SOPHOS

What's New in

Sophos Firewall

Key New Features in Sophos Firewall OS v20

Sophos MDR and XDR Integration

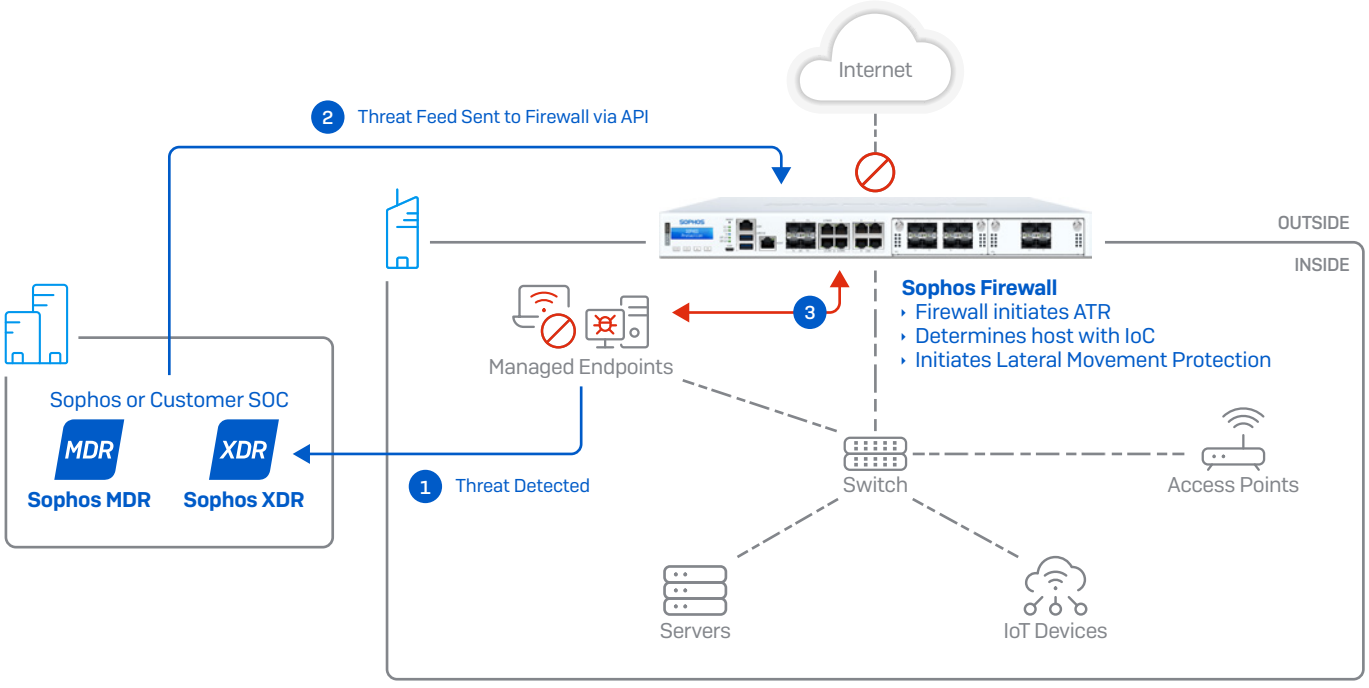
Active Threat Response

Sophos Firewall pioneered the concept of Synchronized Security, allowing cross-product communication and automation to identify and coordinate a response to threats. Sophos Firewall v20 extends Synchronized Security with new Active Threat Response that enables a security analyst (as part of the Sophos MDR team or customer's XDR SOC team) to share threat intel with the firewall in real time to respond to active threats on the network.

For example, if an analyst identifies a new threat communicating with a C2 server, the analyst can now push that information immediately to Sophos Firewall. This which 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 Heartbeat status to the device. No firewall rule configuration is required.

In addition, the Sophos Firewall will automatically block outbound traffic from any additional endpoints that may be ompromised and attempting to communicate with any threat feed IP address like a C2 server.

Active Threat Response provides the same Synchronized Security response as any other RED Heartbeat condition, including 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.



