Key New Features in Sophos Firewall OS v21

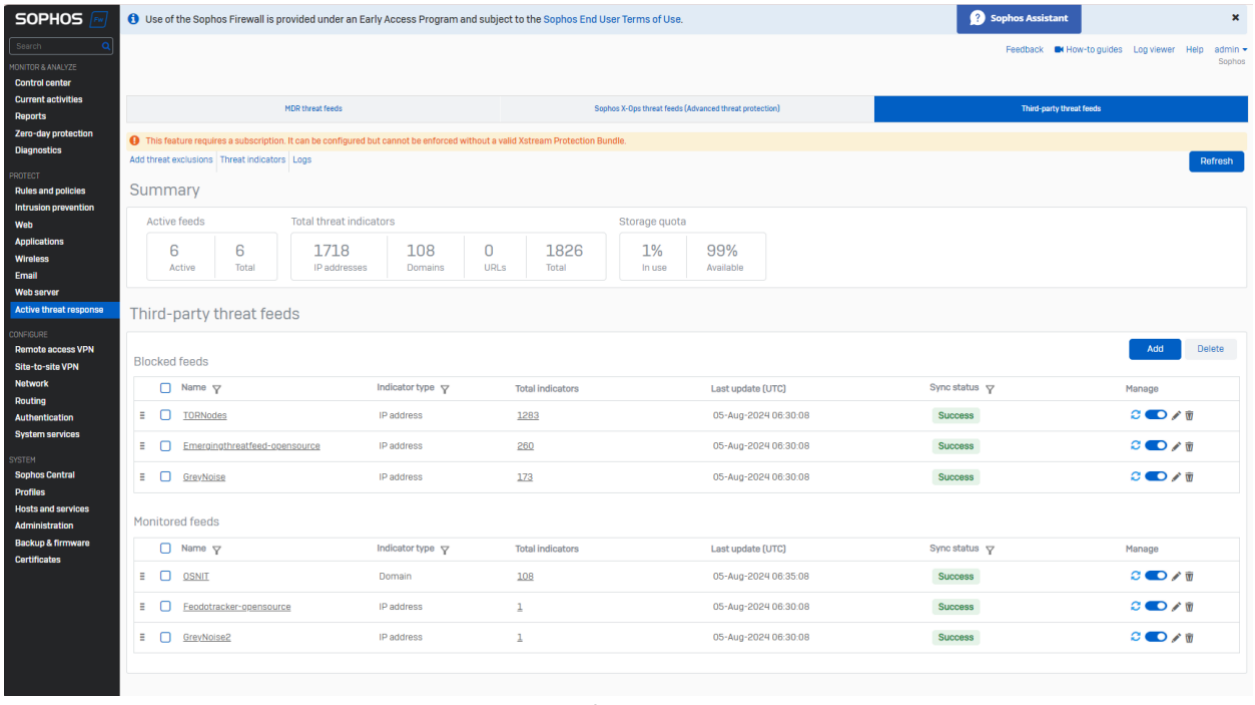
Added Protection

Third Party Threat Feeds

Active Threat Response added in v20, introduced a new extensible threat feed framework in Sophos Firewall. Initial support was provided for dynamic threat intelligence feeds from Sophos X-Ops, and Sophos MDR enabling the firewall to automatically respond by blocking access to any threat published through this framework.

While this is all most customers will ever need, there are certain regions or vertical markets where specific custom threat feeds are encouraged or required. There has also been an interest by our partner community, SoC providers, and many customers for an extensible threat feed capability to support existing or new threat detection and response solutions and services.

