FORTINET
High Performance Network Security

FortiOS™ Handbook - FortiGate-7000

VERSION 5.4.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 1, 2016

FortiOS™ Handbook - FortiGate-7000

01-542-396655-20161201

TABLE OF CONTENTS

Change Log

Date	Change Description
December 1, 2016	Initial Release

Introduction

This document describes what you need to know to get started using a FortiGate-7000. Also included are details about CLI commands that are specific to FortiGate-7000 products.:

This FortiOS Handbook chapter contains the following sections:

FortiGate-7000 overview provides a quick overview of FortiGate-7000 components.

Getting started with a FortiGate-7000 chassis describes how to get started with managing and configuring your FortiGate-7000 product.

Load balancing FortiGate-7000 CLI commands describes FortiGate-7000 load balancing CLI commands.

FortiGate-7000 overview

A FortiGate-7000 product consists of a FortiGate-7000 series chassis (for example, the FortiGate-7040E) with FortiGate-7000 modules installed in the chassis slots. A FortiGate-7040E chassis comes with two interface modules (FIM) to be installed in slots 1 and 2 to provide network connections and session-aware load balancing to two processor modules (FPM) to be installed in slots 3 and 4.

Currently the following modules are available:

- FIM-7901E Interface Module with thirty-two 10GigE interfaces that can be connected to up to thirty-two 10Gbps data networks.
- FIM-7904E Interface Module with eight 40GigE interfaces that can be connected to up to eight 40Gbps data networks. You can also split each 40GigE port into four 10GigE interfaces and connect to up to forty 10Gbps data networks.
- FIM-7910E Interface Module with four 100GigE interfaces that can be connected to up to four 100Gbps data networks. You can also split each 100GigE port into ten 10GigE interfaces and connect to up to forty 10Gbps data networks.
- FPM-7620E Processor Module that processes sessions load balanced b y the interface modules.

Interface modules include an integrated switch fabric and FortiASIC DP2 processors to load balance millions of data sessions over the chassis fabric backplane to processor modules. Processor modules include NP6 processors that offload network processing and CP9 processors that offload content processing and SSL and IPsec encryption from the processor module CPUs.

Licenses, Device Registration, and Support

- Support & FortiGuard services are tied to the FortiGate-7000 chassis serial number
- Register your product under the chassis serial number
- Use the chassis serial number when communicating with Fortinet Support

FortiGate-7000 and FortiGate-5000 SLBC differences

Although both are chassis session-aware load balancing (SLBC) solutions, the FortiGate-7000 series serves as a single integrated FortiGate solution. A FortiGate-7000 product consists of a selected chassis, selected FIM modules and selected FPM modules. Whereas a FortiGate-5000 solution consists of a collection of separately licensed products.

FIM modules are similar in concept to FortiControllers. Both receive and load-balance traffic to the workers. FIM modules; however, do not have 2 different modes of operations. As well, the FIM modules do not run HA A-P mode, but instead they operate similar to FGCP dual mode. If one FIM module goes down traffic will be interrupted. HA redundancy is not a function of a single chassis, but a function of multiple chassis.

FPM modules are similar to FortiGate-5000 workers in that they apply firewall policies and other security features to traffic. However, FPM modules do not have front panel interfaces so can only receive traffic load balanced to them from FIM modules.

Getting started with a FortiGate-7000 chassis

Once you have installed your FortiGate-7000 chassis in a rack and installed interface modules and processing modules in it you can connected power the chassis and the chassis itself and the modules in the chassis will power up. Review the chassis and module front panel LEDs to verify that everything is operating normally.

You can configure and manage the FortiGate-7000 by connecting an Ethernet cable to one of the MGMT1 to MGMT4 interfaces of the interface modules. By default the MGMT1 to MGMT4 interfaces of each interface module are configured as a static aggregate interface called 1-mgmt or 2-mgmt and all have the same IP address. The default MGMT IP address of the interface module in slot 1 (1-mgmt) is 192.168.1.99. The default MGMT IP of the interface module in slot 2 (2-mgmt) is 192.168.2.99.

