Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 20.0

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 20.0 MR1 Build 342

Released on May 15, 2024

New features

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

Important points to know before you upgrade

SSL VPN compatibility for 20.0 MR1 with EoL SFOS versions and UTM9 OS

OpenVPN has been upgraded to 2.6.0 in this version. Firewalls upgraded to 20.0 MR1 won't establish SSL VPN tunnels with the following clients and firewall versions:

- **SFOS 18.5 and earlier versions (end-of-life)**: Site-to-site SSL VPNs won't be established between SFOS 18.5 or earlier versions and SFOS 20.0 MR1. We recommend that you upgrade both firewalls to 20.0 MR1 at the same time. Alternatively, you can use site-to-site IPsec or RED tunnels.
- **Legacy SSL VPN client (end-of-life)**: Remote access SSL VPN tunnels won't be established with the legacy SSL VPN client, which is already end-of-life. You can use the Sophos Connect client or third-party clients, such as OpenVPN client, or use remote access IPsec tunnels. See Remote access SSL VPN with the Sophos Connect client. See Remote access IPsec VPN.
- **UTM9 OS**: Site-to-site SSL VPNs won't be established between UTM9 OS and SFOS 20.0 MR1. We recommend that you migrate these to 20.0 MR1. Alternatively, you can use site-to-site IPsec or RED tunnels.

For site-to-site IPsec tunnels, see Route-based VPN. For RED tunnels, see Site-to-site RED tunnel.

End-of-life RED devices

20.0 MR1 and later versions won't support the following legacy RED devices: RED 15, 15w, and 50. They have been declared end-of-life in 2023. For more details, see the article Sophos RED: End-of-life of RED 15/15(w) and RED 50.

Device access and Local service ACL exception rules

Device access: This release offers enhancements to the device access grid for access from zones to certain services. The grid has also been grouped to offer intuitive configurations and granular control:

- **IPsec and RED**: IPsec and RED services are available on Device access to allow or block traffic based on zones. For example, you can block access to RED service from WAN while allowing access from other zones.
- **VPN services**: IPsec, SSL VPN, VPN portal, and RED are grouped under VPN services.

Local service ACL exception rule:

- **List view**: The list view of exception rules provides detailed information, such as source, destination, service, and action, with full visibility into the rules, eliminating the need to open the rule to check information.
- **Services**: All the services in the device access grid are now available under services in the exception rule, including RED and IPsec services, offering granular control. For example, you can create an exception rule to allow or block VPN on a specific interface when the service is allowed from WAN. You can also specify the country and IP address, dropping VPN requests from specific countries, such as China, and allow VPN traffic from known FQDNs. The additional services available in exception rules are AD SSO, RADIUS SSO, Captive portal, Client authentication, Chromebook, Wireless, SMTP, SNMP, RED, and IPsec.
- **Additional object types**: The object types, FQDN host, FQDN host group, MAC address, and MAC address list, are available for selection in source and destination hosts, eliminating the need to update dynamic IP addresses in local ACL exception rules.

SD-WAN enhancements for scalability

- **Scalability**: This version brings 4x improvements in the gateway availability time during HA failover and device restart, ensuring minimal traffic disruption.
- **Detailed information view**: SD-WAN routes show important gateway information, such as IP address, interface, and name, when you hover over the gateway while configuring the route.

VPN enhancements

SSL VPN

- **OpenVPN 3.0**: Sophos Firewall is now compatible with OpenVPN 3.0 clients. Users can download the compatible configuration file from the VPN portal.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_200_rn.html

Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 20.0

DHCP enhancements

- **IPv6 DHCP prefix delegation**: The firewall requests the preferred prefix from the ISP each time you update the interface configuration or when the firewall restarts.
- **DHCP lease time**: DHCP clients will make renewal requests at 30 seconds if the lease interval's half-time is 30 seconds or less, ensuring continuous WAN connectivity.
- **Boot options**: DHCP now supports boot server and boot file options in the DHCP header. You can also continue to send the parameters through specific DHCP options to provision network devices.

Logging enhancements

- **Download log files**: You can download individual log files from the web admin console on the Diagnostics page under Troubleshooting logs. The Consolidated Troubleshooting Report (CTR) continues to have all the log files.
- **Default log lines in CTR**: The default number of log lines for log files in the Consolidated Troubleshooting report is now 10,000.
- **Syslog delimiter**: You can customize the delimiter in syslog event messages, offering flexibility in managing log data.

True Zero Touch configuration

TPM-based True Zero Touch is available to remotely deploy firewalls in branch offices through Sophos Central. You'll specify the firewall configuration in Sophos Central. The remote firewall administrator connects the firewall to the internet and turns it on. The firewall connects to Sophos Central, downloads and applies the configuration, and then registers with Sophos Central. For more details, see the Sophos Central help.

RED

SD-RED now supports bridge configuration for WAN interfaces with the RED tunnel.

Other enhancements

- **Generative AI assistant**: The firewall now provides assistance using Generative AI through Sophos Assistant with dynamic help and configuration steps.
- **Automatic language detection**: The web admin console and user portal automatically select and store the browser's preferred language for languages the firewall supports, offering a seamless sign-in experience.
- **Custom gateways**: Custom gateways now support the link-local address.
- **Data optimization in Synchronized Application Control**: The firewall only retains the recent five occurrences for each application detected by SAC per endpoint.
- **IPv4 internet host group**: Updated the default public IPv4 host ranges to contain all the public IPv4 address ranges.
- **Object descriptions**: Added description fields for IP, MAC, FQDN, and service objects.
- **Country list**: Updated the country list.
- **Web**: In the web proxy, we've refined the Pharming protection feature to address a potential vulnerability arising from modifications to the destination IP address during proxy DNS resolution. With the updated behavior, the firewall policy will now undergo re-evaluation using the DNS-resolved IP address from Pharming protection.
- **XML API**: 20.0 MR1 doesn't support the XML API version for the end-of-life versions 17.5 and 18.0. If the *APIVersion tag* you use shows old versions, change the tag to the supported API versions.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_200_rn.html