



# TECHNICAL NOTE

## **Fortinet Hardware Acceleration**

**FORTINET**<sup>™</sup>

[www.fortinet.com](http://www.fortinet.com)

*Fortinet Hardware Acceleration Technical Note*  
22 April 2008  
01-30005-0424-20080422

© Copyright 2008 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

**Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Contents

<b>Introduction .....</b>	<b>5</b>
<b>About this document.....</b>	<b>5</b>
<b>Fortinet documentation .....</b>	<b>6</b>
Fortinet Tools and Documentation CD.....	6
Fortinet Knowledge Center .....	6
Comments on Fortinet technical documentation .....	6
<b>Customer service and technical support.....</b>	<b>6</b>
<b>FortiGate hardware accelerated network processing .....</b>	<b>7</b>
<b>Network processor models.....</b>	<b>8</b>
<b>Offloading requirements .....</b>	<b>9</b>
<b>Exceptions to offloading requirements .....</b>	<b>10</b>
IPSec offloading requirements .....	10
HA active-active offloading requirements.....	11
<b>Related CLI settings.....</b>	<b>13</b>
<b>config system interface.....</b>	<b>13</b>
Syntax .....	13
Example .....	15
<b>config system npu .....</b>	<b>15</b>
Syntax .....	15
Example .....	16
<b>Examples .....</b>	<b>17</b>
<b>Accelerated tunnel mode IPSec .....</b>	<b>18</b>
To configure hardware accelerated tunnel mode IPSec.....	18
<b>Accelerated interface mode IPSec .....</b>	<b>19</b>
To configure hardware accelerated interface mode IPSec.....	19
<b>Index.....</b>	<b>21</b>



# Introduction

Some Fortinet products contain proprietary FortiASIC network processors. These network processors provide hardware accelerated network processing for certain eligible traffic types passing through attached ports. This additional processing resource frees FortiGate units' main processing resources for other tasks, thereby improving network performance.

FortiASIC network processors can improve network throughput for:

- traffic with small packets, such as VoIP
- latency-sensitive traffic, such as streaming multimedia
- traffic with long session lifetimes, such as FTP
- IPSec VPN traffic
- active-active HA load-balanced traffic
- P2P traffic

Eligible traffic processing is offloaded to network processors. This fast path processing leverages the additional hardware resources of FortiASIC network processors.

Ineligible traffic is processed by the FortiGate unit's main processing resources, and may involve CPU, RAM, and some hardware accelerated content processing from FortiASIC content processors, but does *not* utilize hardware accelerated network processing from FortiASIC network processors.

This chapter contains the following topics:

- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

## About this document

This document explains how the typical packet processing flow is altered when processing is offloaded to a network processor, lists products that contain network processors, and describes how to configure FortiGate units containing network processors, or containing an AMC (Advanced Mezzanine Card) module that contains network processors. It also contains example IPSec configurations involving a FortiGate unit with a FortiGate-ASM-FB4 module, which contains a network processor.

This document contains the following chapters:

- [FortiGate hardware accelerated network processing](#) describes packet processing differences for the network processing path accelerated by a specialized network processor chip.
- [Related CLI settings](#) describes configuration options in the CLI applicable to network processors.

- [Examples](#) contains sample configurations and network topologies whose traffic processing is accelerated by the network processor contained in an installed FortiGate-ASM-FB4 AMC module.

## Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

### Fortinet Tools and Documentation CD

All Fortinet documentation is available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation, see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

### Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

### Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

# FortiGate hardware accelerated network processing

Some FortiGate models and AMC (Advanced Mezzanine Card) modules can offload some types of network traffic processing from main processing resources to specialized network processors. If your network contains a significant volume of traffic that is suitable for offloading, this hardware acceleration can significantly improve your network throughput.

Hardware acceleration generally alters packet processing flow as follows:

- 1 Packets initiating a session pass to the FortiGate unit's main processing resources.
- 2 The FortiGate unit assesses whether the session matches fast path (offload) requirements.

To be suitable for offloading, traffic must possess only characteristics processable by the fast path. For a list of requirements, see [“Offloading requirements” on page 9](#).

