



# **FORCEPOINT**

## **Sidewinder**

**Release Notes**

**8.3.2P12**

**Revision A**

## Contents

- [About this release](#) on page 2
- [Resolved issues](#) on page 6
- [Installation notes](#) on page 9
- [Known issues](#) on page 10
- [Find product documentation](#) on page 10

# About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

Forcepoint Sidewinder version 8.3.2P12 resolves issues present in the previous release.

## Supported firewall types

Sidewinder supports these firewall types.

- Forcepoint Sidewinder appliances
- Forcepoint Sidewinder, Virtual Appliance
- Forcepoint Sidewinder on Crossbeam X-Series Platforms

These features are not supported on Crossbeam X-Series Platforms for this release:

- Forcepoint Sidewinder Admin Console



**Note:** Use a Forcepoint Sidewinder Control Center Management Server to manage Sidewinder on Crossbeam X-Series Platforms.

- Multicast dynamic routing using the PIM-SM protocol
- Hybrid mode (configuring standard and transparent mode on the same firewall)
- Default route failover
- Quality of Service (QoS)
- Transparent (bridged) mode for these configurations:
  - Dual-Box High Availability (DBHA)
  - Multi-application serialization
- DBHA active-active mode



**Note:** Active-standby DBHA is supported.

- Crossbeam X-Series Operating System (XOS) features:
  - Virtual Application Processor (VAP) group hide-vlan-header parameter

- Equal-cost multi-path routing
- Configuration of the VRRP MAC address



**Note:** If you need functionality similar to the VRRP MAC address, Crossbeam recommends configuring a user-defined MAC address on each traffic circuit/interface pair included in the VRRP failover group. See the Crossbeam support knowledge base article 0004069.

## Compatible products

Sidewinder is compatible with the following products.

- McAfee® Firewall Enterprise ePolicy Orchestrator® Extension
- Forcepoint Sidewinder Control Center
- McAfee® Logon Collector
- McAfee Endpoint Intelligence Agent (McAfee EIA)

For more information, see Knowledge Base article [9275](#) and the Technical Note *Using Firewall Enterprise with other McAfee products* at <https://support.forcepoint.com>.

## Requirements

Before you install this version, make sure the Admin Console and Sidewinder requirements are met.

### Admin Console requirements

The computer that hosts the Admin Console must meet these requirements.

#### Admin Console minimum requirements


Component	Requirements
Operating system	<p>One of these Microsoft operating systems:</p> <ul style="list-style-type: none"> <li>• Windows Server 2008</li> <li>• Windows 7</li> <li>• Windows 8</li> <li>• Windows 10</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported.</p> </div> <p>Compatible legacy Microsoft operating systems:</p> <ul style="list-style-type: none"> <li>• Windows Vista</li> </ul>
Web browser	<p>One of the following:</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer, version 7 or later</li> <li>• Mozilla Firefox, version 1.0 or later</li> </ul>

Component	Requirements
Hardware	<ul style="list-style-type: none"> <li>• 2 GHz x86-compatible processor</li> <li>• 2 GB of memory</li> <li>• 300 MB of available disk space</li> <li>• CD drive</li> <li>• 1024 x 768 display</li> <li>• Network card (to connect to your firewall)</li> <li>• USB port</li> </ul>

## Sidewinder requirements

The firewall must meet these requirements.

### Minimum requirements by type

Firewall type	Platform requirements
Sidewinder appliance	<p>Appliance with a valid support contract:</p> <ul style="list-style-type: none"> <li>• 1 GB of memory</li> <li>• AMD64-compatible processor</li> </ul>
Sidewinder, Virtual Appliance	<p>Virtualization server:</p> <ul style="list-style-type: none"> <li>• <b>Hypervisor operating system</b> — VMware ESX/ESXi version 4.0 or later</li> </ul> <div data-bbox="555 1077 610 1131" style="float: left; margin-right: 10px;">  </div> <div data-bbox="649 1089 1440 1247" style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note:</b> Sidewinder, Virtual Appliance is installed in 64-bit mode by default. Your system must support Intel VT technology (or equivalent) to run properly in a virtual environment. Before starting the virtual appliance, verify that VT is enabled in your computer BIOS.</p> </div> <ul style="list-style-type: none"> <li>• <b>Hardware resources:</b> <ul style="list-style-type: none"> <li>• 2 virtual processors</li> <li>• AMD64-compatible processor</li> <li>• 1 GB of memory</li> <li>• 30 GB of free disk space</li> <li>• 2 or more NICs of type e1000</li> </ul> </li> <li>• <b>Internet connectivity</b> — The firewall requires a persistent Internet connection to maintain an active license and full functionality.</li> </ul>

