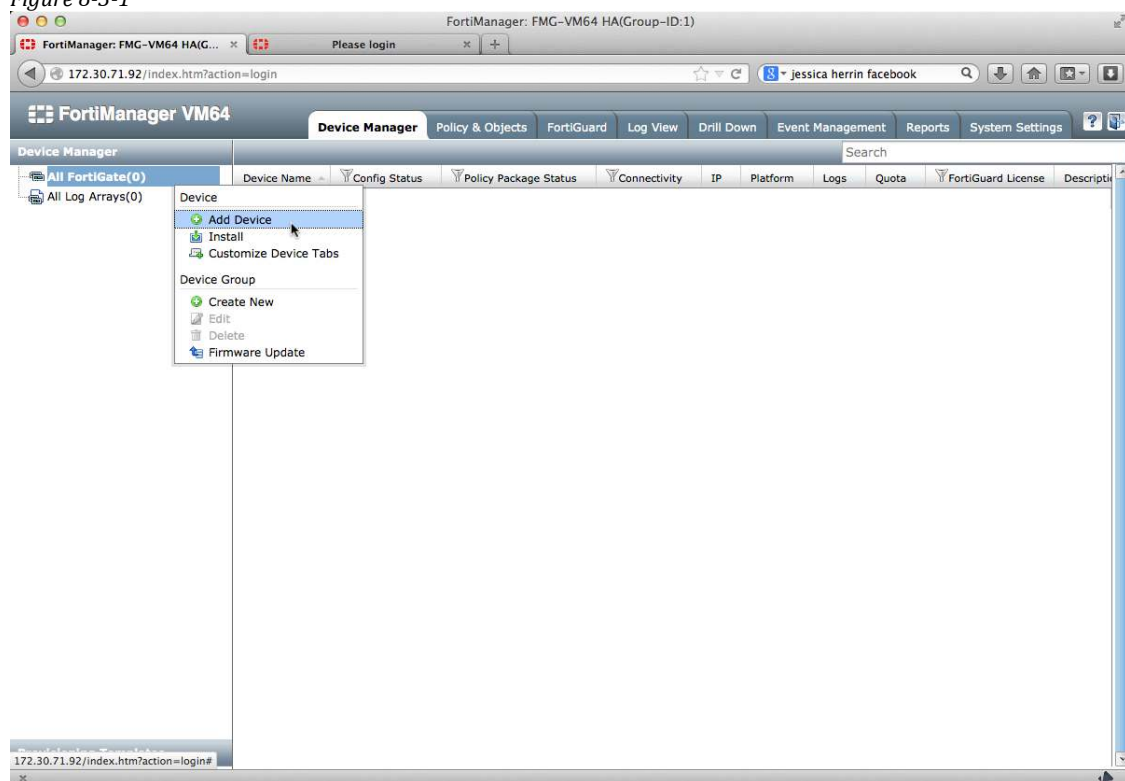


Figure 8-3-2

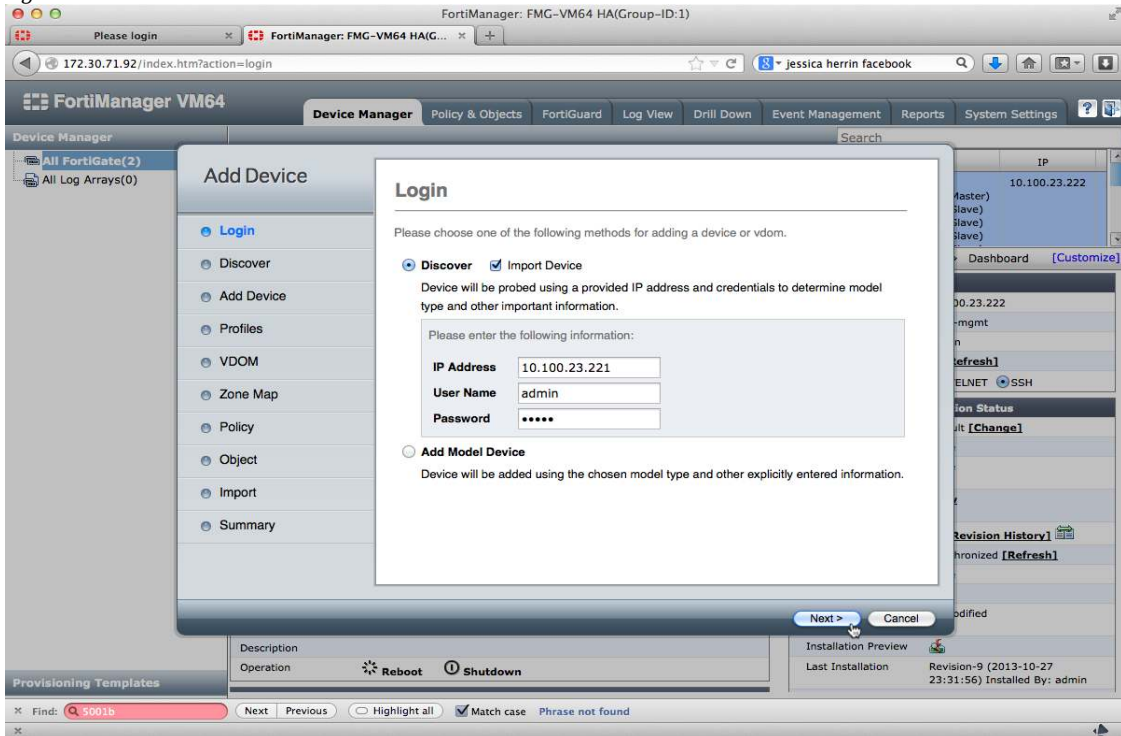