If the traffic is categorized as fast path friendly, the FortiGate unit sends the session key or IPSec security association (SA) and configured processing action to the network processor(s).

- 3 Network processors continuously match packets arriving on their attached ports against the session keys and SAs they have received from the FortiGate unit's main processing resources.
  - If a network processor's network interface is configured to perform hardware accelerated anomaly checks, the network processor drops or accepts packets which match the configured anomaly patterns. These checks are separate from anomaly checks performed by IPS, which is not compatible with network processor offloading. For details, see [“config system interface” on page 13](#).
  - The network processor next checks for a matching session key or SA. If a matching session key or SA is found, and if the packet meets packet requirements, the network processor processes the packet according to the configured action and then sends the resulting packet. Packet processing is hardware accelerated.
  - If a matching session key or SA is not found, or if the packet does not meet packet requirements, the traffic cannot be offloaded. The network processor sends the data to the FortiGate unit's main processing resources, which process the packet. Packet processing is similar to normal network interfaces (that is, packet processing is not hardware accelerated by the network processor, and requires main processing resources). Packet forwarding occurs at normal rates.



**Note:** Network processors do not count offloaded packets, and offloaded packets will not be included in traffic statistics, such as FortiAnalyzer traffic reports.

Some traffic processing can still be hardware accelerated, even though it does not meet general offloading requirements. For example, some IPSec traffic originates from the FortiGate unit itself and does not follow the offloading requirement of ingress from a network processor's network interface, but FortiGate units can still utilize network processor encryption capabilities. For information on exceptions, see [“Exceptions to offloading requirements” on page 10](#).

Packet forwarding rates vary by the percentage of offloadable processing and the type of network processing required by your configuration, but are independent of frame size. For optimal traffic types, network throughput can equal wire speed.

Offloading requirements vary slightly by the model of the network processor.

This section includes the following topics:

- [Network processor models](#)
- [Offloading requirements](#)
- [Exceptions to offloading requirements](#)

## Network processor models

Many Fortinet products contain network processors. Some of these products contain NP1 network processors (also known as FortiAccel), while others contain NP2 network processors. Network processor features, and therefore offloading requirements, vary by network processor model. Differing offloading requirements are noted in [“Offloading requirements” on page 9](#) and [“Exceptions to offloading requirements” on page 10](#).

Some Fortinet products contain multiple network processors. Depending on the product, network processors may or may not be directly connected to each other on the circuit board through an EEI (Enhanced Extension Interface).

- Directly connected network processors have an EEI, and can pass traffic between them without involving the FortiGate unit's main processing resources.
- Indirectly connected network processors have no EEI, and *cannot* pass traffic between them without involving the FortiGate unit's main processing resources.

Sessions can only be offloaded if both the source and destination port are connected to the same network processor or directly (EEI) connected network processor pair.

[Table 1 on page 9](#) lists Fortinet products containing network processors, how many of each processor model are included in each network processor or EEI-connected network processor pair, and which ports share the network processor or EEI-connected network processor pair.

**Table 1: Network processors and their attached ports by Fortinet product**

Fortinet product	Network processors		Shared by ports
	#	Model	
FortiGate-5005FA2	1	NP1	Ports 7 & 8
FortiGate-5001FA2	1	NP1	Ports 1 & 2
FortiGate-3810A	1	NP1	Ports 9 & 10
FortiGate-3600A	1	NP1	Ports 9 & 10
FortiGate-1000AFA2	1	NP1	Ports A1 & A2
FortiGate-3016B	2	NP2	Ports 3-10
	2	NP2	Ports 11-18
FortiGate-310B	2	NP2	Ports 1-8
FortiGate-RTM-XB2	2	NP2	All ports (port number varies)
FortiGate-ADM-XB2	2	NP2	All ports
FortiGate-ADM-FB8	2	NP2	Ports 1-8
FortiGate-ASM-FB4	1	NP2	All ports



**Note:** For both NP1 and NP2 network processors, ports attached to a network processor cannot be used for firmware installation by TFTP.



**Note:** NP1 network processors do not support frames greater than 1500 bytes. If your network uses jumbo frames, you may need to adjust the MTU (Maximum Transmission Unit) of devices connected to NP1 ports.