Firewall type	Platform requirements
Forcepoint Sidewinder on Crossbeam X-Series Platforms	<p>Crossbeam X-Series Platform:</p> <ul style="list-style-type: none"> <li>• <b>Chassis</b> — X50, X60, or X80-S</li> <li>• <b>XOS version</b> — 9.6.5 and later, 9.7.1 and later, 9.9.x, or 10.0</li> <li>• <b>Application Processor Module</b> — APM-50 or APM-9600 <ul style="list-style-type: none"> <li>• At least one local disk (RAID 0 and RAID 1 disk configurations are supported; two-disk, non-RAID configurations are not supported)</li> <li>• 12 GB of memory (minimum)</li> </ul> </li> <li>• <b>Network Processor Module</b> — NPM-50, NPM-86x0, or NPM-96x0</li> <li>• <b>CBI package</b> — MFE-8.3.2-9.mr1.cbi</li> </ul>

## McAfee EIA requirements

Systems must meet these requirements to install McAfee EIA.

### McAfee EIA minimum requirements

Component	Requirements
Operating system	<p>One of these 32-bit or 64-bit Microsoft operating systems:</p> <ul style="list-style-type: none"> <li>• Windows 8.1</li> <li>• Windows 7</li> <li>• Windows XP Service Pack 2 and later</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008</li> <li>• Windows Server 2003 Service Pack 1 and later</li> <li>• Windows Server 2003 R2 Service Pack 1 and later</li> </ul>
Hardware	<ul style="list-style-type: none"> <li>• 2 GHz x86-compatible processor</li> <li>• 2 GB of memory</li> <li>• 300 MB of available disk space</li> <li>• 1024 x 768 display</li> <li>• Network card (to connect to your firewall)</li> <li>• One of the following: <ul style="list-style-type: none"> <li>• USB port</li> <li>• CD drive</li> </ul> </li> </ul>
Other products	<p>McAfee EIA deployment requires:</p> <ul style="list-style-type: none"> <li>• McAfee® Endpoint Intelligence Manager (McAfee EIM) version 2.2.0 and later</li> <li>• McAfee® ePolicy Orchestrator® (McAfee ePO™) version 4.6.5, 5.x, and later</li> <li>• McAfee® Agent Agent version 4.8.0 patch 2 and later</li> </ul>

# Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

## Common Vulnerabilities and Exposures (CVEs)

### BIND

- Upgrades BIND to version 9.11.13.
- Imports fixes for the following CVEs:

```
CVE-2019-6477, CVE-2019-6471, CVE-2018-5743, CVE-2018-5744, CVE-2018-5745,  
CVE-2019-6465, CVE-2018-5741, and CVE-2018-5740.
```

(1115674, 1115398, 1115338, 1115292, 1115414, and 1115085)

### DHCP

- Upgrades DHCP to version 4.4.1
- Import fixes for CVE-2018-5732. (1115654)

### Kernel

- Imports fixes for the following CVEs:

```
CVE-2018-6916, CVE-2018-6918, CVE-2018-6922, CVE-2018-6924, CVE-2017-1082,  
CVE-2018-17156, CVE-2019-5606, CVE-2019-5608, CVE-2019-5610, CVE-2019-5611.
```

(1114865, 1114895, 1115056, 1115299, 1115423, 1115457, 1115522, 1115520, 1115519, 1115520, and 1115519)

Sidewinder is not vulnerable to CVE-2019-5610. The fix is included for maintenance purposes.

### libarchive

- Upgrades to libarchive version 3.4.1.
- Import fixes for the following CVEs:

```
CVE-2018-1000877, CVE-2018-1000878, CVE-2018-1000879, CVE-2018-1000880, CVE-2019-1000019,  
CVE-2019-1000020, CVE-2019-18408, and CVE-2019-19221.
```

(1115189, 1115219, 1115667, and 1115721)

### NTP

- Upgrades to NTP version 4.2.8p13.
- Imports fixes for the following CVEs:

```
CVE-2019-8936 and CVE-2018-12327.
```

(1115359 and 1114995)

### OpenSSH

- Upgrades to OpenSSH version 8.0p1.
- Imports fixes for the following CVEs:

```
CVE-2018-15473, CVE-2018-20685, CVE-2019-6109, and CVE-2019-6111.
```