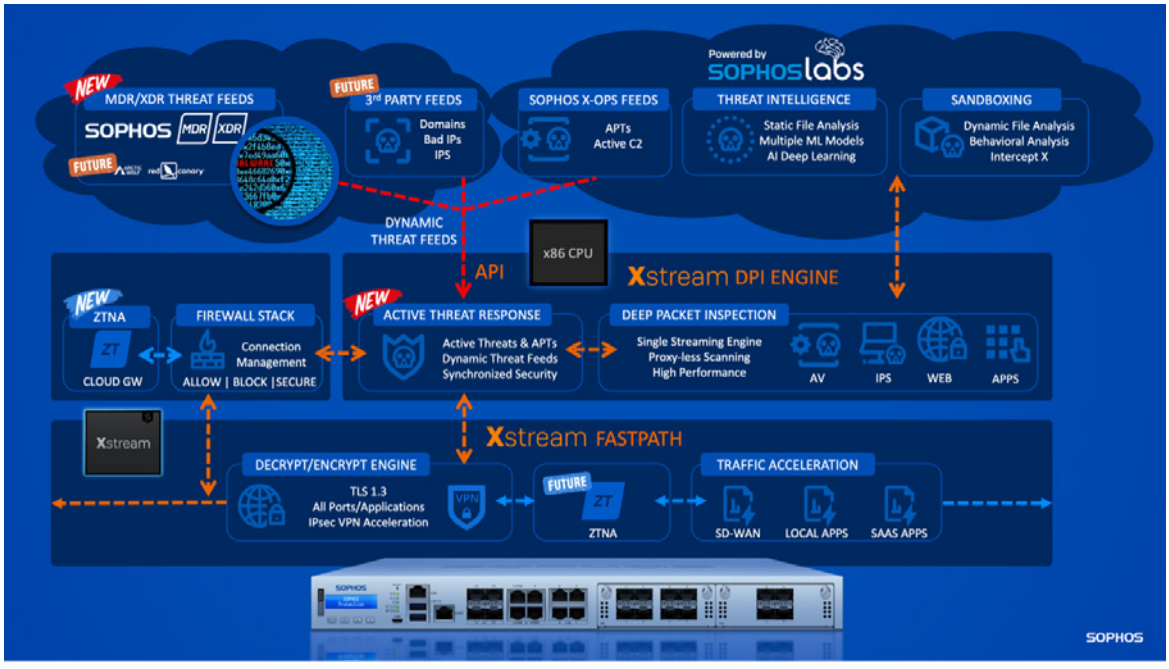
Synchronized Security IoC Telemetry

If a device attempts to connect with a blocked threat, Sophos Firewall will use the Synchronized Security Heartbeat to query details from that device, including host, user, process/executable, as well as the time and the event count.

Dynamic Threat Feeds

Active Threat Response introduces a new dynamic threat feed API framework in Sophos Firewall that is easily extensible. It enables threat intelligence to be shared from Sophos X-Ops, products, and services (initially) and ultimately third-party threat feeds in future releases. Active Threat Response is the first solution to use this concept.

The following illustration provides an abstract representation of Sophos Firewall's Xstream Architecture with the new elements and their relationships as well as future extensions.



Other Synchronized Security Enhancements

In addition to the great new Synchronized Security features mentioned above, we've also further optimized Synchronized Security and increased scalability:

Eliminate False Missing Heartbeats – Devices that are in sleep or hibernate mode will no longer generate a missing Heartbeat, reducing false alerts and notifications.