## Offloading requirements

Offloading traffic to a network processor requires that the FortiGate unit configuration and the traffic itself is suited to hardware acceleration.

Sessions must be fast path ready. Fast path ready session characteristics are:

- Layer 2 type/length must be 0x0800 (IEEE 802.1q VLAN specification is supported); link aggregation between any network interfaces sharing the same network processor(s) may be used (IEEE 802.3ad specification is supported)
- Layer 3 protocol must be IPv4
- Layer 4 protocol must be UDP, TCP or ICMP
- Layer 3 / Layer 4 header or content modification must not require a session helper (for example, SNAT, DNAT, and TTL reduction are supported, but application layer content modification is not supported)
- FortiGate unit firewall policy must not require antivirus or IPS inspection
- origin must not be local host (the FortiGate unit)
- ingress and egress network interfaces are both attached to the same network processor(s)



**Note:** If you disable anomaly checks by Intrusion Prevention (IPS), you can still enable hardware accelerated anomaly checks. For details, see [“config system interface” on page 13](#).



**Note:** For session offloading to NP1 network processors, the session must not use an aggregated link or require QoS, including rate limits and bandwidth guarantees. Traffic shaping and link aggregation are not supported.

If a session is not fast path ready, the FortiGate unit will not send the session key to the network processor(s). Without the session key, all session key lookup by a network processor for incoming packets of that session fails, causing all session packets to be sent to the FortiGate unit's main processing resources, and processed at normal speeds.

If a session is fast path ready, the FortiGate unit will send the session key to the network processor(s). Session key lookup then succeeds for subsequent packets from the known session. Packets within the session must then also meet packet requirements.

- Incoming packets must not be fragmented.
- Outgoing packets must not require fragmentation to a size less than 385 bytes. Because of this requirement, the configured MTU (Maximum Transmission Unit) for network processors' network interfaces must also meet or exceed the network processors' supported minimum MTU of 385 bytes.

If packet requirements are not met, an individual packet will use FortiGate unit main processing resources, regardless of whether other packets in the session are offloaded to the specialized network processor(s).

In some cases, due to these requirements, a protocol's session(s) may receive a mixture of offloaded and non-offloaded processing.

For example, FTP uses two connections: a control connection and a data connection. The control connection requires a session helper, and cannot be offloaded, but the data connection does not require a session helper, and can be offloaded. Within the offloadable data session, fragmented packets will not be offloaded, but other packets will be offloaded.

## Exceptions to offloading requirements

Some traffic types differ from general offloading requirements, but still utilize some of the network processors' encryption and other capabilities. Exceptions include IPSec traffic and active-active high availability (HA) load balanced traffic.

### IPSec offloading requirements

Fortinet's specialized network processors contain features to improve IPSec tunnel performance. For example, network processors can encrypt and decrypt packets, reducing cryptographic load on the FortiGate unit's main processing resources.

Requirements for hardware accelerated IPSec encryption or decryption are a modification of general offloading requirements. Differing characteristics are:

- origin can be local host (the FortiGate unit)
- in Phase I configuration, Local Gateway IP must be specified as an IP address of a network interface for a port attached to a network processor
- SA must have been received by the network processor

- in Phase II configuration:
  - encryption algorithm must be DES, 3DES, AES-128, AES-192, AES-256, or null
  - authentication must be MD5, SHA1, or null
  - if encryption is null, authentication must not also be null
  - if replay detection is enabled, `enc-offload-antireplay` must also be `enable` in the CLI



**Note:** If replay detection is enabled in the Phase II configuration, you can enable or disable IPSec encryption and decryption offloading from the CLI. Performance varies by those CLI options and the percentage of packets requiring encryption or decryption. For details, see ["config system npu" on page 15](#).



**Note:** For session offloading to NP1 network processors, in Phase II configuration, the encryption algorithm must be 3DES and authentication must be MD5. Other encryption and authentication algorithms are not supported.