Figure 8-3-3

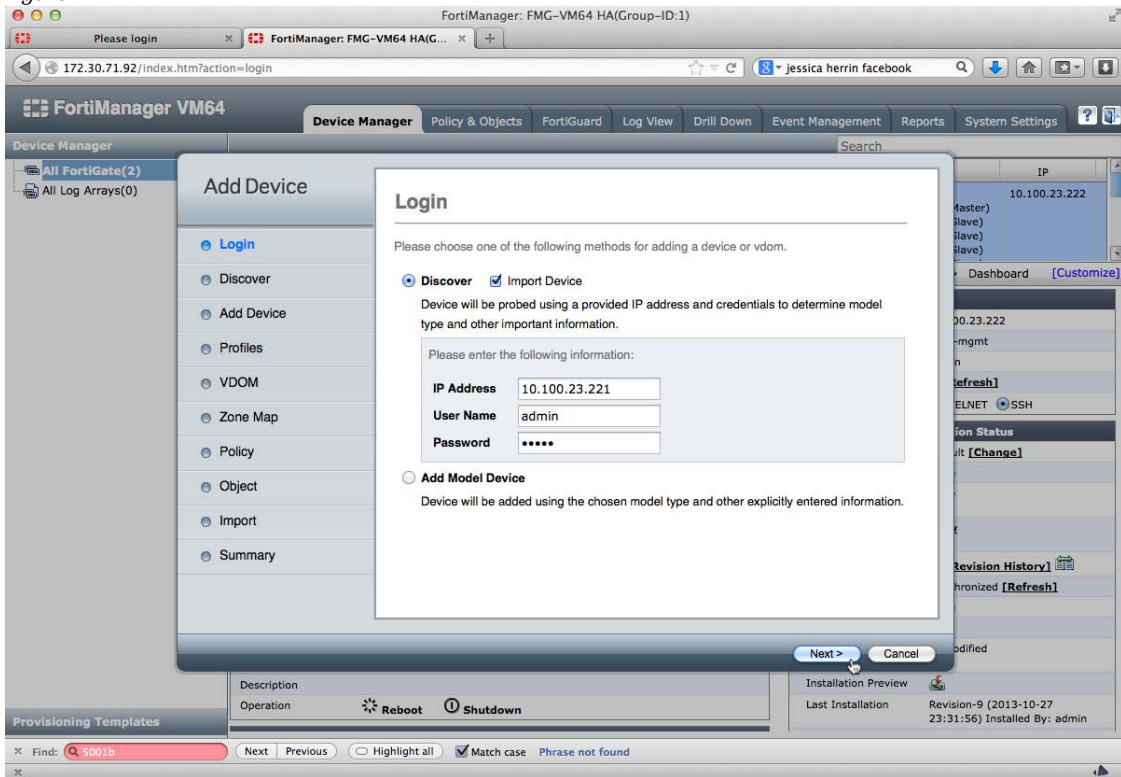


Figure 8-3-4

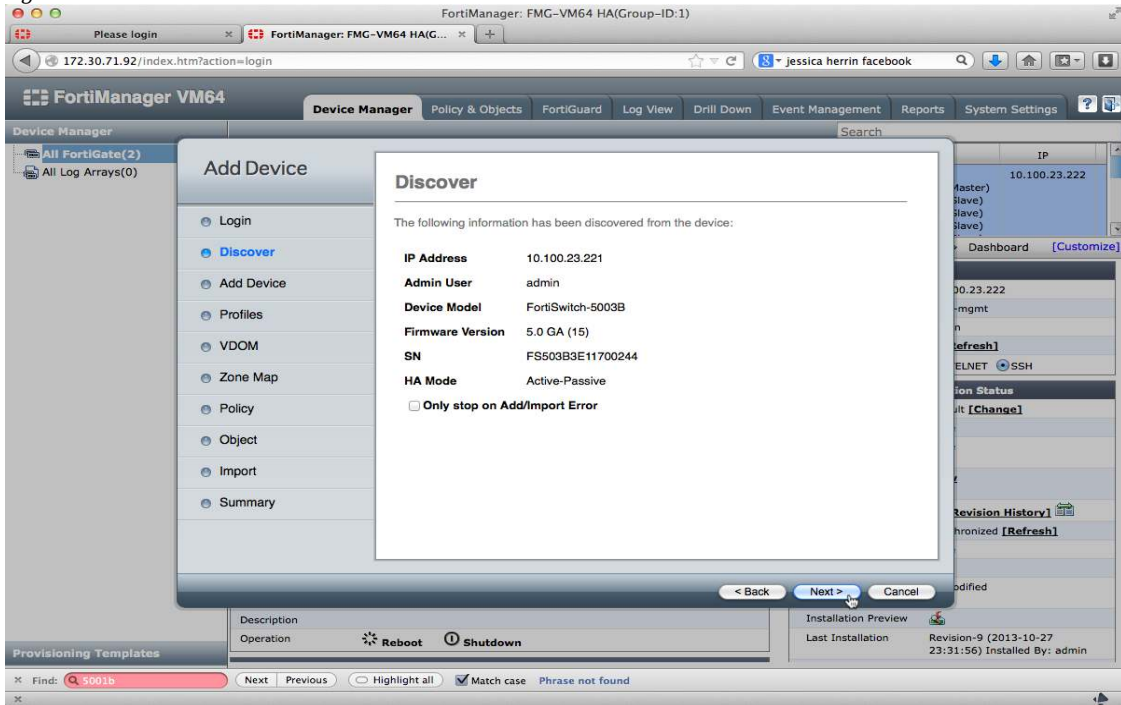