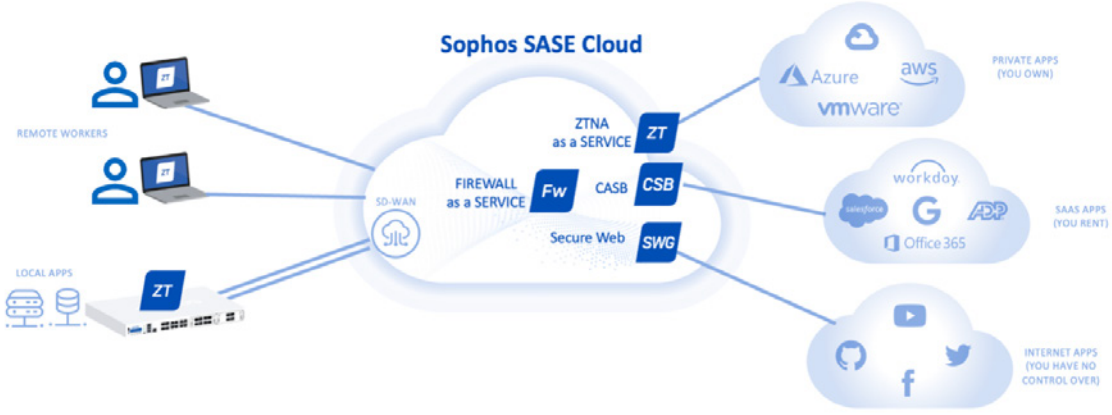
Synchronized Security Scalability – Synchronized Security optimizations mean we can now support up to 15,000 endpoints for those large organizations that are growing rapidly" to "rapidly growing organizations.

SASE and Remote Worker Protection

Pragmatic SASE – Enabling Remote Worker Protection

(SASE – pronounced "sassy") is the continued evolution of cybersecurity in the cloud – delivering network security solutions like ZTNA, SWG, CASB, and firewalling via the cloud to improve security for expanding distributed organizations. Sophos has been a leader in leveraging the cloud to deliver innovative cybersecurity solutions, and we will continue to do so as we transition into the future.

Sophos is taking a pragmatic approach to cloud-hosted network security services, delivering the key capabilities customers are looking to adopt first to secure remote workers and branch offices. We are starting with SD-WAN, ZTNA, and DNS protection and integrating them into Sophos Firewall (both on premise and hosted in the cloud) to make the transition easy and affordable.



ZTNA Gateway Integration

Zero Trust Network Access (ZTNA) is the ultimate remote-access VPN replacement. It provides better security, seamless scalability, easier management, and a more transparent end-user experience. Sophos Firewall v20 makes ZTNA deployments even easier by integrating a ZTNA gateway directly into the firewall. This means any organization that needs to provide remote access to applications hosted behind a firewall doesn't need to deploy a separate gateway on a VM – they can simply take advantage of the gateway integrated into their firewall. When combined with our single-agent deployment on the remote device, ZTNA couldn't possibly get any easier – it's literally zero-touch zero-trust.

ZTNA Free Trial

With the inclusion of a ZTNA gateway in every firewall with v20, we want to remind everyone that it's easier than ever to try ZTNA with the ZTNA free trial available in Sophos Central. This makes it easy for any network administrator to try ZTNA to manage their firewall or any other internally hosted systems and applications while getting the best security possible.

SD-WAN Backbone On-Ramping

While not specifically part of this release, we continue to build out our SD-WAN partnerships as part of our SASE strategy, and these are relevant and noteworthy to Sophos Firewall customers. Sophos has partnered with three top-tier SD-WAN backbone providers to enable smooth and easy on-ramping of local SD-WAN traffic to these high-performance global networks. These SD-WAN backbone providers include CloudFlare's Magic WAN, Akamai's Secure Internet Access (SIA), and Microsoft's Azure Virtual WAN. Sophos Firewall connects seamlessly to these networks, enabling high-performance connectivity and routing, as well as access to their SASE security services.