To apply hardware accelerated encryption and decryption, the FortiGate unit's main processing resources must first perform Phase I negotiations to establish the security association (SA). The SA includes cryptographic processing instructions required by the network processor, such as which encryption algorithms must be applied to the tunnel. After ISAKMP negotiations, the FortiGate unit's main processing resources send the SA to the network processor, enabling the network processor to apply the negotiated hardware accelerated encryption or decryption to tunnel traffic.

Possible accelerated cryptographic paths are:

- IPSec decryption offload
  - Ingress ESP packet > Offloaded decryption > Decrypted packet egress (fast path)
  - Ingress ESP packet > Offloaded decryption > Decrypted packet to FortiGate unit's main processing resources
- IPSec encryption offload
  - Ingress packet > Offloaded encryption > Encrypted (ESP) packet egress (fast path)
  - Packet from FortiGate unit's main processing resources > Offloaded encryption > Encrypted (ESP) packet egress

## HA active-active offloading requirements

Fortinet's specialized network processors can improve network performance in active-active (load balancing) high availability (HA) configurations, even though traffic deviates from general offloading patterns, involving more than one network processor, each in a separate FortiGate unit. No additional offloading requirements apply.

Once the primary FortiGate unit's main processing resources send a session key to its network processor(s), network processor(s) on the primary unit can redirect any subsequent session traffic to other cluster members, reducing traffic redirection load on the primary unit's main processing resources.

As subordinate units receive redirected traffic, each network processor in the cluster assesses and processes session offloading independently from the primary unit. Session key states of each network processor are not part of synchronization traffic between HA members.

For more information about active-active HA load balancing, see the [FortiGate HA Overview](#).

# Related CLI settings

Fortinet products containing specialized network processors have associated CLI settings related to configuring network processor specific functionality.

If the FortiGate unit itself does not contain a network processor, but can receive an AMC (Advanced Mezzanine Card) module, installing an AMC that contains a network processor, such as a FortiGate-ASM-FB4 module, causes network processor settings to appear in the CLI.

Settings in this chapter apply to FortiOS v3.0 MR5 and MR6.

This section includes the following topics:

- [config system interface](#)
- [config system npu](#)

## config system interface

Network interfaces associated with a port attached to a network processor can be configured to use hardware acceleration to drop or allow certain anomaly types, separately from and in advance of any anomaly checks specified by Intrusion Prevention (IPS). Configured behavior applies separately to each of these network interfaces.

### Syntax

```
config system interface
edit <name_str>
    set fp-anomaly {drop_icmpland | pass_icmpland}
    {drop_ipland | pass_ipland} {drop_iplsrr | pass_iplsrr}
    {drop_iprr | pass_iprr} {drop_ipsecurity |
pass_ipsecurity} {drop_ipssrr | pass_ipssrr}
    {drop_ipstream | pass_ipstream} {drop_iptimestamp |
pass_iptimestamp} {drop_ipunknown_option |
pass_ipunknown_option} {drop_unknown_prot |
pass_ipunknown_prot} {drop_tcpland | pass_tcpland}
    {drop_udpland | pass_udpland} {drop_winnuke |
pass_winnuke}
end
```

