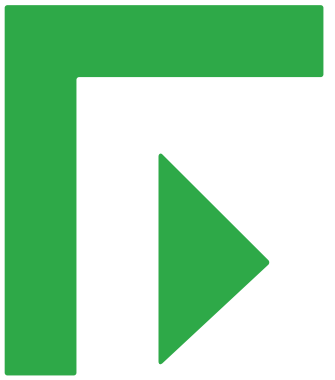

FORCEPOINT

Sidewinder

Release Notes

7.0.1.03H14

Revision A

Table of 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 7.0.1.03H14 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

Compatible products

Sidewinder is compatible with the following products.

- Forcepoint Sidewinder Control Center

For more information, see:

- Knowledge Base article 9275
- 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. For more information, see the *McAfee Firewall Enterprise Release Notes*, version 7.0.1.03.

In addition to the operating systems listed in the *Admin Console requirements* section of the *McAfee Firewall Enterprise Release Notes*, version 7.0.1.03, we also support:

- 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.

New features

This release of the product includes these new features.

Hardware

Support Sidewinder Firewall on model 1402-C3 hardware

Note: The 1402-C3 cannot upgrade directly from Sidewinder 7 to Sidewinder 8; see Knowledge Base article 10466 for more information (1114132).

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, 1113949)

Common Vulnerabilities and Exposures (CVEs)

BIND

Imports fixes for these CVEs:

- 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 Knowledge Base article 10240 for more information (1113990)
- CVE-2015-8704 and CVE-2015-8705; see Knowledge Base article 10199 for more information (1113903)
- CVE-2015-8000; see Knowledge Base article 10182 for more information (1113753)

DHCP

Addresses the following security vulnerabilities by upgrading DHCP to version 4.3.3-P1:

- CVE-2015-8605; see Knowledge Base article 10218 for more information (1113948)

Kernel

Imports fixes for these CVEs:

- CVE-2016-1886, FreeBSD-SA-16:18.atkbd; see Knowledge Base article 10265 for more information (1114087)
- Addresses the Firestorm vulnerability; see Knowledge Base article 10221 for more information (1113967)

NTP

- Addresses the following security vulnerabilities by upgrading NTP to version 4.2.8p8: CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, CVE-2016-4957; see Knowledge Base article 10260 for more information (1114084)
- Addresses the following security vulnerabilities: CVE-2016-1547, CVE-2016-1550, CVE-2016-2518, CVE-2016-2519, CVE-2015-7704, CVE-2016-8138; mitigation is incorporated for the following security vulnerabilities: CVE-2016-1548, CVE-2016-1549; incorporates fixes for CVE-2016-1551, CVE-2016-2516, CVE-2016-2517 for general maintenance; see Knowledge Base article 10257 for more information (1114011)
- Addresses the following security vulnerabilities: CVE-2015-7973, CVE-2015-7977, CVE-2015-7978, CVE-2016-7979, CVE-2015-8139, CVE-2015-8158; incorporates fixes for CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-8138, and CVE-2015-8140 for maintenance; see Knowledge Base article 10212 for more information (1113921)
- Addresses the following security vulnerabilities: 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; see Knowledge Base articles 10105 and 10166 for more information (1113902)

  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.

OpenSSH

- Addresses the following security vulnerability by upgrading OpenSSH to version 7.3p1: CVE-2016-6515, see Knowledge Base article 10481 for more information (1114154)
- Addresses the following security vulnerabilities: CVE-2010-4755, CVE-2016-3115; includes the changes for non-vulnerable issues in CVE-2011-5000; see Knowledge Base article 10247 for more information (1114015, 1114016)

OpenSSL

Imports fixes for these CVEs:

- CVE-2106-2105, CVE-2106-2106, CVE-2106-2107; see Knowledge Base article 10250 for more information (1114014)
- CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0799, CVE-2016-0800, CVE-2016-2842; not vulnerable to CVE-2016-0798, but a change is included for maintenance purposes; CVE-2016-0703 and CVE-2016-0704 were addressed in 70103H12, but are mentioned here for completeness; see Knowledge Base article 10223 and 10225 for more information (1113976, 1113977)
- CVE-2015-3197; see Knowledge Base article 10211 for more information (1113926, 1113934)
- CVE-2015-3194, CVE-2015-3195; see Knowledge Base article 8483 for more information (1113509)
- CVE-2016-2177 and CVE-2016-2178; see Knowledge Base articles 10479 and 10480 for more information (1114091)

Upgrades OpenSSL to version 1.0.2 (1114095)

SSLv2 and minimum cipher lengths of 40 bit and 56 bit are removed (1114180)

General Maintenance Changes

Licensing and Downloads

- Changes domain names for dynamic component downloads from McAfee to Forcepoint (1114120)

Specifically, changes:

```
downloads.securecomputing.com to sidewinder.downloads.forcepoint.com; used for patches and upgrades
 downloads.securecomputing.com to sidewinder.downloads.forcepoint.com; used for geo-location updates
 downloads.securecomputing.com to av.sidewinder.downloads.forcepoint.com; used for McAfee Anti-Virus
 updates
 downloads.securecomputing.com to sig.sidewinder.downloads.forcepoint.com; used for IPS signature
 updates
 go.mcafee.com to sidewinder.activations.forcepoint.com; used for licensing
```

See Knowledge Base article 10504 for this change for more information.

acld and hostd

- Improves how acld and hostd handle cases where host lookups fail with an error. Better diagnostics are reported in the audit, and the previous DNS lookup results continue to be used until the next DNS lookup succeeds (1113929)

Admin Console

- Upgrade OpenSSL to version 1.0.2 (1114095)

Audit

- Fixes scp audit export to FreeBSD 10 hosts (1114181)

cf_interface

- Fixes a cf_interface issue in certain bridge configurations (1114182)

cf_ips

- Adds ability to view the IPS version from the command line (1113904)

Kernel

- Corrects a TE issue when route synchronization takes place from a primary to a standby firewall (1099163)
- Removes support for uniprocessor kernels from Sidewinder 7 (1114132)

NTP

- Deprecated ntpdc; use ntpq instead (1113968)
- Reduces the frequency of time slew audits (1113932)
- Improves ntpd outbound query IP address selection on LSHA clusters (1113938)

RealAudio Proxy

- Fixes a memory leak in the RealAudio proxy when acld is running slowly and the server connection encounters an unexpected error during the initial connect (1114135)

SNMP

- Corrects an issue when SNMPd starts in FIPS mode (1113993)
- Corrects a Type Enforcement issue in snmpwalk (1114062)

SNMP Proxy

- Corrects an issue where return traffic is not passed to the SNMP Proxy when an overlapping IP Filter rule is used (1114044)

SSH Proxy

- Corrects an issue with the sftp rename command (1113935)

submit

- Deprecates the submit tool (1113907)

Installation notes

To bring your firewall to version 7.0.1.03H14, follow the patch installation process appropriate for your environment.

The firewall must be at version 7.0.1.03.

- **Standalone or HA cluster** — See the *Forcepoint Sidewinder Administration Guide*.
- **Firewall or HA cluster managed by Control Center** — See the *Forcepoint Sidewinder Control Center Release Notes* and *Forcepoint Sidewinder Control Center Product Guide*.

Note: If your firewall is managed by Control Center, it must be at version 5.1.2 or later to manage firewalls at version 7.0.1.03H14.

Known issues

For a list of known issues in this product release, see this Knowledge Base article: 9386.

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