Figure 8-3-5

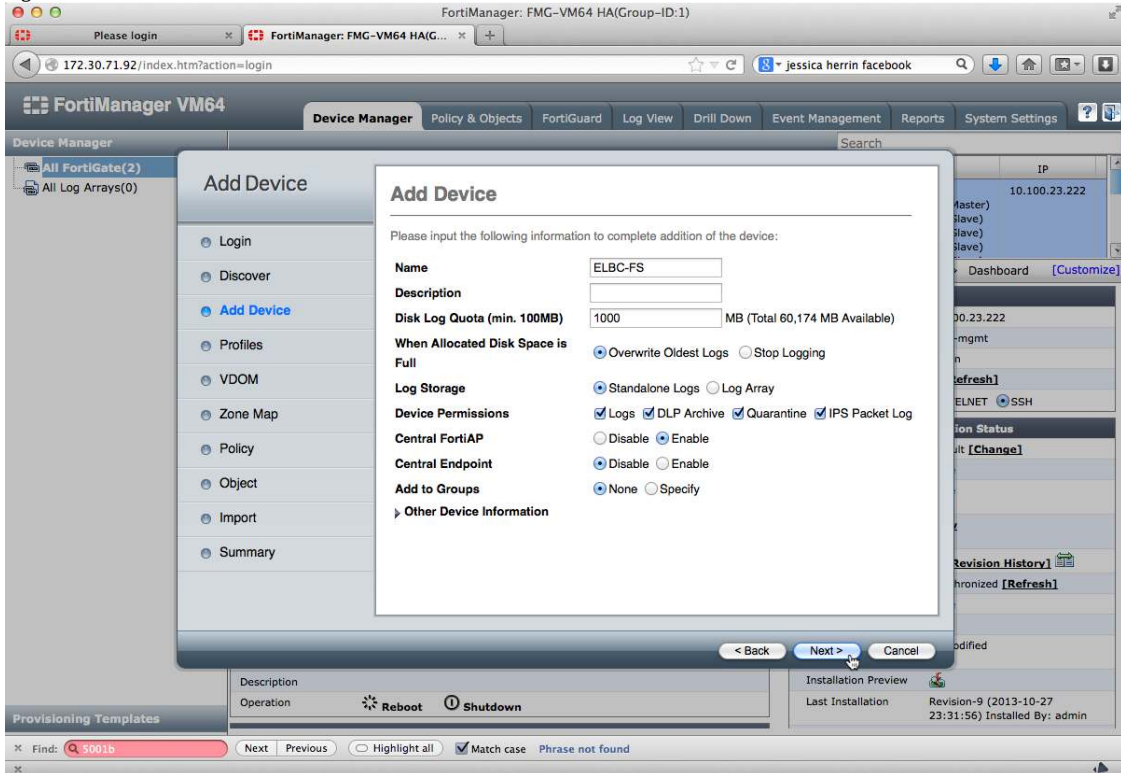


Figure 8-3-6