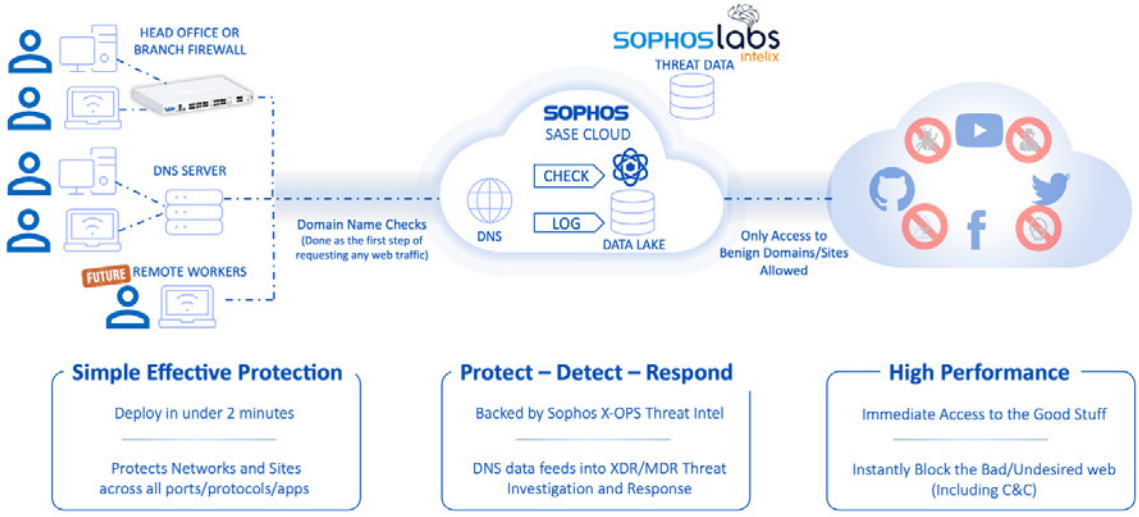
Full guides are available online:

- Cloudflare Magic WAN: Sophos KBA | Cloudflare Documentation
- Akamai SIA: Sophos KBA | Akamai Documentation
- Azure Virtual WAN: Sophos KBA | Microsoft Documentation

Sophos DNS Protection

This is also not specifically part of Sophos Firewall v20 but is worth mentioning here, as it overlaps with the Sophos Firewall v20 release and is an important new cloud-delivered web security service that will be available in early access very soon. It's very relevant to Sophos Firewall customers interested in SASE services.

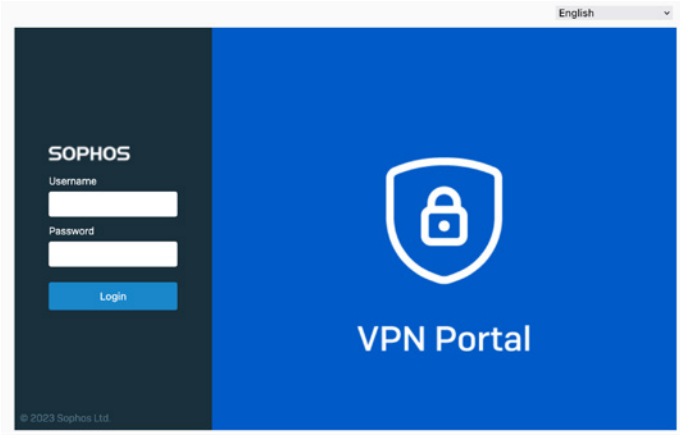
Sophos DNS Protection delivers a new Sophos-hosted domain name resolution service with compliance and security features that are fully supported by Sophos Firewall. This service provides an added layer of web protection, preventing access to known compromised or malicious domains across all ports, protocols, or applications – both unencrypted and encrypted. More information on this service and how to take advantage of it will be published in the coming weeks.



Distributed Networking: VPN, SD-WAN, IPv6, and Scalability

New VPN Portal

Sophos Firewall v20 introduces a new hardened and highly secure containerized self-service VPN portal for remote-access users. It provides remote-access self-service options such as downloads for the Sophos Connect Client, VPN configurations, auto-provisioning, and clientless VPN bookmarks.



The new portal is accessible from the previous user portal port of 443 to maintain compatibility and can share a common port with the WAF or SSL VPN.

The legacy user portal is now accessed via port 4443 or 65009 and continues to offer other services such as additional client downloads, email quarantine management, policy overrides, and hotspots. Note that we strongly encourage customers to NOT expose the legacy user portal to the WAN and only use the new VPN portal from outside the firewall.