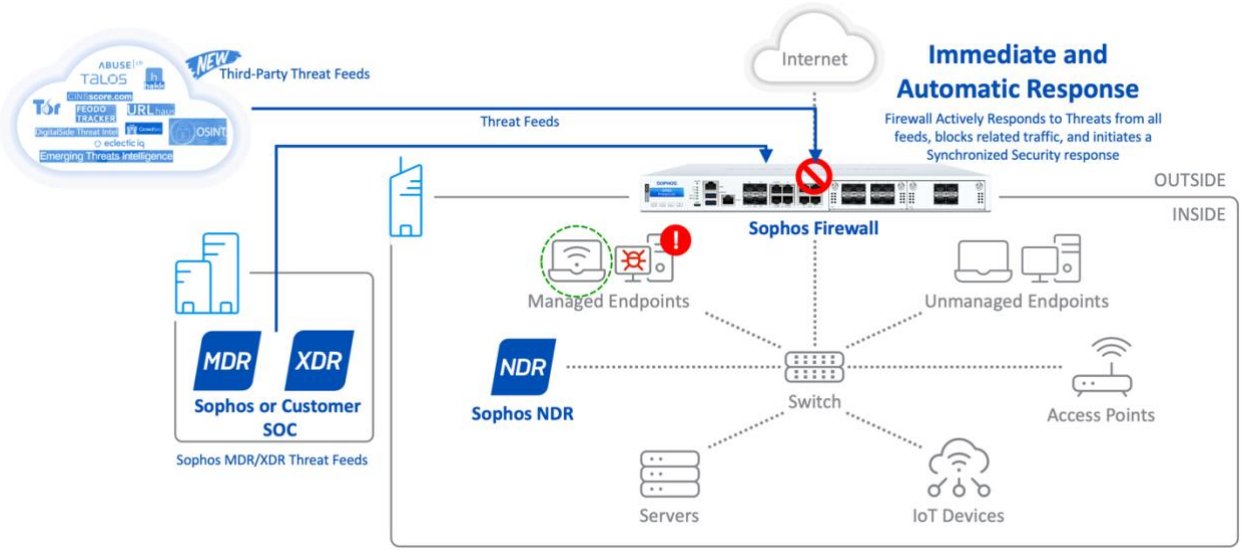
To enable these use cases, Sophos Firewall v21 extends the threat feed framework to support third-party threat feeds. Now, you can easily add additional vertical or custom threat feeds to the firewall which will monitor and respond in the same automatic way – blocking any activity associated with them – across all security engines and without requiring any additional firewall rules.



Setup and monitor your third-party threat feeds under the Active Threat Response menu

MSP Services are also supported enabling Sophos Partners to utilize this capability to its full potential as part of their own managed threat detection and response service. Even competing MDR solutions are supported, enabling Sophos Firewall to integrate more tightly with a customer's existing threat detection and response environment.

For example, if the firewall identifies a device communicating with a C2 server published via any of the threat feed sources, Sophos Firewall will automatically initiate Active Threat Response to block all requests and traffic attempting to contact that C2 server from any host on the network and assign a red Security Heartbeat status to the compromised device. No firewall rule configuration is required.



Support for third-party threat feeds extends Active Threat Response

A variety of specialized and vertical threat feeds are supported including those provided by security organizations, industry consortiums, and community-based, or open-source threat intelligence sources, such as:

- Cisco Talos
- GreyNoise Intelligence
- Abuse.ch / URLhaus
- Hakk Solutions
- OSINT (Open-source Intelligence) / DigitalSide
- CINS Score
- CrowdSec
- EclicticIQ
- Feodo Tracker
- And more!

Synchronized Security for all Threat Feeds

Active Threat Response triggers the same Synchronized Security response as any other red Security Heartbeat condition. This includes enforcement of any firewall rules that contain Heartbeat conditions. The firewall will also coordinate Lateral Movement Protection, which will inform all healthy managed endpoints that there is a compromised host on the LAN so they can block traffic from that device.

Enhanced Scalability

Sophos Firewall v21 includes several enhancements to networking providing improved performance and scalability for many organizations:

High Availability Enhancements

Added resiliency, seamless transitions, and reduced downtime – High availability deployments are enhanced with seamless failover of dynamic routes.SD-RED tunnel failover has also been significantly improved, enabling tunnels to be reestablished within a few second of an HA failover, reducing downtime. Improved interactions with Active Directory domains during HA failovers.

IPsec VPN Enhancements

Enhanced Site-to-Site IPsec Performance: FQDN-based remote gateways have been optimized to improve scalability for distributed deployments. In addition, using DHCP relays over XFRM interfaces is available for traffic to DHCP servers deployed behind the firewall. And for RBVPN deployments, an increase of up to 20x in XFRM interface up-time significantly minimizes disruption during tunnel flap and reboot.