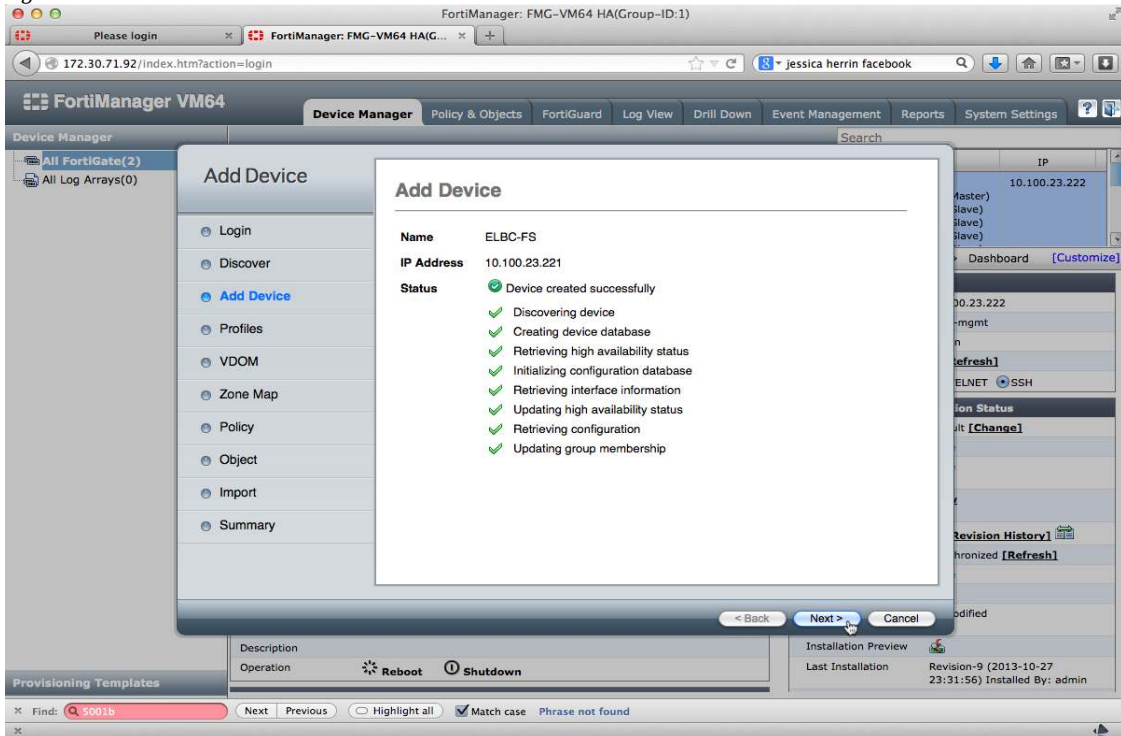


Figure 8-3-7

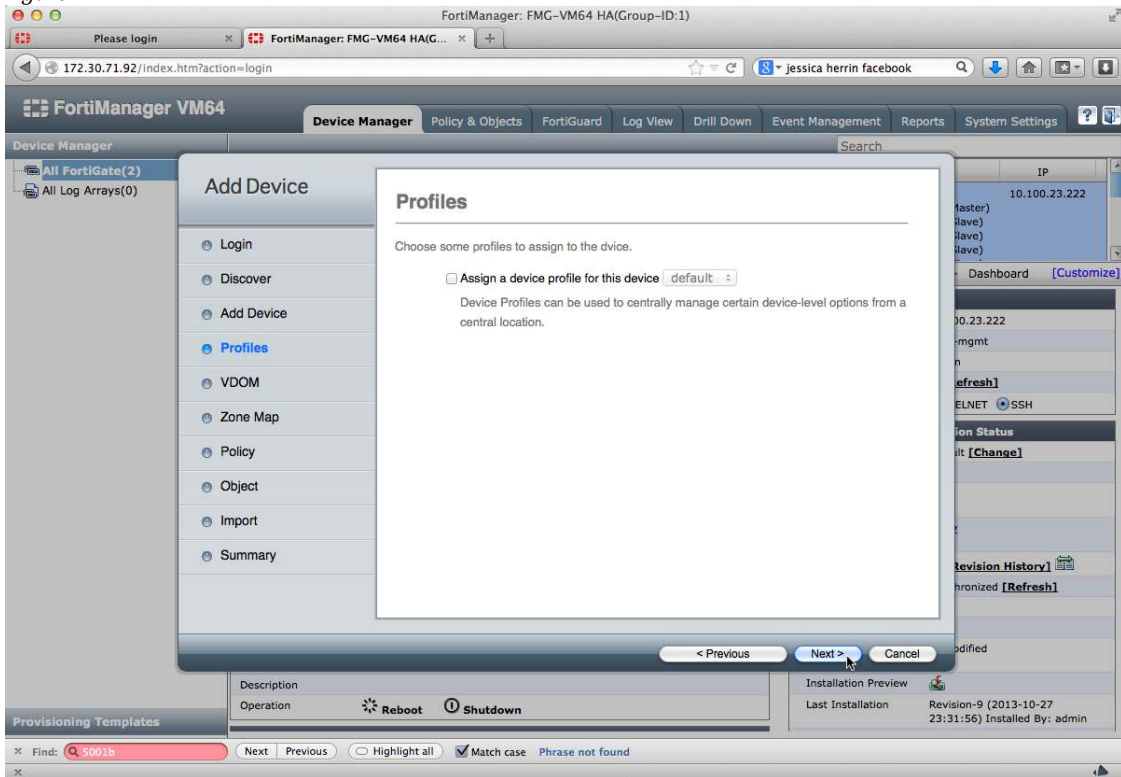