VPN, SD-WAN, and IPv6 Enhancements

IPsec Connection Stateful HA Failover - Adds seamless transitioning for RBVPN, PBVPN, and remote access VPN without losing a session in the event of a high-availability failover. Also adds new command-line interface (CLI) options to manage settings.

FQDN Host Support for SSLVPN - Adds fully qualified domain name (FQDN) host and group support for SSLVPN remote access and site-to-site VPN.

IPsec VPN Tunnel Status Monitoring via SNMP - Adds support for monitoring IPsec VPN tunnel status via SNMP.

Multiple 0.0.0.0 (=*/ ANY) Remote Gateway Support for RBVPN – Eliminates the need for explicit DDNS in distributed multi-location deployments.

Unique PSK Support – Now supports unique PSK for VPN connections with the same local and remote gateway connections using IKEv2 policy with unique local and remote IDs.

DH Group 27-30 / RFC6954 – Support for IPsec VPN.

SD-WAN Scalability – Increased SD-WAN gateway scalability by 3x to 3072 gateways and the number of SD-WAN profiles to 1024

IPv6 DHCP Prefix Delegation – Seamlessly integrates with ISP-provided DHCP-PD for LAN networks, which automates the assignment of IPv6 prefixes to subnets, which simplifies network setup and reduces manual configuration overhead.

IPv6 BGP – Enhancements to the dynamic routing engine now support BGPv6 for improved IPv6 interoperability.

Quality of Life Enhancements

Interface Enable/Disable – A popular feature carried over from our SG UTM product line, you can now quickly and easily disable or enable interfaces on the firewall without losing any configuration. A new status of "Turned off" is shown directly on the Control Center for disabled interfaces. It is not possible to disable alias or tunnel interfaces or interfaces that are individual members of a LAG or bridge, however, you can disable the entire LAG or bridge interface.

Object Reference Lookup – You can now see the usage count of all host and service objects as well as a full list of all locations where that object is referenced such as in rules, policies, routing, etc. You can also directly edit or remove objects for many entities without switching context from the hosts and services list.

Hi-Res Display User Interface Scalability – The management console now takes advantage of high-resolution displays to scale the interface and enable tables to utilize full HD width (1920 pixels) to show more information, reducing the need to scroll horizontally.

Auto-Rollback on Failed Firmware Updates – If a firewall device fails to complete a firmware upgrade for any reason, including devices in a high-availability cluster, the device (or cluster) will be rolled back automatically to the previous firmware version, and an alert will appear in the Control Center.

Backup Restore Enhancements – Backups from a Sophos Firewall with integrated Wi-Fi can now be restored to a device without integrated Wi-Fi if the associated wireless networks are first removed before running the backup.

Azure AD SSO for captive portal – Sophos Firewall OS v19.5 added Azure AD SSO for the web admin portal. Version 20 now it adds support for user authentication to the captive portal using Azure AD credentials.

Azure Group Import – You can now take advantage of the new import assistant for Azure AD groups to import just those groups that match attributes you specify or import all groups. This eliminates the need to manually create groups.

Automatic Azure RBAC – If a user's role changes in Azure, the firewall will automatically promote them on their next login to their new role and apply the appropriate profile and privileges.

Web Application Firewall Enhancements

Geo IP Policy Enforcement – Provides the ability to block users from accessing WAF-protected resources from a specified country or IP addresses that can't be associated with a specific country.

Custom Cipher Configuration and TLS Version Settings – Enables the use of more secure ciphers and the exclusion of ciphers that are less secure.

Improved Security – Adds HTTP Strict Transport Security (HSTS) for HTTPS enforcement for the client browser and X-Content-Type-Options enforcement to disable MIME-type sniffing.

Azure Deployment Enhancements

Azure Single Arm Deployment Support – For Microsoft Azure public cloud deployments, customers can now choose a smaller instance size with single-arm deployments and save on infrastructure costs. This reduces network and operational complexity.

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

23-10-03 EN (DD)

SOPHOS