Variables	Description	Default
<pre>fp-anomaly {drop_icmpland   pass_icmpland} {drop_ipland   pass_ipland} {drop_iplsrr   pass_iplsrr} {drop_iprr   pass_iprr} {drop_ipsecurity   pass_ipsecurity} {drop_ipssrr   pass_ipssrr} {drop_ipstream   pass_ipstream} {drop_iptimestamp   pass_iptimestamp} {drop_ipunknown_o ption   pass_ipunknown_op tion} {drop_unknown_pro t   pass_ipunknown_pr ot} {drop_tcpland   pass_tcpland} {drop_udpland   pass_udpland} {drop_winnuke   pass_winnuke}</pre>	<p>By configuring this option, enable hardware anomaly checking, and list whether to drop or allow (pass) specific anomaly types.</p> <ul style="list-style-type: none"> <li>• drop_icmpland: Drop ICMP land.</li> <li>• pass_icmpland: Allow ICMP land to pass.</li> <li>• drop_ipland: Drop IP land.</li> <li>• pass_ipland: Allow IP land to pass.</li> <li>• drop_iplsrr: Drop IP with loose source record route option.</li> <li>• pass_iplsrr: Allow IP with loose source record route option to pass.</li> <li>• drop_iprr: Drop IP with record route option.</li> <li>• pass_iprr: Allow IP with record route option to pass.</li> <li>• drop_ipsecurity: Drop IP with security option.</li> <li>• pass_ipsecurity: Allow IP with security option to pass.</li> <li>• drop_ipssrr: Drop IP with strict source record route option.</li> <li>• pass_ipssrr: Allow IP with strict source record route option to pass.</li> <li>• drop_ipstream: Drop IP with stream option.</li> <li>• pass_ipstream: Allow IP with stream option to pass.</li> <li>• drop_iptimestamp: Drop IP with timestamp option.</li> <li>• pass_iptimestamp: Allow IP with timestamp option to pass.</li> <li>• drop_ipunknown_option: Drop IP with unknown option.</li> <li>• pass_ipunknown_option: Allow IP with unknown option to pass.</li> <li>• drop_ipunknown_prot: Drop IP with unknown protocol.</li> <li>• pass_ipunknown_prot: Allow IP with unknown protocol to pass.</li> <li>• drop_tcpland: Drop TCP land.</li> <li>• pass_tcpland: Allow TCP land to pass.</li> <li>• drop_winnuke: Drop TCP WinNuke.</li> <li>• pass_winnuke: Allow TCP WinNuke to pass.</li> <li>• drop_udpland: Drop UDP land.</li> <li>• pass_udpland: Allow UDP land to pass.</li> </ul> <p>Separate each anomaly's option with a space. To add or remove an option from the list, completely retype the new list.</p> <p>When no options are specified, anomaly checking performed by the network processor is disabled. If pass options are specified, packets may still be rejected by other anomaly checks, including policy-required IPS performed using the FortiGate unit's main processing resources.</p> <p>Log messages are generated when packets are dropped due to options in this setting.</p>	<p>No options specified (disabled).</p>

## Example

You might configure a FortiGate-ASM-FB4 module to drop packets with TCP WinNuke or unknown IP protocol anomalies, but to pass packets with an IP time stamp, using hardware acceleration provided by the network processor.

```
config system interface
  edit AMC-SW1/1
    set fp-anomaly drop_winnuke drop_ipunknown_prot
    pass_iptimestamp
  end
```

## config system npu

Network processing unit (npu) settings configure offloading behavior for IPSec VPN and traffic shaping. Configured behavior applies to all network processors contained by the FortiGate unit itself or any installed AMC modules.

### Syntax

```
config system npu
  set enc-offload-antireplay {enable | disable}
  set dec-offload-antireplay {enable | disable}
  set offload-ipsec-host {enable | disable}
  set traffic-shaping-mode {bidirection | unidirection}
end
```

Variables	Description	Default
enc-offload-antireplay {enable   disable}	Enable or disable offloading of IPSec encryption. This option is used only when replay detection is enabled in Phase II configuration. If replay detection is disabled, encryption is always offloaded.	disable
dec-offload-antireplay {enable   disable}	Enable or disable offloading of IPSec decryption. This option is used only when replay detection is enabled in Phase II configuration. If replay detection is disabled, decryption is always offloaded.	enable

Variables	Description	Default
offload-ipsec-host {enable   disable}	Enable or disable offloading of IPsec encryption of traffic from local host (FortiGate unit). <b>Note:</b> For this option to take effect, the FortiGate unit must have previously sent the security association (SA) to the network processor. For details on SA offloading, see <a href="#">“IPSec offloading requirements” on page 10</a> .	disable
traffic-shaping-mode {bidirection   unidirection}	Select the offloaded traffic shaping bandwidth calculation method. <ul style="list-style-type: none"> <li><b>unidirection:</b> The bandwidth limit applies per direction. For example, a unidirectional limit of 10 KBps would result in an overall limit of 20 KBps — 10 KBps per direction.</li> <li><b>bidirection:</b> The bandwidth limit applies to both directions overall. For example, a bidirectional limit of 10 KBps would result in an overall limit of 10 KBps — 5 KBps per direction.</li> </ul> This option applies only if the FortiGate unit itself or any installed AMC modules contain a network processor that supports offloading of traffic shaping.	Varies by model.