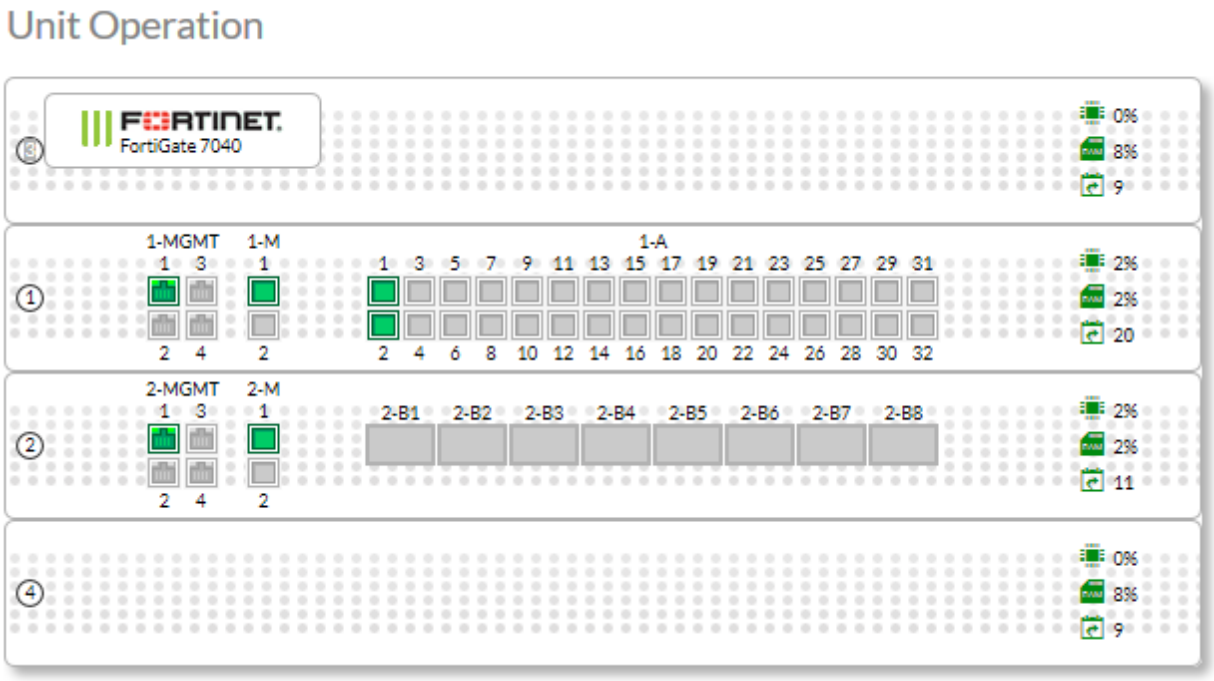
Usually you would connect to the MGMT1 interface of the interface module in slot 1. Connect to the GUI by browsing to https://192.168.1.99. Log into the GUI using the admin account with no password. Connect to the CLI by using SSH to connect to 192.168.1.99.

You can also connect two or more of the mgmt interfaces to a switch and set up an LACP configuration on the switch for redundant management connections to the chassis.

For security reasons you should add a password to the admin account before connecting the chassis to your network.

No matter which of the 8 front panel mgmt interfaces you connect to you can make a management connection to 1-mgmt or 2-mgmt interface IP address. Each FIM module includes a virtualized interface of the other FIM modules management IP address. Also, no matter which front panel mgmt interface you connect to and which IP address you use, all management traffic is sent and received by the FIM module in slot 1.

Example FortiGate-7040 unit operation widget view



The FortiGate-7000 system operates as a cluster, so no matter which management interface you connect to you can see and configure all of the interfaces on both interface modules. The system functions like a single large FortiGate that includes all of the interfaces in the interface modules in slot 1 and slot 2. The names of the interfaces on the interface module in slot 1 are prefixed with a 1 and the names of the interfaces on the interface module in slot 2 are prefixed with a 2.

On the GUI and CLI the MGMT 1 to MGMT 4 interfaces are called 1-mgmt for the interface module in slot 1 and 2-mgmt for the interface module in slot 2. You can see this from the Unit Operation dashboard widget or from the **Network > Interfaces** GUI page.

In most cases, configuring and operating a FortiGate-7000 system is the same as configuring any other FortiGate product. You can connect networks to interface module interfaces and then from the GUI or CLI you can configure interfaces and the add firewall policies and routes and so on to control traffic though the FortiGate-7000 system.

