



# **FORCEPOINT**

## **Sidewinder**

**Release Notes**

**8.3.2P11**

**Revision A**

## Contents

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

# About this release

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

Forcepoint Sidewinder version 8.3.2P11 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.

**Table 1: 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.

**Table 2: 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 style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin: 5px 0;"> <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.

**Table 3: 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

- Imports a fix for CVE-2017-3145. See Knowledge Base article [15080](#) for more information. (1114801)

### FreeBSD

- Imports fixes for the following CVEs:

CVE-2016-1880, CVE-2016-1881, CVE-2016-1883, CVE-2016-1888, and CVE-2016-1889.

(1114396)

### Kernel

- Tightens defenses against the Meltdown attack, CVE-2017-5754. This change also mitigates CVE-2017-5715 and CVE-2017-5753.

This change prevents execution of programs not published by Forcepoint by disallowing binaries of the type "scrp" from being executed, which a rogue administrator (Admn) could have done previously. Scripts are still allowed with the type "scrp".

This change also provides detection of a Meltdown attack in progress, killing the offending program and auditing that the attack occurred. This change has no performance impact. See Knowledge Base article [14992](#) for more information. (1114777)

- Imports a fix for CVE-2017-1086. (1114736)

### NTP

- Upgrades NTP to version 4.2.8p11.
- Imports fixes for the following CVEs:

CVE-2016-1549, CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, and CVE-2018-7185.

(1114851)

### OpenSSH

- Imports a fix for CVE-2017-15906. (1114724)

### OpenSSL

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

CVE-2016-8610, CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2018-0733, and CVE-2018-0739.

See Knowledge Base article [14990](#) and Knowledge Base article [15825](#) for more information. (1114729, 1114734, 1114741, 1114821, and 1114885)

### Tcpdump

- Upgrades to tcpdump version 4.9.2.

- Imports fixes for the following CVEs:

```
CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-11544, CVE-2017-11545,
CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898,
CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986,
CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992,
CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998,
CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004,
CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010,
CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016,
CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022,
CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028,
CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034,
CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040,
CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046,
CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052,
CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689,
CVE-2017-13690, CVE-2017-13725, and CVE-2017-16808.
```

(1114588, 1114604, 1114669, 1114670, 1114671, 1114672, 1114673, 1114679, and 1114743)

## General Maintenance Changes

### Admin Console

- Upgrades OpenSSL in the Admin Console. (1114658)

### BIND

- Upgrades BIND to version 9.11.2-P1. (1114747, 1114797, and 1114891)
- Fixes named-internet error connecting to zone not allowed. (1114908)

### Certificate management

- Implements performance improvements in the cert command. (1114425)
- Updates the list of Trusted Internet Certificate Authorities (CAs) with a new list from Mozilla. (1114558)

### cf\_interface

- Fixes cf interface errors associated with static IPv6 configuration that occurred when pushing the Control Center policy. (1114880)

### CMD and IKE

- Corrects an issue with accessing freed memory. (1114764)
- Corrects an issue that can cause the cmd and ikmpd daemons to utilize high CPU cycles. (1114622 and 1114624)

### Config backup

- Provides a more detailed error message when a configuration backup fails due to a directory being found in the place where a file is expected to be. (1114620)
- Adds a utility to reload SwEDE database to fix corruption. (1114829)
- Corrects an issue with config backup and restore with active passport turned on. (1114752)

### Diagnostic tool

- Adds handling for the case where multiple core output is enabled. Include the core for the given PID. Adds audit.raw to the diagnostic output so audit can be filtered. Adds top output to the diagnostic output. (1114923)

### Hostd

- Corrects an issue that could cause frequent crashes of the hostd process. (1114705)
- Makes hostd more responsive to server TTL updates. (1114705)

### **IPS**

- Validates IPS group objects to prevent errors. Makes sure that no two IPS signature group objects have the same engine\_id. (1114818)

### **Kernel**

- Increases the frequency of max ipfilter session audits to every 30 seconds. (1114921)
- Corrects an issue where promoted sessions would occasionally hang. (1114928)
- Fixes a kernel panic caused by a locking problem in tcpoutput. (1114913)
- Fixes an issue caused by a locking error when closing IPsec key socket. (1114947)

### **NSS**

- Corrects an issue in which a configuration change or rollaudit can cause a significant delay in proxy traffic if a proxy has been flooded. (1114897)

### **NTP**

- Improves time accuracy on firewalls that run NTP in multiple zones. Prior to this change, NTP instances in local zones could overwrite the drift setting in the kernel, leading to time inaccuracies. This patch ensures that NTP instances in local zones will never update the drift setting. (1114608)

### **Package management**

- To make management of obsolete packages easier, cf package list makes it clearer which packages can be removed and which cannot. (1114719)
- A new cf package autoremove command has been added. The command removes all obsolete packages from the firewall. (1114719)

### **Proxies**

- Allows the SNMP proxy to run on all LSHA cluster members. (1114774)
- Improves proxy session destruction process when proxy antivirus is enabled. (1114738)
- Corrects an issue with multi-request non-transparent auditing. (1114541)
- Improves DNS proxy handling of traffic congestion. (1114280, 1114413, 1114607, 1114609, 1114610, 1114699, 1114708, 1114713, 1114718, 1114863, and 1114910)
- Fixes memory leaks and an issue with rekeying in the SSH proxy. (1114749)
- Corrects an issue that could cause the HTTP proxy to utilize high CPU cycles. (1114938)

### **Sendmail**

- Sets the maximum number of sendmail processes to 50 when sendmail is not configured. (1114655)

### **Type Enforcement**

- Fixes a Type Enforcement error when IPS is used with the DNS proxy. (1114739)

### **Virtual appliance**

- Enables Sidewinder on ESXi 6.0/VM Version 11. (1114580)

### **Miscellaneous**

- Updates Forcepoint copyright year to 2018. (1114900)

# 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*

