Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 19.5

Sophos Firewall

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

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

Version 19.5 MR2 Build 624

Released on May 09, 2023

New features

This page describes the new features introduced. For details, see the Sophos Firewall help.

Important security and hardening enhancements

The release implements two security enhancements that help harden your firewall and follow the industry best practices to protect your firewall from attacks.

These changes impact access to the web admin console and user portal from the WAN zone.

Web admin console access from specific WAN IP addresses:

- We strongly recommend turning off web admin console access from all WAN sources (the entire internet) to reduce the potential for a brute force or reconnaissance attack.
- For remote management of your firewalls, we recommend using Sophos Central. It's free for customers.
- If you must provide access to the web admin console from WAN, go to Administration > Device access, add a local service ACL exception rule, allowing specific IP addresses and networks.
- Web admin console will no longer be available from all WAN sources. So, you won't be able to select WAN under HTTPS on Administration > Device access.

Note Existing deployments aren't impacted. If you've already turned on web admin console access from all WAN sources, the functionality continues to work after you upgrade to SFOS 19.5 MR2.

Unused WAN access to web admin console and user portal:

- Web admin console and user portal access from all WAN sources will be turned off if there aren't any successful sign-ins from the WAN zone for 90 consecutive days. This applies to all deployments.
- Access given to specific WAN IP addresses and networks through a Local service ACL exception rule isn't impacted. These sources will continue to have access even if there are no sign-ins.

This has been done to prevent instances where the access was turned on but remains unused, leaving the firewall potentially exposed on the internet to brute force and reconnaissance attacks.

Note If you've already turned it on before migration and are actively using it, the functionality will continue to work.

For details, see Best practices for securing your firewall.

IPsec how-to article list accessible from web admin console

Routing and NAT configurations for IPsec: A how-to article list is directly linked from Site-to-site VPN > IPsec to help with IPsec configurations that require routing and NAT. The list includes articles that address use cases, such as system-generated DHCP relay and authentication traffic and traffic to a host through an existing IPsec tunnel.

Other enhancements

The version offers the following enhancements:

Dynamic routing: The firewall now supports up to 4000 multicast groups providing additional scalability in dynamic routing deployments. This eliminates issues related to dynamic routes being unable to join multicast groups.

SD-RED: A new banner on the Wireless pages highlights the approaching End-of-Life (EOL) date for legacy RED 15, 15w, and RED 50 devices. EOL is on August 31, 2023.

You must upgrade your RED devices to the latest models, which offer higher performance and improved connectivity.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_195_rn.html

Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 19.5

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_195_rn.html