



FORCEPOINT

Sidewinder

Release Notes

8.3.2P08

Revision B

Table of contents

- 1 About this release.....3
 - Supported firewall types.....3
 - Compatible products..... 3
 - Requirements..... 4
- 2 Resolved issues..... 7
- 3 Installation instructions.....11
- 4 Known issues..... 12
- 5 Find product documentation..... 13
 - Product documentation..... 13

About this release

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

Forcepoint™ Sidewinder® version 8.3.2P08 resolves issues present in the previous release.



Note: We have rebranded Sidewinder (formerly McAfee Firewall Enterprise) and the Sidewinder product documentation.

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:

- KnowledgeBase article [KB67462](#)
- Technical Note [PD22824](#)


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"> • Windows Server 2008 • Windows 7 • Windows 8 • Windows 10 <div>  <p>Note: 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"> • Windows XP Professional • Windows Vista
Web browser	<p>One of the following:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer, version 6 or later • Mozilla Firefox, version 1.0 or later
Hardware	<ul style="list-style-type: none"> • 2 GHz x86-compatible processor • 2 GB of memory • 300 MB of available disk space • CD drive • 1024 x 768 display • Network card (to connect to your firewall) • USB port

Sidewinder requirements

The firewall must meet these requirements.

Table 2: Minimum requirements by type

Firewall type	Platform requirements
Sidewinder appliance	Appliance with a valid support contract: <ul style="list-style-type: none">• 1 GB of memory• AMD64-compatible processor
Sidewinder, Virtual Appliance	Virtualization server: <ul style="list-style-type: none">• Hypervisor operating system — VMware ESX/ESXi version 4.0 or later <div> Note: 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.</div> <ul style="list-style-type: none">• Hardware resources:<ul style="list-style-type: none">• 2 virtual processors• AMD64-compatible processor• 1 GB of memory• 30 GB of free disk space• 2 or more NICs of type e1000• Internet connectivity — The firewall requires a persistent Internet connection to maintain an active license and full functionality.
Forcepoint Sidewinder on Crossbeam X-Series Platforms	Crossbeam X-Series Platform: <ul style="list-style-type: none">• Chassis — X50, X60, or X80-S• XOS version — 9.6.5 and later, 9.7.1 and later, 9.9.x, or 10.0• Application Processor Module — APM-50 or APM-9600<ul style="list-style-type: none">• At least one local disk (RAID 0 and RAID 1 disk configurations are supported; two-disk, non-RAID configurations are not supported)• 12 GB of memory (minimum)• Network Processor Module — NPM-50, NPM-86x0, or NPM-96x0• CBI package — MFE-8.3.2-9.mr1.cbi

McAfee EIA requirements

Systems must meet these requirements to install McAfee EIA.

Table 3: McAfee EIA minimum requirements

Component	Requirements
Operating system	One of these 32-bit or 64-bit Microsoft operating systems: <ul style="list-style-type: none">• Windows 8.1• Windows 7• Windows XP Service Pack 2 and later

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

Resolved issues

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

- Rebranded from McAfee Firewall Enterprise to Forcepoint Sidewinder (1113900)

Common Vulnerabilities and Exposures (CVEs)

BIND

Imports fixes for these CVEs:

- CVE-2015-5722 and CVE-2015-5986; see [KB83603](#) for more information (1088359)
- CVE-2015-5477; see [KB83603](#) for more information (1082105)
- CVE-2015-4620; see [KB83603](#) for more information (1075258)
- CVE-2015-8704 and CVE-2015-8705; see [KB86499](#) for more information (1113883)
- CVE-2015-8000; see [KB86287](#) for more information (1109899)
- CVE-2016-1285, CVE-2016-1286, CVE-2016-2088; vulnerable to CVE-2016-1285 and CVE-2016-1286; not vulnerable to CVE-2016-2088, but the fix is included for maintenance purposes; see [KB86994](#) for more information (1113943)

DHCP

Addresses the following security vulnerabilities by upgrading DHCP:

- CVE-2015-8605; see [KB86756](#) for more information (1113906)

Kernel

Imports fixes for these CVEs:

- CVE-2015-5675; see [KB85729](#) for more information (1089624)
- CVE-2015-5358, FreeBSD-SA-15:13.tcp; DoS issue; see [KB85360](#) for more information (1082100)
- Addresses the Firestorm vulnerability; see [KB86811](#) for more information (1113624)
- CVE-2016-1885; not vulnerable, fix included for maintenance purposes; see [KB87006](#) for more information (1113985)