(1115081, 1115206, 1115227, and 1115401)

### OpenSSL

- Upgrades to OpenSSL version 1.0.2u.
- Imports fixes for the following CVEs:

```
CVE-2019-1551, CVE-2018-0734, CVE-2018-5407, CVE-2019-1559, CVE-2018-0732,  
CVE-2018-0737, CVE-2019-1547, CVE-2019-1552, and CVE-2019-1563.
```

(1115790, 1115280, 1115321, 1115322, 1114991, 1115507, 1115538, and 1115542)

### Python

- Imports fixes for the following CVEs:

```
CVE-2018-1060 and CVE-2018-1061.
```

(1114997)

### qsrt

- Imports fixes for CVE-2017-1082. (1115299)

### Quagga

- Imports fixes for the following CVEs:

```
CVE-2016-4049, CVE-2017-5495, CVE-2017-16227, CVE-2018-5378, CVE-2018-5379,  
CVE-2018-5380, and CVE-2018-5381.
```

(1114053, 1114368, 1114723, 1114846)

### Tcpdump

- Upgrades to tcpdump version 4.9.3.
- Upgrades to libpcap version 1.9.1.
- Imports fixes for the following CVEs:

```
CVE-2018-10103, CVE-2018-10105, CVE-2018-14461, CVE-2018-14462, CVE-2018-14463,  
CVE-2018-14464 CVE-2018-14465 CVE-2018-14466 CVE-2018-14467 CVE-2018-14468 CVE-2018-14469,  
CVE-2018-14470 CVE-2018-14879 CVE-2018-14880 CVE-2018-14881 CVE-2018-14882 CVE-2018-16227,  
CVE-2018-16228 CVE-2018-16229 CVE-2018-16230 CVE-2018-16300 CVE-2018-16301 CVE-2018-16451,  
and CVE-2018-16452.
```

(1115602, 1115603, 1115606, 1115608, 1115609, 1115612, 1115613, 1115616, 1115617, 1115620, 1115621, 1115624, 1115625, 1115628, 1115629, 1115632, 1115633, 1115636, 1115637, 1115640, 1115641, 1115644, 1115645, and 1115648)

### zsh

- Upgrades to zsh version 5.7.1.
- Imports fixes for the following CVEs:

```
CVE-2014-10070, CVE-2014-10071, CVE-2014-10072, CVE-2016-10714, CVE-2017-18205,  
CVE-2017-18206, CVE-2018-0502, CVE-2018-1071, CVE-2018-1083, CVE-2018-1100, CVE-2018-13259,  
CVE-2018-7548, and CVE-2018-7549.
```

(1114856, 1114866, 1114879, 1114903, and 1115093)

## General Maintenance Changes

---

### ACL

- Increases the size of acl'd's cache for domain objects. (1115791)

- Adds a tunable time-to-live for the host cache, and check for daemon pings in large loops. (1115791 1115833)

### **Admin Console**

- Adds NTP copyright and license to the **Help > About** screen. (1115381)
- Upgrades OpenSSL in the Admin Console. (1115431)

### **Antivirus**

- Corrects an issue that would cause the McAfee scanner to unexpectedly block some files. (1115005)

### **Audit**

- Improves memory management in auditdbd. (1115111)
- Fixes the spelling of sysctl net.inet.ip.maxfragsperpacket in audit messages. (1115046)

### **BIND**

- Supplies 64-bit versions of the DNS utilities dig, host, and nslookup. (1115291)
- Corrects the operation of the ipv6\_transport option. (1115487)

### **Certificate management**

- Updates the list of Trusted Internet CAs with a new list from Mozilla. (1114802)
- Corrects an issue with cf cert view when a state field is missing from the backend database. (1115436)

### **entrelayd**

- Corrects an issue which could cause entrelayd to utilize high CPU cycles. (1114929)

### **High Availability**

- Adds prioritization to faild debug audits. (1115466)

### **IKE**

- Corrects an issue with multiple rekeys on a single VPN simultaneously. (1115086)

### **Kernel**

- Avoids packet loss from expiring ARP entries by making sure that ARP entries used from a cache are refreshed before they expire. (1115097)
- Improves IPv6 packet length processing. (1114213)
- Improves IPv6 input processing. (1115413)
- Fixes a memory leak in IPS. (1115382)