Figure 8-3-8

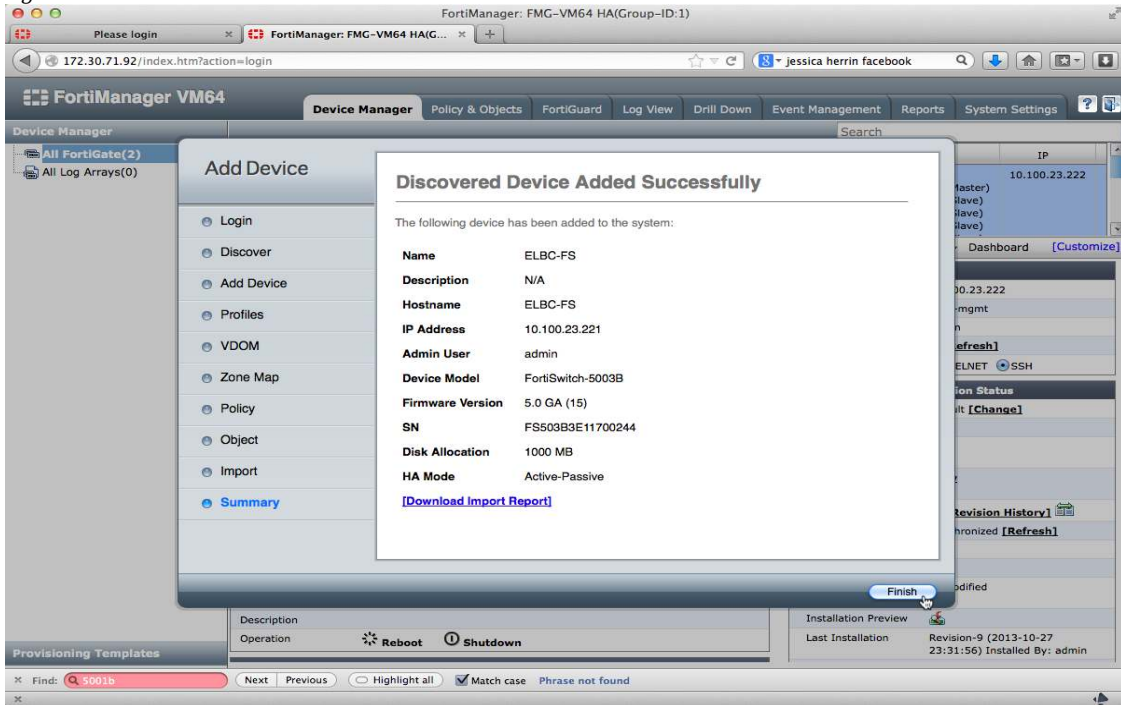
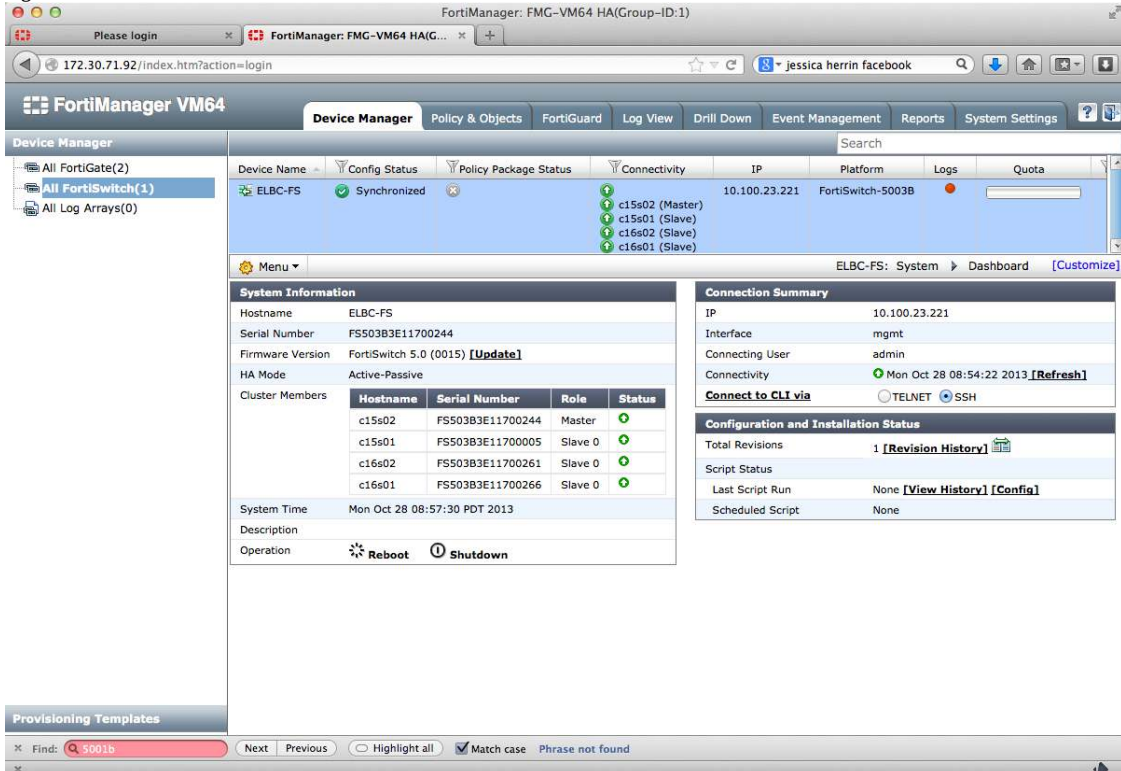