NTP

- Addresses the following security vulnerabilities by upgrading NTP to version 4.2.8p6: CVE-2015-8158, CVE-2016-7979, CVE-2015-7978, CVE-2015-7977, CVE-2015-7973, CVE-2015-8139, CVE-2015-1798, CVE-2015-5194, CVE-2015-5195, CVE-2015-5300, CVE-2015-7691, CVE-2015-7692, CVE-2015-7702, CVE-2015-7703, CVE-2015-7704, CVE-2015-7705, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7852, CVE-2015-7854, CVE-2015-7855
- Incorporates fixes for CVE-2015-8138, CVE-2015-7976, CVE-2015-7975, CVE-2015-7974, and CVE-2015-8140 for general maintenance; see [KB86643](#), [KB84695](#), [KB86067](#) for more information (1113898, 1110996)
- Imports fixes for CVE-2014-9297 and CVE-2015-1799; see [KB84695](#) for more information (1055055)

OpenSSH

Imports fixes for these CVEs:

- CVE-2015-6563 and CVE-2015-6564; see [KB85413](#) for more information (1089304)
- CVE-2015-5600; see [KB85413](#) for more information (1082488)
- CVE-2015-5352 for maintenance; see [KB85413](#) for more information (1085041)
- CVE-2016-0777 and CVE-2016-0778; see [KB86500](#) for more information (1113884)

Addresses the following security vulnerabilities by upgrading OpenSSH: CVE-2010-4755, CVE-2016-3115; also includes the changes for non-vulnerable issues which are included with the upgrade: CVE-2011-5000; see [KB87133](#) for more information (1113950, 1113963)

A few configuration options allowed in the previous version are no longer allowed. These include the pps enable or disable option and the mask restrict flag.

OpenSSL

Imports fixes for these CVEs:

- CVE-2015-3194, CVE-2015-3195; this brings OpenSSL up to version 1.0.1q; see [KB86282](#) for more information (1110719)
- CVE-2015-1788, CVE-2015-1789, CVE-2015-1790, and CVE-2015-1793 vulnerabilities; also incorporates fixes for CVE-2015-1792 and CVE-2015-1791 for maintenance; see [KB84883](#) for more information (1059809)
- CVE-2015-4000 AKA Logjam; see [KB84883](#) for more information (1066963)
- CVE-2015-3197; see [KB86642](#) for more information (1113917, 1113920)
- CVE-2016-0800, CVE-2016-0705, CVE-2016-0798, CVE-2016-0797, CVE-2016-0799, CVE-2016-0702, CVE-2016-0703, CVE-2016-0704, CVE-2016-2842; this brings OpenSSL up to version 1.0.1s; see [KB86874](#) and [KB86889](#) for more information (1113936, 1113945)
- CVE-2106-2105, CVE-2106-2106, CVE-2106-2107; this brings OpenSSL up to version 1.0.1t; see [KB87171](#) for more information (1114007)

Sendmail

- Blocks all SSLv2 and SSLv3 connections to sendmail; instead, use TLS to remediate CVE-2014-3566; see [KB83237](#) for more information (1100183)

SNMP

- Imports a fix for CVE-2015-5621; see [KB85743](#) for more information (1088356)

XML Parser

- Imports a fix for CVE-2015-1283; see [KB85907](#) for more information (1088109)

General Maintenance Changes

Admin Console

- Upgrades the Admin Console to OpenSSL version 1.0.1 (1102131)

Authentication

- Corrects an issue with intermittent authentication errors (1102439)

Certificate/Key Management

- Updates the list of Trusted Internet CAs (1050773)

cf_antivirus

- Allows the verify command to run with Sophos anti-virus engine (1095566)

cf_cluster

- Informs read-only admins that they cannot run cf cluster status or cf cluster failover_status (1113919)

cf_ips

- Adds the ability to view the IPS version from the command line (1112554)

entrelayd

- Adds extra diagnostics to entrelayd, to resolve the spin-loops that some customers have experienced; if a spin-loop occurs, entrelayd saves a core file for debugging purposes, then restarts itself (1107305)

IPsec VPN

- Corrects an issue with ikmpd running hot due to improper handling of file descriptors (1042974)