Management Enhancements – Bulk activate and deactivate options are now available for connections. Enhanced filtering on the VPN manage page now consolidates information across multiple pages. And an XFRM interfaces-specific view has been added on the Interfaces page for easy filtering of RBVPN interfaces.

Authentication and Web Protection Enhancements

Authentication Enhancements – Google Workspace integration via LDAP client and Google Chromebook SSO are now supported. Performance for burst login handling is improved up to 4x for Radius SSO, STAS, and Synchronized User ID enabling the handling of thousands of simultaneous login requests even in multiple SSO environments (mix of STAS, Radius SSO, and Synchronized User ID). In addition, support has been added for a transparent AD SSO experience when HSTS is enforced, enabling Kerberos and NTLM handshakes over HTTP or HTTPS.

Web Protection Performance Enhancements – Enforcing SafeSearch, YouTube restrictions, Google App login domains, and Azure AD tenant restrictions now greatly reduces the load on the system, enabling added performance.

Streamlined Management and Quality of Life Enhancements

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

Let's Encrypt Certificate Support – A long-requested feature, Let's Encrypt certificate support enables the automatic deployment and renewal of certificates based on certificate signing requests (CSRs). Let's Encrypt certificates are supported for WAF, SMTP, TLS configuration, hotspot sign-in, the Web Admin console, user portal, captive portal, VPN portal, and SPX portal.

Static Route Management - Users can clone static routes, turn them on or off, and add descriptions. There's now a blackhole route option and support for Equal-Cost Multi-Path (ECMP) for load balancing.

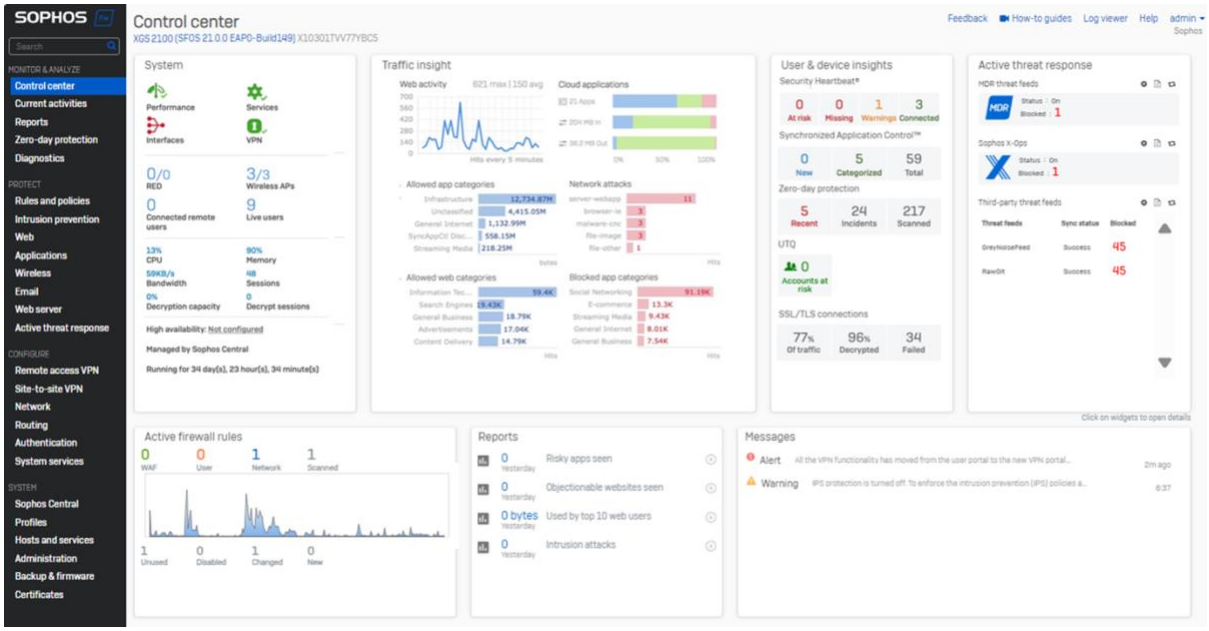
Expanded Object Reference - Offers added visibility into network object references (usage) for interfaces, zones, gateways, and SD-WAN profiles. It also supports XML API support to retrieve object reference (usage) counts, offering visibility into unused objects.