## Example

You could configure the traffic shaping limit to be applied as a bidirectional total limit during hardware accelerated sessions.

```
config system npu
    set traffic-shaping-mode bidirection
end
```

# Examples

Hardware accelerated IPsec processing, involving either partial or full offloading, can be achieved in either tunnel or interface mode IPsec configurations.

To achieve offloading for both encryption and decryption:

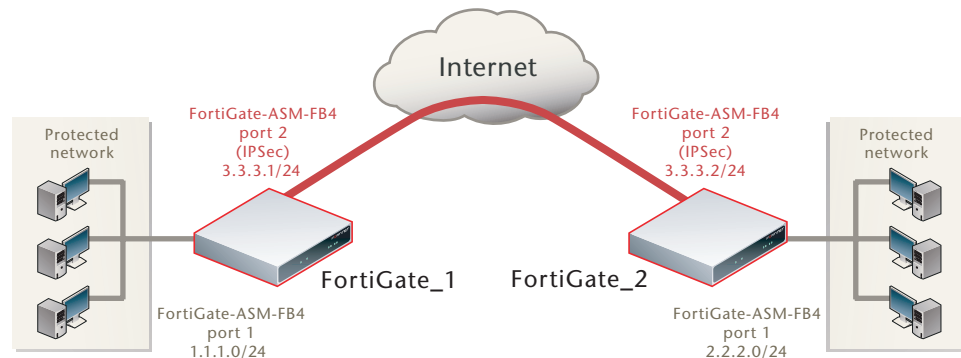
- In Phase I configuration's Advanced section, Local Gateway IP must be specified as an IP address of a network interface associated with a port attached to a network processor. (In other words, if Phase 1's Local Gateway IP is Main Interface IP, or is specified as an IP address that is not associated with a network interface associated with a port attached to a network processor, IPsec network processing is not offloaded.)
- In Phase II configuration's P2 Proposal section, if the checkbox "Enable replay detection" is enabled, `enc-offload-antireplay` and `dec-offload-antireplay` must be set to `enable` in the CLI.
- `offload-ipsec-host` must be set to `enable` in the CLI.

This section contains example IPsec configurations whose IPsec encryption and decryption processing is hardware accelerated by FortiGate-ASM-FB4 modules. [Figure 1](#) illustrates the example network topology. [Table 2](#) lists the example network interfaces and IP addresses.



**Note:** Hardware accelerated IPsec does not require both tunnel endpoints to have the same network processor model. However, if hardware is not symmetrical, the packet forwarding rate is limited by the slower side.

**Figure 1: Example network topology for offloaded IPsec processing**



**Table 2: Example ports and IP addresses for offloaded IPsec processing**

	FortiGate_1		FortiGate_2	
	Port	IP	Port	IP
<b>IPSec tunnel</b>	FortiGate-ASM-FB4 port 2	3.3.3.1/24	FortiGate-ASM-FB4 port 2	3.3.3.2/24
<b>Protected network</b>	FortiGate-ASM-FB4 port 1	1.1.1.0/24	FortiGate-ASM-FB4 port 1	2.2.2.0/24

This section includes the following topics:

- [Accelerated tunnel mode IPSec](#)
- [Accelerated interface mode IPSec](#)

## Accelerated tunnel mode IPSec

The following steps create a hardware accelerated tunnel mode IPSec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

### To configure hardware accelerated tunnel mode IPSec

- 1 On FortiGate\_1, go to **VPN > IPSec**.
- 2 Configure Phase I.  
For tunnel mode IPSec and for hardware acceleration, specifying the Local Gateway IP is required.  
Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate\_2's FortiGate-ASM-FB4 module port 2.
- 3 Configure Phase II.  
If you enable the checkbox "Enable replay detection," set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see "[config system npu](#)" on page 15.
- 4 Go to **Firewall > Policy**.
- 5 Configure one policy to apply the Phase 1 IPSec tunnel you configured in step 2 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.
- 6 Go to **Router > Static**.
- 7 Configure a static route to route traffic destined for FortiGate\_2's protected network to VPN IP address of FortiGate\_2's VPN gateway, 3.3.3.2, through the FortiGate-ASM-FB4 module's port 2 (device).