Kernel

- Corrects a reference count leak that could lead to a kernel crash when an extremely large number of packets are processed (1062197)

- Requeues IPsec packets after ESP decapsulation (1096341)
- Fixes a division by zero error when processing NAT addresses (1104233)
- Corrects an issue processing IPsec data related to disconnected sockets (1085987)
- Resolves duplicate FIN/ACKs being sent for socket mated connections (1086453)
- Allows the sysctl to display the host cache when the cache is larger (1086453)
- Improves VPN performance on model 1402-C3 hardware (1049591)
- Fixes a session establishment error that occurs when TCP window size on server is initially set to zero (1077336)
- Fixes ping problems to local interface with ICMP6 (1072841)
- Improves policy loading when preserving source port with a redirect address (1058663)
- Removes a diagnostic tripwire in the kernel that was giving a false positive (1061494)
- Ensures that the next sequence number is correct when acking SYN/ACK (1052933)
- Adds a sysctl to configure IP Filter behavior with dynamic DNS host objects; see the `cf_host` manpage for more information (1113944)
- Allows the IPsec SHA-2 hash length to be configurable. When Sidewinder first implemented SHA-2 support for IPsec, it truncated all SHA-2 hashes to 96 bits, as specified in an early draft standard. The final RFC specifies that the hash should be truncated to the hash size divided by two. You can now select which behavior is best for your environment. (1113973)
- Sets the default of `net.inet.tcp.drop_synfin` to enabled. The SYN with FIN scan Network Defense no longer enables or disables this setting. (1113983)

Man Pages

- Corrects errors in the `cf appgroup` man page (1059846)

McAfee EIA

- Adds support for utf-8 encoded metadata sent from McAfee EIA on a multilingual operating system (1049504)
- Corrects an issue with `configreport` so it can handle cases where certifications do not exist for McAfee EIA (1093970)

monitord

- The `monitord` daemon has been modified to not monitor system (kernel) processes (1102111)

NTP

- Deprecated `ntpd`; use `ntp` instead (1113933)
- Improves `ntpd` outbound query IP address selection on LSHA clusters (1113938)
- Reduces the frequency of time slew audits (1113925)

OpenSSL

- Imports bug fixes from vendor (1059809)

Policy

- Decreases compile times on policies with overlapping IP address ranges; the rule compiler now identifies adjacent and overlapping IP address ranges used in rules and combines them when possible (1113942)

Proxies

- Corrects an issue in session termination processing (1066945)
- Increases the maximum allowed HTTP header length and resolves certain rule interactions when HTTP upstream proxy support is used (1110763)
- **HTTP**
 - Fixes a memory leak in the HTTP proxy (1047557)
 - Improves handling of SmartFilter user groups (1057645)
- **ICA**
 - Fixes an ICAP issue that did not allow newer versions of Citrix traffic to pass through the firewall (1049090, 1052255)
- **SNMP**

- Fixes issue with the SNMP proxy not properly forwarding traffic to the correct server (1097731, 1096668)
- **SSH**
 - Corrects an issue with the SSH Proxy causing clients to hang when enforcing permissions on SFTP version 6 (1064634)
 - Adds the option `min_appdefense_socket_mate` to the SSH Proxy config file that turns no application defense proxy SSH rules into socket mated rules (1074651)
 - Corrects an issue with the sftp rename command (1040548)

SmartFilter

- Fixes a file descriptor leak in sfagent (1083066)

submit

- Deprecated the submit tool (1113907)

Timezone

- Reverts updates for the June 30, 2015 leap second made by 8.3.2E53 and makes the patch obsolete; see [KB84813](#) for more information (1067030)

Upgrades

- Resolves an issue when upgrading from 8.2.1 (1113930)

Installation instructions

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

The firewall must be at version 8.3.2P03 or later.

- **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 this KnowledgeBase article: [KB79061](#).

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

1. Go to the **ServicePortal** at <https://support.mcafee.com> and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

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

Copyright © 1996 - 2016 Forcepoint LLC
Forcepoint™ is a trademark of Forcepoint LLC.
SureView®, ThreatSeeker®, TRITON®, Sidewinder® and Stonesoft® are registered trademarks of Forcepoint LLC.
Raytheon is a registered trademark of Raytheon Company.
All other trademarks and registered trademarks are property of their respective owners.