Sophos release notes

Product type: Network Security Product: Sophos (XG) Firewall Version: 18.5

Sophos Firewall

These release notes are for Sophos Firewall (formerly known as Sophos XG Firewall).

See the product documentation at Sophos Firewall help.

Latest version | Previous versions | Resolved issues | Known issues | Upgrade information | Supported platforms | Support

Version 18.5 MR2 Build 380

Released on November 29, 2021

New features

This page describes the new features introduced in 18.5 MR2.

For details, see the help.

Important point to consider before you upgrade to v18.5 MR2

An upgrade to 18.5 MR2 refreshes the firewall certificate used by endpoints to send a heartbeat to the firewall. To make sure that endpoints can download the refreshed certificate from Sophos Central after the firewall is upgraded to 18.5 MR2, see Security Heartbeat connection issue with 18.5 MR2.

FIPS 140-2 certification

You can configure Sophos Firewall to use a cryptography library that is certified for the Federal Information Processing Standard 140-2 (FIPS 140-2) level 1 for the following appliances:

- XGS series hardware
- Virtual machines

IPsec VPN

- **IPsec VPN**: Introduced support for GCM and suite-B ciphers for IPsec VPN. AES-GCM for IPsec significantly improves IPsec VPN performance.
- **Remote access IPsec**: Increased the maximum idle time-out to 6 hours for IPsec remote access connections.
- **Route-based VPN**: For route-based VPN connections with source NAT rules, MASQ now carries the xfrm IP address on the inner IP header and the WAN IP address on the outer header.

Authentication

- **MFA with Time-based OTP (TOTP)**:
  - We added MFA support for the built-in "admin" account and alert notifications for all administrator accounts not using MFA.
  - We added the token initialization process for signing in to the web admin console as well as for existing users signing in to the user portal.
  - We streamlined the MFA experience with easy-to-find and configure MFA settings on the web admin console.
  - We removed the ability to view existing OTP secrets and QR codes for token recovery. Lost tokens must be deleted and re-initialized through the sign-in process.
- **Users**: Enhanced view of multiple group membership for Active Directory users. The web admin console now shows all the groups a user belongs to.

Certificates

- Removed the ability to download private keys for CSRs and uploaded certificates. So, you can't use CSRs and private keys generated on Sophos Firewall for external systems. You need to use other methods, such as tools built into operating systems.
- Shown useful information about the different types of certificate authorities.
- Made it easy to find locally-added certificates and certificates with private keys.
- Made it easy to copy or download a certificate's public key to check and confirm.

Consolidated Troubleshooting Report (CTR)

- Introduced the ability to capture the complete troubleshooting logs, including log file rotation in the CTR.
- Introduced the ability to generate the CTR from the backend.
- Eliminated time-out and console freeze during CTR generation.

Usability

- **Sophos Assistant**: Introduced Sophos Assistant, a new interactive help on the web admin console. The help flows guide you, making it easier to complete complex configurations.
- **IPv6 web categorization for HTTPS requests**: HTTPS requests that connect directly to an IPv6 address will now have the “IP address” web category instead

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_185_rn.html

Sophos release notes

Product type: Network Security Product: Sophos (XG) Firewall Version: 18.5

a global switch on **Intrusion Prevention** > **IPS policies** to turn on or turn off IPS protection. If you're currently using IPS, the switch is automatically set to **On** when you migrate to 18.5 MR2.

- **Installation wizard**: Provided a default option for a 2-port bridge rather than the previous single bridge configuration for all ports.

Enhancements

The enhancements introduced in 18.5 MR2 are as follows:

- Xstream Flow Processor driver update related to performance optimizations. The update is mandatory for XGS 4300, XGS 4500, XGS 5500, and XGS 6500 appliances.
- Upgraded JQuery to version 3.5.0.
- Introduced hardware reset on XGS 87 and XGS 107 appliances. Press and hold the hardware reset button to perform a factory reset to help recover from a bad configuration.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_185_rn.html