You can configure aggregate interfaces that include physical interfaces from both interface modules. Interfaces added to a aggregate or redundant interface do not have to be on the same interface module.

Managing individual modules

You can connect to the GUI or CLI of individual modules in the chassis using the system management IP address and special port number. Normally you can manage the chassis by connecting to the management IP address, which connects you to the FIM module in slot 1. But in some cases you may want to connect to individual modules. For example, to view the traffic being processed by a specific FPM module you can connect to its GUI.

For example, if the system management IP address is 1.1.1.1 you can connect to the GUI of the FIM module in slot 1 using the system management IP address (for example, by browsing to https://1.1.1.1). You can also use the system management IP address followed by the special port number, for example https://1.1.1.1:44301.

The special port number (in this case 44301) <special-port-number> is a combination of the service port and the chassis slot number. For example, for https access to the module in chassis slot 1 the special port number is 44301.

To connect to the GUI of the FPM module in slot 3 you would browse to https://1.1.1.1:44303.

You can also use the special port number for other management connections. For example, to send and SNMP query to the FPM module in slot for use the port number 16103.

Firmware upgrades

All of the components in your FortiGate-7000 product run the same firmware image. You upgrade the firmware from the GUI or CLI just as you would any FortiGate product. Durning the upgrade process the firmware of all of the modules in the chassis is upgrading in one step. Firmware upgrades should be done duing a quiet time because traffic will be briefly interrupted during the upgrade process.

Restarting the chassis

To restart the modules in the chassis, connect to any CLI and enter the command `execute reboot`. When you enter this command all of the modules in the chassis reboot.

Some SLBC details

The FortiGate-7000 chassis uses session-aware load balancing (SLBC) to distribute traffic from the FIM modules to the FPM modules. Most network traffic is distributed to all of the FPM modules (workers). However, for various reasons some traffic types cannot be load balanced. Traffic that cannot be load balanced is all processed by one of the workers. Internal to the system this FPM module is designated as the ELBC master.

All traffic that cannot be load balanced is directed to the ELBC master. You can also configure the system to send any type of traffic to the ELBC master or to other specific FPM modules. All this is controlled by the `config loadbalance flow-rule` command. Traffic that just is sent to the ELBC master includes, IKE, Kerberos, BGP, RIP, IPv4 and IPv6 DHCP, PPTP, BFD, and IPv4 and IPv6 multicast.

The FortiGate-7000 system includes a configuration synchronization system that synchronizes the configuration to all modules in the chassis. To support this feature, The FIM module in slot 1 becomes the config-sync master and this module makes sure the configurations of all modules are synchronized. As well, all management traffic is directed to the config-sync master. As well, all management traffic is received and sent by this module.

Management Traffic and Gateways

Local-in management traffic is always received by the FIM module in slot 1 (the config-sync master). Usually this traffic is directed to the chassis management IP address. You can define a chassis management gateway.:

```
config load-balance setting
   set chassis-mgmt-ip <ip> <mask>
   set chassis-mgmt-gateway <gateway-ip>
```

This gateway is only active on the FIM module in slot 1.

On the other hand, local-out traffic such as FortiGuared web filtering queries initiated by one of the FPM modules passes through one of the virtual mgmt interfaces to either 1-mgmt or 2-mgmt on the FIM module in slot 1, depending on the route defined. This route is active on all modules.

Failover

A chassis cluster will continue to operate if even if one of the FIM or FPM module fails. If an FPM module fails, traffic fails over to the remaining FPM modules. If an FIM module fails, the other FIM module will continue to operate and will become the config-sync master. However, traffic received by the failed FIM module will be lost.

You can use LACP or redundant interfaces to connect interfaces of both FIMs to the same network. In this way, if one of the FIMs fails the traffic will continue to be received by the other FIM.

FortiGate-7000 systems also support FGCP HA between chassis. FGCP configuration is the same as a normal FortiGate FGCP cluster.

Load balancing FortiGate-7000 CLI commands

The most notable difference between a FortiGate-7000 system and other FortiGates are the commands described in this section for configuring load balancing. The following commands are available:

```
config load-balance flow-rule
config load-balance setting
```

In most cases you do not have to use these commands. However, they are availble to customize some aspects of load balancing.

config load-balance flow-rule

Use this command to add flow rules that add exceptions to how matched traffic is processed by an SLBC cluster. Specifically you can use these rules to match a type of traffic and control whether the traffic is forwarded or blocked. And if the traffic is forwarded you can specify whether to forward the traffic to a specific worker or to all workers.