Figure 8-3-9



Chassis Shelf Manager

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 its 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 <http://docs.fortinet.com>.

FortiGate Log Settings

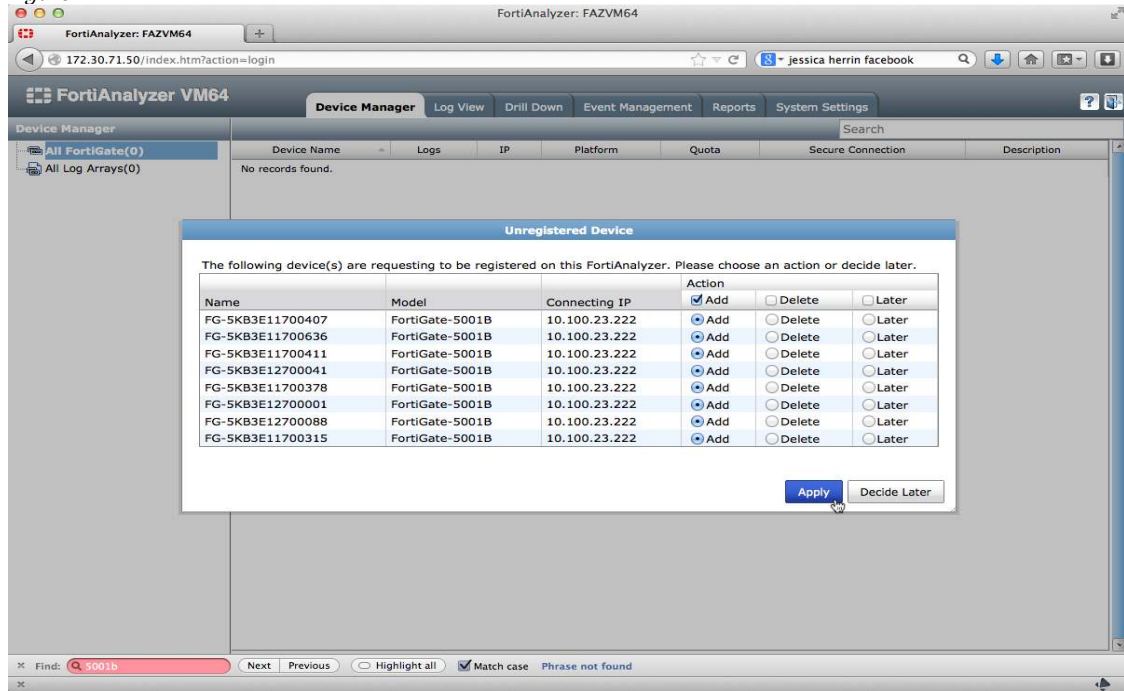
Logging can either be configured via the FortiManager or via the CLI. Once complete, the FortiGates will automatically attempt to register with the FortiAnalyzer.

```
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
```