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "AMC-SW1/2"
    set dst 2.2.2.0 255.255.255.0
    set gateway 3.3.3.2
  next
end
```

- 8 On FortiGate\_2, go to **VPN > IPSec**.
- 9 Configure Phase I.  
For tunnel mode IPSec and for hardware acceleration, specifying the Local Gateway IP is required.  
Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate\_1's FortiGate-ASM-FB4 module port 2.

- 10 Configure Phase II.  
If you enable the checkbox “Enable replay detection,” set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see [“config system npu” on page 15](#).
- 11 Go to **Firewall > Policy**.
- 12 Configure one policy to apply the Phase 1 IPsec tunnel you configured in step 9 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.
- 13 Go to **Router > Static**.
- 14 Configure a static route to route traffic destined for FortiGate\_1’s protected network to VPN IP address of FortiGate\_1’s VPN gateway, 3.3.3.1, through the FortiGate-ASM-FB4 module’s port 2 (device).  
You can also configure the static route using the following CLI commands:
 

```
config router static
edit 2
set device "AMC-SW1/2"
set dst 1.1.1.0 255.255.255.0
set gateway 3.3.3.1
next
end
```
- 15 Activate the IPsec tunnel by sending traffic between the two protected networks.  
To verify tunnel activation, go to **VPN > IPSEC > Monitor**.

## Accelerated interface mode IPsec

The following steps create a hardware accelerated interface mode IPsec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

### To configure hardware accelerated interface mode IPsec

- 1 On FortiGate\_1, go to **VPN > IPsec**.
- 2 Configure Phase I.  
For interface mode IPsec and for hardware acceleration, the following settings are required.
  - Select Advanced.
  - Enable the checkbox “Enable IPsec Interface Mode.”
  - In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate\_2’s FortiGate-ASM-FB4 module port 2.
- 3 Configure Phase II.  
If you enable the checkbox “Enable replay detection,” set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see [“config system npu” on page 15](#).
- 4 Go to **Firewall > Policy**.

- 5 Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 2 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.
- 6 Go to **Router > Static**.
- 7 Configure a static route to route traffic destined for FortiGate\_2's protected network to the Phase 1 IPsec device, FGT\_1\_IPsec.

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_1_IPsec"
    set dst 2.2.2.0 255.255.255.0
  next
end
```

- 8 On FortiGate\_2, go to **VPN > IPsec**.
- 9 Configure Phase I.

For interface mode IPsec and for hardware acceleration, the following settings are required.

- Enable the checkbox "Enable IPsec Interface Mode."
- In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate\_1's FortiGate-ASM-FB4 module port 2.

- 10 Configure Phase II.

If you enable the checkbox "Enable replay detection," set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see ["config system npu" on page 15](#).

- 11 Go to **Firewall > Policy**.
- 12 Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 9 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.
- 13 Go to **Router > Static**.
- 14 Configure a static route to route traffic destined for FortiGate\_1's protected network to the Phase 1 IPsec device, FGT\_2\_IPsec.