One common use of this command is to control how traffic that is not load balanced is handled. For example, use the following command to send all GRE traffic to the worker in slot 8. In this example the GRE traffic is received by FortiController front panel ports F1 nd F5:

```
config load-balance flow-rule
   edit 0
      set src-interface 1f1 f5
      set ether-type ip
      set protocol gre
      set action forward
      set forward-slot 8
   end
```

The default configuration includes a number of flow rules that send traffic such as BGP traffic, DHCP traffic and so on to the primary worker. This is traffic that cannot be load balanced and is then just processed by the primary worker.

Syntax

```
config load-balance flow-rule
   edit 0
      set status {disable | enable}
      set src-interface <interface-name> [interface-name>...}
      set vlan <vlan-id>
      set ether-type {any | arp | ip | ipv4}
      set src-addr-ipv4 <ip-address> <netmask>
      set dst-addr-ipv4 <ip-address> <netmask>
      set src-addr-ipv6 <ip-address> <netmask>
      set dst-addr-ipv6 <ip-address> <netmask>
      set protocol {any | icmp | tcp | udp | igmp | sctp | gre | esp }
      ah | ospf | pim | vrrp}
      set src-l4port <start>[-<end>]
      set dst-l4port <start>[-<end>]
      set action {forward | mirror-ingress | mirror-egress | stats | drop}
```

```
    set mirror-interface <interface-name>
    set forward-slot {master | all | load-balance | FPM3 | FMP4 | FPM5 | FPM6}
    set priority <number>
    set comment <text>
end
```

status {disable | enable}

Enable or disable this flow rule. Default for a new flow-rule is disable.

src-interface <interface-name> [interface-name>...}

The names of one or more FIM interface front panel interfaces accepting the traffic to be subject to the flow rule.

vlan <vlan-id>

If the traffic matching the rule is VLAN traffic, enter the VLAN ID used by the traffic.

ether-type {any | arp | ip | ipv4 | ipv6}

The type of traffic to be matched by the rule. You can match any traffic (the default) or just match ARP, IP, or IPv4 traffic.

{src-addr-ipv4 | dst-addr-ipv4 | src-addr-ipv6 | dst-addr-ipv6} <ip-address> <netmask>

The source and destination address of the traffic to be matched. The default of 0.0.0.0 0.0.0.0 matches all traffic.

protocol {any | icmp | tcp | udp | igmp | sctp | gre | esp | ah | ospf | pim | vrrp}

If ether-type is set to ip, ipv4 or ipv6 specify the protocol of the IP or IPv4 traffic to match the rule. The default is any.

{src-l4port | dst-l4port} <start>[-<end>]

Specify a source port range and a destination port range. This option appears for some protocol settings. For example if protocol is set to tcp or udp. The default range is 0-0.

action {forward | mirror-ingress | mirror-egress | stats | drop}

How to handle matching packets. They can be dropped, forwarded to another destination or you can record statistics about the traffic for later analysis. You can combine two or three settings in one command for example you can set action to both forward and stats to forward traffic and collect statistics about it. Use append to add multiple options.

The default action is forward.

The mirror-ingress option copies (mirrors) all ingress packets that match this flow rule and sends them to the interface specified with the mirror-interface option.

The mirror-egress option copies (mirrors) all egress packets that match this flow rule and sends them to the interface specified with the mirror-interface option.

set mirror-interface <interface-name>

The name of the interface to send packets matched by this flow-rule when action is set to mirror-ingress or mirror-egress.

forward-slot {master | all | load-balance | FPM3 | FMP4 | FPM5 | FPM6}

The worker that you want to forward the traffic that matches this rule to. master forwards the traffic the worker that is operating as the primary worker (usally the FPM module in slot 3. All means forward the traffic to all workers. load-balance means use the default load balancing configuration to handle this traffic. FPM3, FPM4, FMP5 and FPM3 allow you to forward the matching traffic to a specific FPM module. FPM3 is the FPM module in slot 3. FPM4 is the FPM module in slot for. And so on..

