SOPHOS

What's New In

Sophos Firewall

Key New Features in Sophos Firewall OS v21.5

Added protection and performance

Sophos NDR Essentials integration with Sophos Firewall

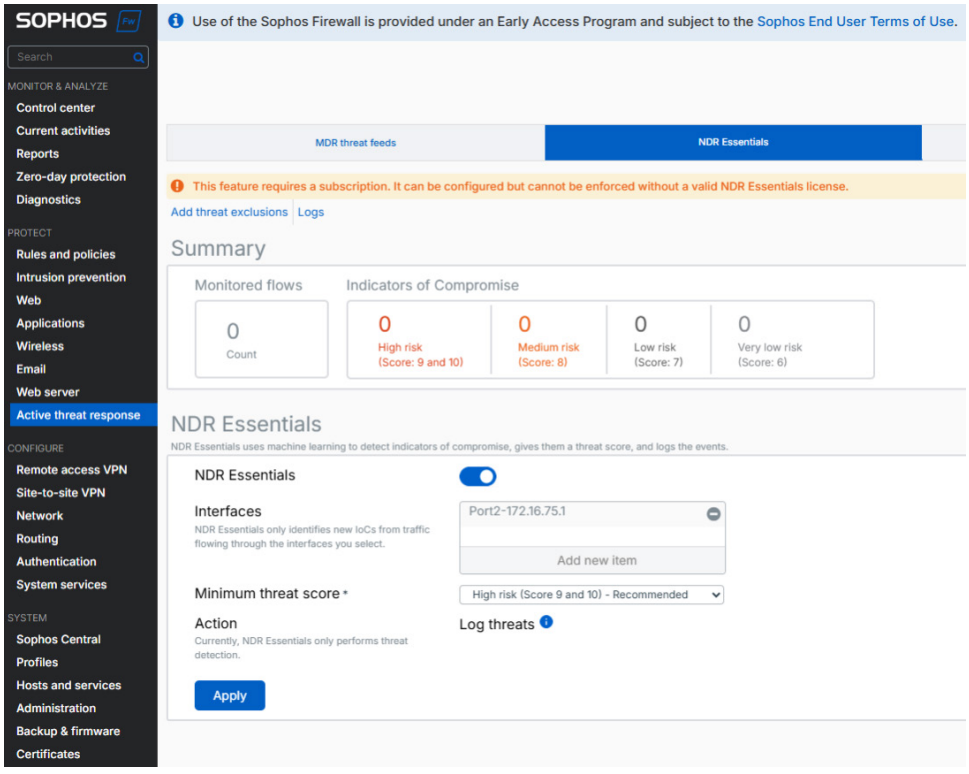
Network Detection and Response (NDR) is a category of network security products that is designed to detect abnormal traffic behavior to help identify active adversaries operating on the network. Skilled attackers are very effective at evading detection, but they ultimately need to move across or communicate out of the network to carry out an attack. NDR typically sits within the network utilizing sensors that monitor and analyze network traffic to identify this kind of suspicious activity.

NDR products have been around for many years, and Sophos NDR has been part of our MDR/XDR portfolio of products since early 2023. However, with SFOS v21.5, we are integrating NDR with Sophos Firewall, an industry first, and making it no extra charge for Sophos Firewall customers with Xstream Protection.

Integrating NDR with a Next-Gen Firewall may seem like an obvious choice, but the challenge is doing it in a way that doesn't impact the performance of the firewall. NDR traffic analysis requires significant processing power. As a result, we've taken the novel approach of deploying an NDR solution in the Sophos Cloud to offload the heavy lifting from the firewall.

Sophos Firewall v21.5 introduces our new NDR Essentials cloud-delivered Network Detection and Response platform. It utilizes the latest AI detections to help identify active adversaries and shares that information using the Sophos Firewall threat feeds API as part of Active Threat Response to keep you informed of any detections and their relative risk.

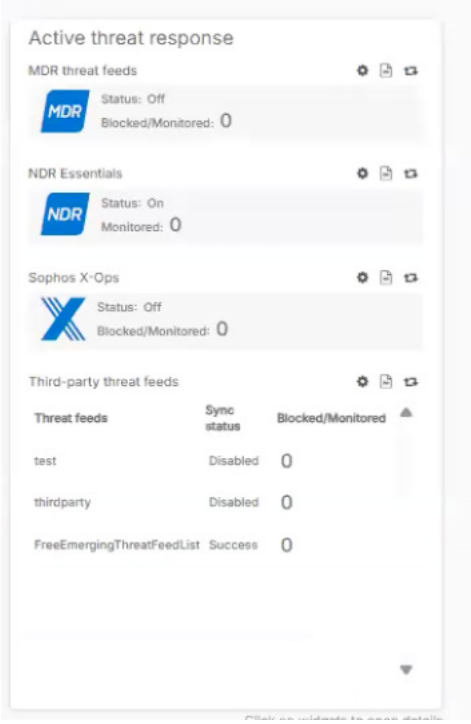
How it works: Sophos Firewall captures metadata from TLS-encrypted traffic and DNS queries and sends that information to NDR Essentials in the Sophos Cloud where the data is analyzed using multiple AI engines. It can detect malicious encrypted payloads without performing TLS decryption, as well as new and unusual domains generated through algorithms that are often a key indicator of compromise. The meta data extraction is performed by a new lightweight engine implemented on the Xstream FastPath, and as a result, is only available on XGS Series hardware firewalls. Virtual, software and cloud firewalls may get this NDR integration capability in the future, but not in v21.5.