Logging to the Analyzer

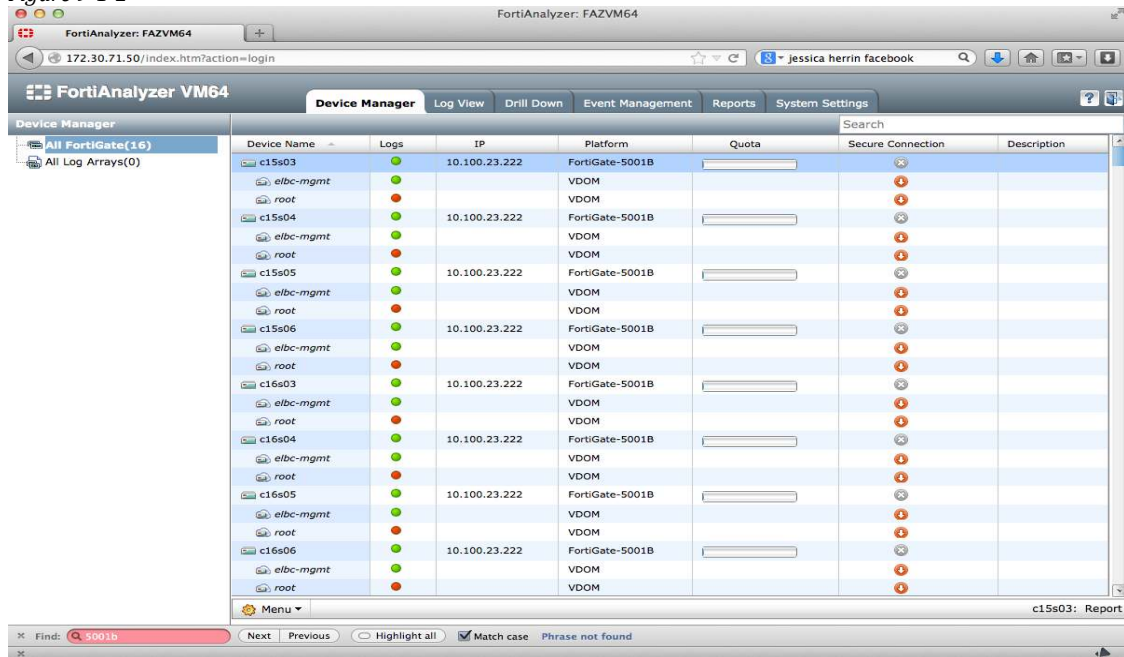
Grant the FortiGates registration access to the FortiAnalyzer