Improved VPN configuration - The firewall now supports free text and value-based search in VPN configurations such as network, subnet, users for remote access and site-to-site VPNs.

Dynamic Routing - A new option to redistribute BGP routes into OSPFv3.

Improved Control Center with Card Views – The Sophos Firewall Control Center has been redesigned with new card views to further enhance visibility into important network events and data. An all-new Active Threat Response card consolidates threat information from MDR, Sophos X-Ops, and Third-Party Threat Feeds into a single, easy-to-view section.

Refreshed Web Admin Console - The Sophos Firewall Web Admin console implements the latest Sophos design style guide matching Sophos Central and providing a fresh new look.



The refreshed Sophos Firewall Control Center sports new card views and the latest design

Seamless Upgrades

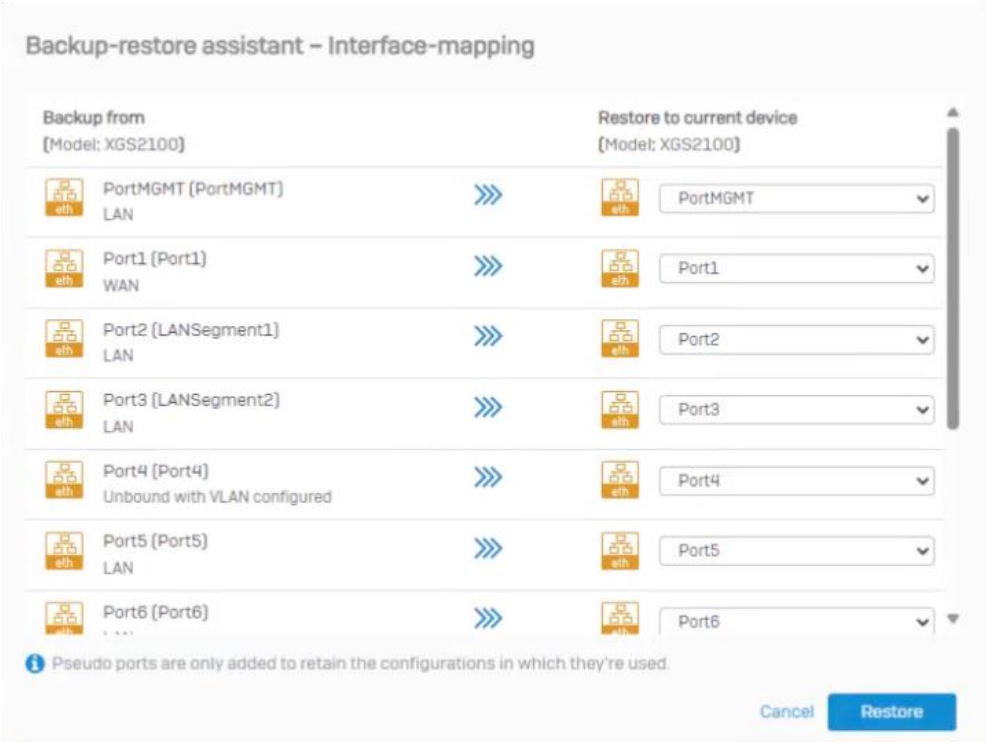
Sophos Firewall v21 includes helpful features first introduced in v20 MR2 that make firewall upgrades to the latest XGS Series easy.

Any-to-Any Backup and Restore with Port Mapping

The new Sophos Firewall backup and restore assistant enables firewall configuration backups to be easily restored on a different firewall appliance with flexible interface mapping options.

This makes it easy to upgrade Sophos Firewall XG Series to XGS Series, upgrade any XGS Series model to any other XGS Series model, or even migrate to or from software or virtual appliances. This also means you can easily migrate interfaces to higher-speed ports on your new or upgraded firewall.

You can also get creative and export a configuration template from a virtual appliance and then restore it on multiple hardware or virtual deployments to simplify a multi-device upgrade.



Easily map interfaces from the old to the new appliance

For more information on upgrading and the new backup/restore assistant, see this article.

Thank you for your participation in the Sophos Firewall v21 early access program!