Setup and monitor your NDR Essentials feed under Active threat response alongside your other threat feeds.

The new NDR Essentials threat feed is managed alongside your other threat feeds (Sophos X-Ops, MDR, and third-party feeds) in the Active Threat Response area of the firewall as shown in the screenshot above. Setup is simple: Flip a switch to turn it on, select which internal interfaces to monitor, a minimum threshold for detection risk — and you're done!

NDR Essentials detections are scored on a range from 1 (low risk) to 10 (highest risk). You decide what risk score sets the threshold for an alert based on your environment. The recommended default is high-risk (9-10). All detections that are scored greater than or equal to 6 are logged, but only those meeting or exceeding your threshold trigger notifications and are shown as alerts on the new Control Center dashboard widget. Detections scored less than 6 may be false positives and are not logged as a result. No NDR Essentials detections are blocked currently, but this maybe an option in the future. All detections are fully accessible via the Active Threat Response report available both on-box and via Sophos Central Firewall Reporting.



Any NDR Essentials detection meeting or exceeding your risk threshold setting is displayed on the revised Control Center widget.

If you want further detection insights and threat hunting capabilities, you are strongly encouraged to check out Sophos Extended Detection and Response (XDR) with the full implementation of Sophos NDR with the new NDR Investigation Console. You may also wish to consider our full 24/7 Managed Detection and Response service. All of these products and services work better together with your Sophos Firewalls.

Remote access VPN SSO

Entra ID (Azure AD) single-sign on for Sophos Connect client and VPN portal

One of your top requested features makes remote access VPN easier for end-users enabling them to use their corporate network credentials with the Sophos Connect client and the firewall VPN portal. Entra ID (Azure AD) single-sign on integration with Sophos Connect and the VPN portal is now included in SFOS v21.5. It provides cloud-native integration over the industry standard OAuth 2.0 and OpenID Connect protocols for a seamless experience. Supported with Sophos Connect client 2.4 and later on Microsoft Windows.

Other VPN and scalability enhancements

User Interface and Usability Enhancements: Connection types have been renamed from "site-to-site" to "policy-based," and tunnel interfaces have been renamed to "route-based" to make these more intuitive.

Improved IP lease pool validation: Across SSLVPN, IPsec, L2TP, and PPTP remote access VPN to eliminate potential IP conflicts.

Strict Profile Enforcement: On IPsec profiles that exclude default values to ensure a successful handshake, eliminating potential packet fragmentation and tunnels failing to establish properly.

Route-Based VPN Scalability: Route-based VPN capacity is doubled with support for up to 3,000 tunnels.

SD-RED Scalability: Sophos Firewalls now support up to 1,000 site-to-site RED tunnels and up to 650 SD-RED devices.

Sophos DNS Protection

Sophos DNS Protection made easy

Last year, we launched our DNS Protection service and made it free for all Xstream Protection-licensed firewall customers. With this release, Sophos DNS Protection gets further integration with Sophos Firewall in the form of a new control center widget to indicate the service's status, as well as new troubleshooting insights via logging and notifications and a new guided tutorial on how to setup Sophos DNS Protection easily.

Streamlined management and quality of life enhancements

As with every Sophos Firewall release, this version includes several quality-of-life enhancements that make day-to-day management easier.

Resizable Table Columns: A long-requested feature, many firewall status and configuration screens now support resizable column widths that are retained in browser memory for subsequent visits. Many screens such as SD-WAN, NAT, SSL, Hosts and services, and site-to-site VPN, all benefit from this new feature.

Extended Free Text Search: SD-WAN routes now enable searching by route name, ID, objects, and object values like IP addresses, domains, or other criteria. Local ACL rules also now support searching by object name and value, including content-based search.

Default Configuration: By popular demand, the default firewall rules, and rule group previously created when setting up a new firewall have been removed with only the default network rule and MTA rules provided during initial setup. The default firewall rule group and the default gateway probing for custom gateways are both set to "None" by default.

New Font: The Sophos Firewall user interface now sports a new lighter, cleaner, sharper, font for added readability and improved performance.

Other enhancements

Virtual, Software, Cloud Licensing: All Sophos Firewall virtual, software, and cloud licenses (BYOL) no longer have RAM limits. Licenses are now strictly limited by core count and have no RAM restrictions.

Larger file size limit in WAF: Supports a configurable request (upload) file size limit for Web Application Firewall (WAF), which can now scan files up to 1 GB.

Secure By Design: We are continually improving the security of Sophos Firewall, and in this release are adding real-time telemetry gathering to flag any unexpected changes to core OS files using secure hash validation. This will enable our monitoring teams to proactively identify potential security incidents early before they can become a real problem.

DHCP Prefix Delegation Relaxation: Now supports /48 to /64 prefixes, improving interoperability with ISPs. Router Advertisements (RA) and the DHCPv6 server are also now enabled by default.

Path MTU Discovery: This will resolve TLS decryption errors due to the latest ML-KEM (Kyber) key exchange support in browsers. The Sophos Firewall deep packet inspection engine will now automatically detect and adjust the MTU for each flow ensuring optimal performance based on specific network conditions.

NAT64 (IPv6 to IPv4 traffic): NAT64 is supported for IPv6 to IPv4 traffic in explicit proxy mode. In this mode, IPv6-only clients can access IPv4 websites. The firewall also supports IPv4 upstream proxy for IPv6-only clients.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2025-03-31 EN (DD)

SOPHOS