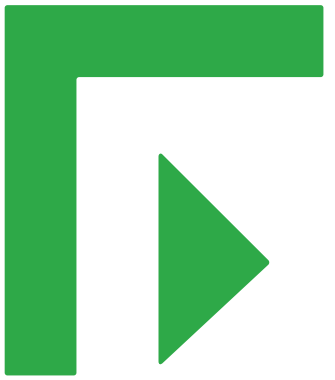

FORCEPOINT

Sidewinder

Release Notes

7.0.1.03H15

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 7.0.1.03H15 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 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. 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.

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. (1114595 and 1114545)
- Upgrades BIND to 9.9.9-P7.
  Imports fixes for CVE-2016-6170, CVE-2017-3136, CVE-2017-3137. See Knowledge Base article 12551 and Knowledge Base article 12679 for more information. (1114424)
- Upgrades BIND to 9.9.9-P6.
  Imports fixes for CVE-2017-3135. See Knowledge Base article 12382 for more information. (1114379)

  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)

  Imports fixes for CVE-2016-2776 and CVE-2016-8864. See Knowledge Base article 8757 and Knowledge Base article 12046 for more information. (1114228 and 1114305)

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. (1114347)

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. (1114438)
- 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. (1114314)

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. (1114330, 1114352, 1114366, and 1114439)

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. (1114371)
- Upgrades OpenSSL to 1.0.2j.
  Imports fixes for CVE-2016-6304, CVE-2016-2183, CVE-2016-6303, CVE-2016-6302, CVE-2016-2182, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2181, CVE-2016-6306, and CVE-2016-7052. Not vulnerable to CVE-2016-6309 or CVE-2016-7052, but a related change is included for maintenance purposes. See Knowledge Base article 10448 for more information. (1114244, 1114235, and 1114231)

tcpdump

- Upgrades tcpdump to 4.9.0. (1114373)

General Maintenance Changes

Audit

- Corrects an SCP audit export issue. (1114273)

BIND

- Corrects an issue with the dig and rndc utility versions. (1114272)

cf_config

- Allows a configuration restore on a Control Center-managed firewall at a different hotfix version. (1114209)

High Availability

- Sidewinder firewall clusters with members running at different H-patch levels no longer synchronize policy changes between members. (1114290)

Kernel

- Corrects an IPv6 issue on igb-based NICs. (1114260)

License

- Supports licenses for virtual firewalls running in conjunction with vMotion. (1114220 and 1114562)

NSS

- Corrects an issue where a configuration change or rollaudit can cause a significant delay in proxy traffic if a proxy has been flooded. (1114629)

OpenSSH

- Comments out the deprecated field RhostsRSAAuthentication from the /etc/ssh/sshd_config file. (1114501)
- Does not comment out port configuration in sshd_config during upgrade. (1114563)

Package Management

- Deletes temporary files if a package installation fails. (1114380)
- 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. (1114380)

Timezone Update

- Updates timezone information to tzdata2016j. (1114326)

Upgrades

- Corrects an issue which prevented an upgrade from 70103H15 to v8 using the 70103UP821 rev B patch. (1114495)

Miscellaneous

- Updates the Forcepoint copyright year to 2017. (1114422)
- Updates the End User License Agreement. (1114531 and 1114564)
- Modifications made to support a new license and download server. (1114494)
- Corrects an issue with the master boot record (MBR) on certain hardware models. (1114187 and 1114546)

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 7.0.1.03.

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 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 7.0.1.03H15.

Known issues

For a list of known issues in this product release, see 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