priority <number>

Set the priority of the flow rule in the range 1 (highest priority) to 10 (lowest priority). Higher priority rules are matched first. You can use the priority to control which rule is matched first if you have overlapping rules.

comment <text>

Optionally add a comment that describes the rule.

config load-balance setting

Use this command to set a wide range of load balancing settings.

```
config load-balance setting
   set chassis-mgmt-status {disable | enable}
   set chassis-mgmt-ip <ip> <mask>
   set chassis-mgmt-gateway <gateway-ip>
   set chassis-mgmt-route-dst <class_ip> <net_netmask>
   set mgmt-interface-auto-assign-ip {disable | enable}
   set max-miss-heartbeats <heartbeats>
   set max-miss-mgmt-heartbeats <heartbeats>
   set weighted-load-balance {disable | enable}
   set dp-load-distribution-method {round-robin | src-ip | dst-ip | src-dst-ip | src-ip-
       sport | dst-ip-dport | src-dst-ip-sport-dport}
      config workers
         edit 3
            set status enable
            set weight 5
         end
   end
```

chassis-mgmt-status {disable | enable}

Enable or disable being able to manage the chassis with one management IP address. This option is enabled by default. If disabled the chassis-mgmt-ip and chassis-mgmt-gateway and chassis-mgmt-route-dst options are not available and you manage the chassis by connecting to individual FIM interface module management interfaces.

chassis-mgmt-ip <ip> <mask>

The IP address and netmask to be used for managing the chassis if chasis-mgmt-status is enabled.

chassis-mgmt-gateway <gateway-ip>

The IP address of the next hop router to allow access to the management IP from a differenet subnet. This option is only available if chasis-mgmt-status is enabled.

chassis-mgmt-route-dst <class_ip> <net_netmask>

The management route destination for chassis mgmt. This option is only available if chasis-mgmt-status is enabled.

mgmt-interface-auto-assign-ip {disable | enable}

Enable access to each module in the chassis using a variation on the management IP address that uses a special port number that includes the chassis slot number. This option is enabled by default.

When enabled you can use the following formula to access any module in a chassis:

<protocol><address>:<special-port-number>

Where <special-port-number> is a combination of the service port and the chassis slot number. For example, for https access to the module in chassis slot 2 browse to the following if the management IP address is 192.168.1.99:

https://192.168.1.99/44302

Note that this applies to all management access, including SNMP. For example, to send an SNMP query to the module in chassis slot 3 you would set the SNMP query port to 16103.

max-miss-heartbeats <heartbeats>

Set the number of missed heartbeats before a worker is considering to have failed. If this many heartbeats are not received from a worker, this indicates that the worker is not able to process data traffic and no more traffic will be sent to this worker.

The time between heartbeats is 0.2 seconds. Range is 3 to 300. 3 means 0.6 seconds, 10 (the default) means 2 seconds, and 300 means 60 seconds.

max-miss-mgmt-heartbeats <heartbeats>

Set the number of missed management heartbeats before a worker is considering to have failed. If a management heartbeat fails, there is a communication problem between a worker and other workers. This communication problem means the worker may not be able to synchronize configuration changes, sessions, the kernel routing table, the bridge table and so on with other workers. If a management heartbeat failure occurs, no traffic will be sent to the worker.

The time between managment heartbeats is 1 second. Range is 3 to 300 seconds. The default is 20 seconds.

weighted-load-balance {disable | enable}

Enable weighted load balancing depending on the slot weight. Use the config slot command to set the weight for each slot.

dp-load-distribution-method {round-robin | src-ip | dst-ip | src-dst-ip | src-ip-sport | dst-ip-dport | src-dst-ip-sport-dport}

Set the method used to distribute sessions among workers. Usually you would only need to change the method if you had specific requirements or you found that the default method wasn't distributing sessions in the manner that you would prefer. The default is src-dst-ip-sport-dport.

config workers

Set the weight and enable or disable each worker. Use the edit command to specifiy the slot the worker is installed in. You can enable or disable each worker and set each worker's weight.

The weight range is 1 to 10. 5 is average, 1 is -80% of average and 10 is +100% of average. The weights take effect if weighted-loadbalance is enabled.

```
config workers
   edit 3
      set status enable
      set weight 5
   end
```

FORTINET®

High Performance Network Security