### **Package management**

- Corrects an issue where uninstalling a patch would incorrectly change the status of patches that it made obsolete. (1114964)
- Removes a warning about /vcdrom/packages/upscripts when running "cf package autoremove". (1114965)

### **Passport**

- Corrects several issues and improves auditing in the SSO daemon. (1115021)
- Improves error handling in the NTLM authentication warder. (1115185)

### **Proxies**

- Allows body with the HTTP PATCH method. (1115339)
- Addresses errors seen in the HTTP proxy when antivirus is enabled. (1115075)
- Addresses errors seen when closing a SOCKS5 proxy connection before it is fully set up. (1115121)
- Improves memory management in the proxies. (1115122 1115078 1115075)
- Improves error reporting in App ID. (1115209)



- Corrects an auditing issue in the HTTP proxy. (1115185)
- Corrects a memory issue encountered when using SSL decrypt/re-encrypt. (1114919)
- Improves header processing in the HTTP proxy. (1115001)
- Fixes an authentication error associated with not finding the default warder. (1115399)
- Corrects a memory management issue encountered when using HTTP proxy decrypt/re-encrypt. (1115451)
- Fixes a problem with the non-transparent FTP proxy and includes some antivirus updates. (1115787)

#### Sendmail

- Changes the sendmail default for Diffie-Hellman (DH) from 1024 to 2048 bits. (1114979)
- Sets the sendmail default for max processes to 50. (1114962)

#### Smartfilter

- Changes the default SmartFilter URL to [sflist.sidewinder.downloads.forcepoint.com](https://sflist.sidewinder.downloads.forcepoint.com). (1115004)

#### SNMP

- Improves the reporting of interface operational status via SNMP. (1115159)
- Changes the SNMP agent versionConfigureOptions MIB definition to align with net-snmp.org MIB definition. (1115144)

#### Miscellaneous

- Removes the ability to configure SSLv2, 40-bit, and 56-bit cipher choices from the Admin Console and cf. Support for SSLv2, 40-bit, and 56-bit ciphers was previously removed in 8.3.2P09. (1114986 1115277)
- Updates the End User License Agreement. (1115114 1115425 1115672)
- Updates the Forcepoint Copyright year to 2020. (1115426)
- Increases the default data size to 2GB in /boot/loader.conf. (1115467)

## Installation notes

To bring your firewall to the latest patch version, follow the patch installation process appropriate for your environment.

### Before you begin

The firewall must have 8.3.2P03 and 8.3.2P10 installed.

- **Standalone or HA cluster** — See the *Forcepoint Sidewinder Product Guide*, version 8.3.2P03 and later.
- **Firewall or HA cluster managed by Control Center** — See the *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2P02 and *Forcepoint Sidewinder Control Center Product Guide*, version 5.3.2.



**Note:** If your firewall is managed by Control Center, it must be at version 5.3.2P02 or later to manage firewalls at version 8.3.2P03 or later.

- **Crossbeam X-Series Platforms firewall** — See the *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x.

# Known issues

---

For a list of known issues in this product release, see Knowledge Base article [9764](#).

# Find product documentation

---

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

## Product documentation

---

Every Forcepoint product has a comprehensive set of documentation.

Sidewinder documentation includes:

### Typical documents

- *Forcepoint Sidewinder Product Guide*
- *Forcepoint Sidewinder Release Notes*
- *Forcepoint Sidewinder Command Line Interface Reference Guide*
- *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*
- *Technical Note — Using Firewall Enterprise with other McAfee products*
- *Application Note — Configuring Department of Defense Common Access Card Authentication on Firewall Enterprise*

### Hardware

- *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*
- *Forcepoint Sidewinder, Virtual Appliance Installation Guide*
- *Forcepoint Sidewinder, Virtual Appliance Evaluation for Desktop Installation Guide*
- *Forcepoint Sidewinder Quick Start Guide*
- *Forcepoint Sidewinder Hardware Guide*, models S4016, 1402-C3, S5032, S6032, and S7032
- *Forcepoint Sidewinder Hardware Guide*, models S1104, S2008, and S3008

### Certification

- *Firewall Enterprise Common Criteria Evaluated Configuration Guide*
- *Firewall Enterprise FIPS 140-2 Configuration Guide*
- *Firewall Enterprise FIPS 140-2 Level 2 Kit Installation Guide*, S models

Contact [opensource@forcepoint.com](mailto:opensource@forcepoint.com) if you need access to the modified BIND or DHCP source code, per the ISC/Mozilla license agreement.