Figure 9-1-1



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

Figure 9-1-2



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

Figure 9-1-3

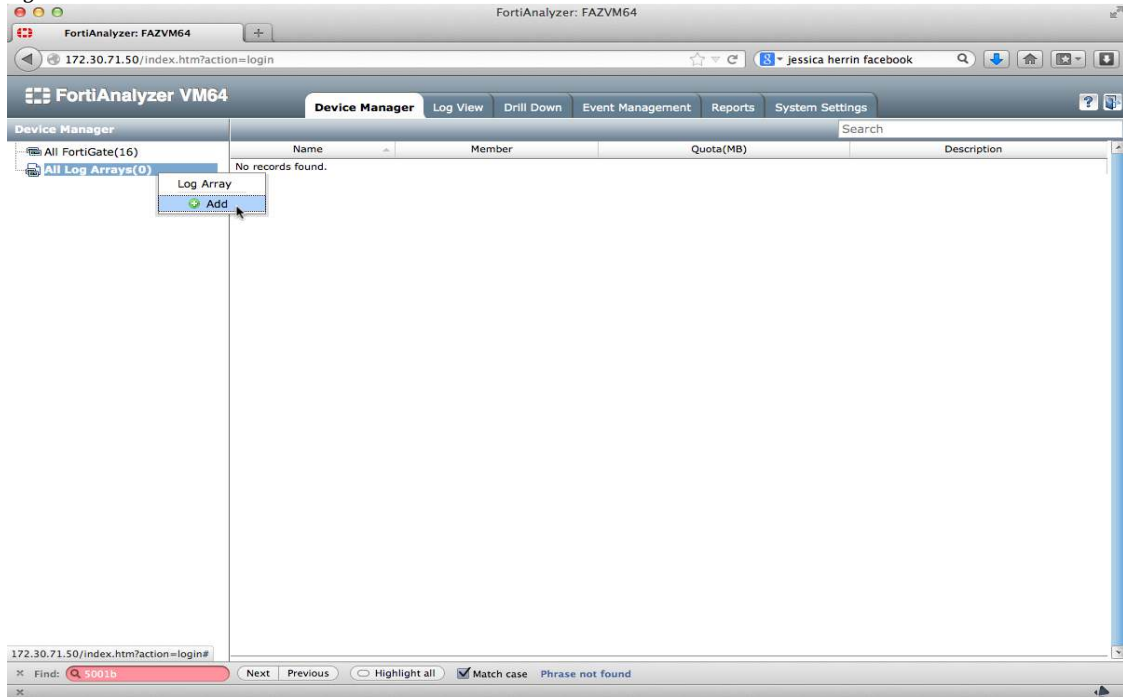


Figure 9-1-4

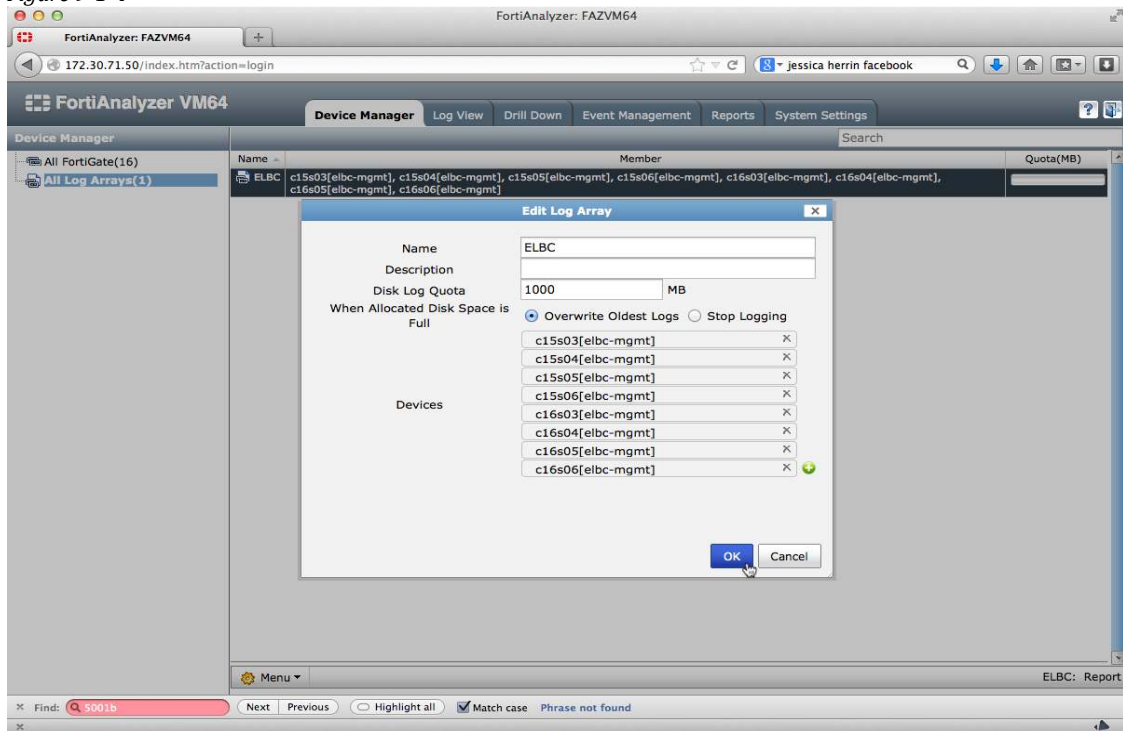
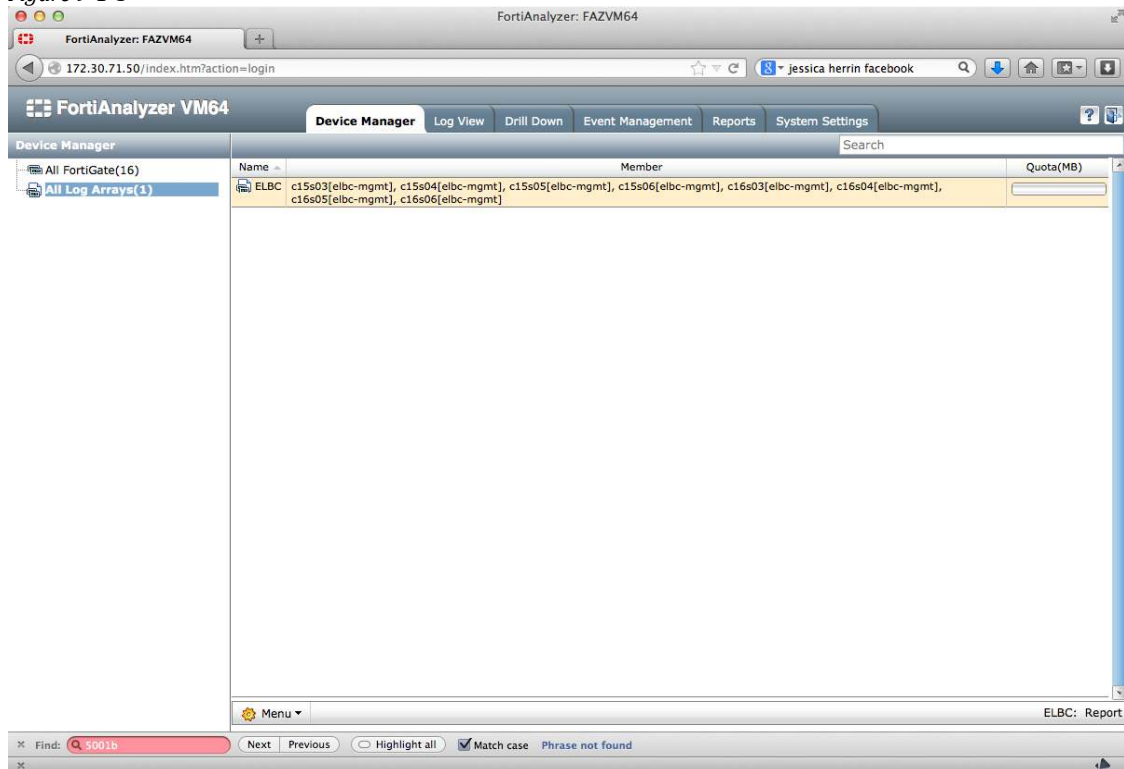


Figure 9-1-5



Verify that logs have been transmitted to the FortiAnalyzer.

Figure 9-1-6

