Sidewinder

Release Notes

8.3.2P10

Revision A

Contents

About this release

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

Forcepoint Sidewinder version 8.3.2P10 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	One of these Microsoft operating systems: • Windows Server 2008 • Windows 7 • Windows 8 • Windows 10 **Note:** Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported. Compatible legacy Microsoft operating systems: • Windows Vista
Web browser	One of the following: • Microsoft Internet Explorer, version 7 or later • Mozilla Firefox, version 1.0 or later

Component	Requirements
Hardware	• 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: • 1 GB of memory • AMD64-compatible processor
Sidewinder, Virtual Appliance	Virtualization server: • **Hypervisor operating system** — VMware ESX/ESXi version 4.0 or later **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. • **Hardware resources**: • 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.

Firewall type	Platform requirements
Forcepoint Sidewinder on Crossbeam X-Series Platforms	Crossbeam X-Series Platform: • **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 • 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: • Windows 8.1 • Windows 7 • Windows XP Service Pack 2 and later • 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	• 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: • USB port • CD drive
Other products	McAfee EIA deployment requires: • 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.

Common Vulnerabilities and Exposures (CVEs)

BIND

- Upgrades BIND to 9.9.10-P3.
  Imports fixes for CVE-2017-3140, CVE-2017-3141, CVE-2017-3142, and CVE-2017-3143. (1114569 and 1114614)
- Upgrades BIND to 9.9.9-P8.
  Imports fixes for CVE-2017-3136, CVE-2017-3137, and CVE-2017-3138. See Knowledge Base article 12679 for more information. (1114468)
- Upgrades BIND to 9.9.9-P6.
  Imports fixes for CVE-2017-3135. See Knowledge Base article 12382 for more information. (1114383)
- Upgrades BIND to 9.9.9-P5.
  Imports fixes for CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, and CVE-2016-9778. See Knowledge Base article 12250 for more information. (1114338)
- Upgrades BIND to 9.9.9-P4.
  Imports fixes for CVE-2016-8864. See Knowledge Base article 12046 for more information. (1114286)

libarchive

- Upgrades libarchive to 3.3.1.
  Imports fixes for CVE-2017-5601, CVE-2016-8687, CVE-2016-10350, and CVE-2016-10349. (1114524, 1114525, and 1114526)
- Upgrades libarchive to 3.2.1.
  Imports fixes for CVE-2016-6250, CVE-2016-5844, CVE-2016-5418, CVE-2016-4809, CVE-2016-4302, CVE-2016-4301, CVE-2016-4300, CVE-2016-7166, CVE-2015-8932, CVE-2015-8933, CVE-2015-8934, CVE-2015-8915, CVE-2015-8916, CVE-2015-8917, CVE-2015-8918, CVE-2015-8919, CVE-2015-8920, CVE-2015-8921, CVE-2015-8922, CVE-2015-8923, CVE-2015-8924, CVE-2015-8925, CVE-2015-8926, CVE-2015-8927, CVE-2015-8928, CVE-2015-8929, CVE-2015-8930, and CVE-2015-8931. (1114221, 1114222, and 1114224)

libc

- Imports fixes for CVE-2016-6559. See Knowledge Base article 12254 for more information. (1114356)

NTP

- Upgrades NTP to 4.2.8p10.
  Imports fixes for CVE-2016-9042, CVE-2017-6451, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, and CVE-2017-6464. See Knowledge Base article 12552 for more information. (1114450)
- Upgrades NTP to 4.2.8p9.
  Imports fixes for CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, and CVE-2016-9312. See Knowledge Base article 12449 for more information. (1114412)

OpenSSH

- Upgrades OpenSSH to 7.5p1.

Imports fixes for CVE-2016-8858, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, and CVE-2016-10012. See Knowledge Base article 12799 for more information. (1114485, 1114486, and 1114487)

- Comments out the deprecated fields RSAAuthentication, RhostsRSAAuthentication, ServerKeyBits, and KeyRegenerationInterval from the /etc/ssh/sshd_config file.

OpenSSL

- Upgrades OpenSSL to 1.0.2k.
  Imports fixes for CVE-2017-3730, CVE-2017-3731, CVE-2017-3732, and CVE-2016-7055. See Knowledge Base article 12338 and Knowledge Base article 12116 for more information. (1114484)

General Maintenance Changes

ACLD

- Corrects an issue involving promoted connections with multiple IP address redirection. (1114357)

Admin Console

- Corrects setting public key authentication in the Remote Access Management screen. (1114294)

Certificates

- Updates the default certificates to use SHA-2. (1114261)
- Prevents the creation of an enterprise certificate on a standalone firewall. (1114465)
- Updates the list of Trusted Internet Certificate Authorities (CAs) from Mozilla. (1114239)
- If the SSH proxy is using DSA, still allows a 1024-bit key. (1114517)
- Uses SHA1 digest for keys smaller than 1024 bits. (1114539)

cf_cluster

- Adds a function to renew enterprise certificates. (1113995)

cf_ssl

- Corrects an issue where overly large endpoint lists could be created for SSL rules. (1114254)

Kernel

- Adds a sysctl to configure IP Filter behavior with redirection dynamic DNS host objects. (1114303)
- Substantially decreases the effect of a BlackNurse ICMP attack. (1114308)
- Adds ksem support to kernel for POSIX semaphores. (1114375)

NSS

- Corrects an issue where a configuration change or rollaudit can cause a significant delay in proxy traffic if a proxy has been flooded. (1114630)

OpenSSL

- Enables a TLS option for listing elliptic curve algorithms for STARTTLS. (1114547)

Package Management

- Deletes temporary files if a package installation fails. (1114298)
- This is an inactive patch that is installed on the alternate slice. This allows you to increase the available space in the vcdrom by removing obsolete packages. In addition, the patch can be rolled back, rather than uninstalled, if you later want to revert this patch. (1114298)

Policy

- Adds a new config file (/secureos/etc/host.conf), which allows you to set the minimum time to live (TTL) for host objects. It also allows the TTL override on host objects to be less than the DNS TTL. (1114377)
- Improves handling of Default AppDefense Group changes. (1114254)
- Decreases memory usage and compile times when expanding IP address range and subnet endpoint objects during rule compilation. Ranges that overlap or are adjacent are combined when possible. (1114270)

Proxies

- Adds support for passing the TLS server name indication (SNI) option through decrypted/re-encrypted proxy sessions. (1114219 and 1114334)
- Removes an unneeded external SSL cache from the HTTP proxy. (1114321)
- Corrects an issue with the HTTP proxy that is encountered when virus-scanning large files. (1114449)
- Corrects an issue with the SMTP proxy that is encountered when using the CHUNKING extension. (1114606)
- SNMP Proxy performance has improved. (1114536)

tcpdump

- Upgrades tcpdump to 4.9.0. (1114391)

Timezone Update

- Updates timezone information from IANA. (1114414)

Miscellaneous

- Updates the Forcepoint copyright year to 2017. (1114422)
- Updates the End User License Agreement. (1114532 and 1114565)

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 be at version 8.3.2P03 or later.

Note: This is an inactive patch that is installed on the alternate slice. This allows you to increase the available space in the vcdrom by removing obsolete packages. In addition, the patch can be rolled back, rather than uninstalled, if you later want to revert this patch.

- **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