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_2_IPsec"
    set dst 1.1.1.0 255.255.255.0
  next
end
```

- 15 Activate the IPsec tunnel by sending traffic between the two protected networks. To verify tunnel activation, go to **VPN > IPSEC > Monitor**.

# Index

## Numerics

3DES 11

## A

active-active HA 5, 10, 11  
 AES-128 11  
 AES-192 11  
 AES-256 11  
 aggregation, link 9, 10  
 AMC (Advanced Mezzanine Card) 5, 7, 13  
 anomaly  
   checks 13, 14  
   drop 14  
   hardware checks 13, 14  
   IPS checks 13, 14  
   pass 14  
 antireplay 11, 15, 17, 18, 19, 20  
 antivirus 9

## B

bandwidth  
   calculation method 16  
   limitation 16  
 bandwidth guarantees 10  
 bidirection 16

## C

CLI 13, 17  
 cluster member 11  
 comments, documentation 6  
 CPU 5  
 cryptographic load 10

## D

decryption 15, 17, 18, 19, 20  
 DES 11  
 DNAT 9  
 documentation  
   commenting on 6  
   Fortinet 6  
 drop anomaly 14

## E

EEl (Enhanced Extension Interface) 8  
 encryption 15, 16, 17, 18, 19, 20  
 ESP 11  
 example IPSec configurations 17

## F

fast path 5  
   required session characteristics 9  
 firmware install 9  
 FortiAccel 8  
 FortiAnalyzer traffic reports 7  
 FortiASIC 5  
 FortiGate documentation  
   commenting on 6  
 FortiGate-1000AFA2 9  
 FortiGate-3016B 9  
 FortiGate-310B 9  
 FortiGate-3600A 9  
 FortiGate-3810B 9  
 FortiGate-5001FA2 9  
 FortiGate-5005FA2 9  
 FortiGate-ADM-FB8 9  
 FortiGate-ADM-XB2 9  
 FortiGate-ASM-FB4 9, 17  
 FortiGate-RTM-XB2 9  
 Fortinet documentation 6  
 Fortinet Knowledge Center 6  
 fragmented packets 10  
 frame size 8  
 frame size, maximum 9  
 FTP 5, 10

## H

high availability (HA) 11  
   active-active 5, 10  
   load balancing 10

## I

ICMP land 14  
 IEEE 802.1q 9  
 IEEE 802.3ad 9  
 interface mode 19  
 interface mode IPSec 17  
 introduction  
   Fortinet documentation 6  
 Intrusion Prevention 13  
 Intrusion Prevention System (IPS) 9, 13, 14  
 IP land 14  
 IPSec 5, 7, 8, 10, 15, 16, 17, 18, 19  
   interface mode 17  
   tunnel 10  
   tunnel mode 17  
 IPSec Interface Mode 17, 19, 20  
 IPv4 9  
 ISAKMP 11

**J**

jumbo frames 9

**L**

latency 5  
 Layer 2 9  
 Layer 3 9  
 Layer 4 9  
 link aggregation 9, 10  
 load balancing 5, 10, 11  
 Local Gateway IP 10, 17, 18, 19, 20  
 local host 9, 10, 16  
 log messages 14  
 loose source record route 14

**M**

Main Interface IP 17  
 main processing resources 5  
 master unit 11  
 maximum frame size 9  
 MD5 11  
 MTU (Maximum Transmission Unit) 9, 10

**N**

network  
   performance 5  
   topology 17  
 network processing unit (NPU) 15  
 NP1 8, 9, 10, 11  
 NP2 8, 9

**P**

P2 Proposal 17  
 P2P 5  
 packet  
   forwarding rate 7, 8, 17  
   processing flow 7  
   small 5  
 pass anomaly 14  
 Phase 1 11, 17, 18, 19, 20  
 Phase 2 11, 15, 17, 18, 19, 20  
 policy 9  
 ports, attached to network processors 9  
 primary unit 11

**Q**

QoS 10, 16

**R**

RAM 5  
 rate limits 10  
 record route option 14  
 replay detection 11, 15, 17, 18, 19, 20  
 route 18, 19, 20

**S**

security association (SA) 7, 11, 16  
 security option 14  
 session  
   key 7  
   lifetime 5  
 SHA1 11  
 slave unit 11  
 small packets 5  
 SNAT 9  
 static route 18, 19, 20  
 stream option 14  
 streaming multimedia 5  
 strict source record route 14

**T**

TCP land 14  
 TCP WinNuke 14, 15  
 TFTP 9  
 timestamp option 14  
 topology 17  
 traffic shaping 10, 16  
 traffic statistics 7  
 TTL reduction 9  
 tunnel mode 18  
 tunnel mode IPsec 17

**U**

UDP land 14  
 unidirection 16  
 unknown option 14  
 unknown protocol 14

**V**

VLAN 9  
 voice over IP (VoIP) 5  
 VPN 5, 15  
   configuration 5  
   gateway 18, 19

**W**

wire speed 8

**F**ORTINET™

[www.fortinet.com](http://www.fortinet.com)

**F**ORTINET™

[www.fortinet.com](http://www.fortinet.com)