SOPHOS

Cybersecurity evolved.

XG Firewall v18 Webcast Questions

Date: November 2019

Sophos XG Firewall Community Webcast

This document includes a summary of the questions from the XG Firewall v18 community webcast held on November 14, 2019. The content covered new features and an overview of the new Xstream Architecture. All information is correct as of November 2019. As is the nature of software development, any information given regarding the availability of features or software release dates provided may be subject to change.

General

Q. When is the scheduled release date of v18?

The planned release date is late January 2020. Prior to that there will be further EAP (Early Access Program) releases. EAP 2 was released on November 19, 2019. EAP 3 is scheduled for December 2019.

Q. Will a video download of the presentation be made available?

A recording of the webcast is available under https://vimeo.com/373499629

Q. We are using Cyberoam hardware with XG v17. Can we upgrade to v18 on the same appliances?

No. Cyberoam hardware appliances will not be supported in v18. Please refer to the things you need to know before you upgrade section under https://community.sophos.com/products/xg-firewall/sfos-eap/sfos-v18-early-access-program/b/blog/posts/sophos-xg-firewall-v18-eap1_5f00_refresh1-firmware-has-been-released

Q. Will the Xstream Architecture be available for SG appliances?

Customers who have migrated to XG Firewall (SFOS) on an SG Series appliance may be able to benefit from the Xstream Architecture. This will depend upon the revision number of the appliance. Further information on which appliances are supported in v18 will be provided shortly.

Customers running the Sophos UTM software on an SG Series appliance would need to migrate to XG Firewall (SFOS) on a supported appliance.

Q. Is the Sandstorm license included in TotalProtect?

The **Sandstorm Protection** subscription will have significantly enhanced functionality from v18 onwards. Through the addition of SophosLabs Threat Intelligence Analysis, customers have access to both static and dynamic malware analysis using Deep Learning. This license is part of the bundles which end with 'Plus', e.g. TotalProtect Plus, EnterpriseProtect Plus, FullGuard Plus, etc.

Q. Is v18 backwards compatible with previously created backups?

V18 is compatible with recent versions of v17.5, but older backup versions will not import successfully into v18 systems.

General (cont'd)

Q. A number of features are said to be in the backlog. Can I see that somewhere?

We do not publish our long-term roadmap or the backlog. Please contact your Sophos Partner or local Sophos Sales office if you have questions regarding a specific feature request.

Some of the following features were mentioned as in backlog or under consideration for future release but no specific dates were provided:

- Disable interfaces in the user interface
- Dynamic search and object search
- Groups in Sophos Connect
- DHCP and DNS - automatic reverse lookups
- OS or device detection
- Port-scan detection
- Let's Encrypt support
- Deploy browser certificates via Synchronized Security

The following features are currently NOT planned or in backlog:

- 'Live Connections' Flow Monitor per interface
- Drag and drop interface (similar to Sophos UTM)
- Colored groups for firewall rules (similar to Sophos UTM)

Q. Will Sophos release a new Sizing Guide for v18?

We plan to provide sizing assets for the v18 release. We are moving away from the per user sizing guide that we previously had to a new approach. There will also be an additional training module on how to do sizing. For more complex cases, your local Sophos SE has access to both a sizing tool (which we may make available to partners via the Partner Portal) and a sizing desk, so please reach out to your local Sophos team for further help.

Q. Are there any changes to zero-touch deployment in v18?

Zero-touch deployment will continue to use a USB stick in v18, as it does today. We are planning to remove the need for the USB stick in the future and will let the XG Community know once that is scheduled.

Q. Can you explain extended VLAN which is shown as coming in EAP 3?

This is an advanced L2 deployment scenario and will close some feature gaps between XG Firewall and SG UTM, incl. VLAN filtering, non-IP protocol filtering by specifying the Ethernet frame type, ARP broadcast, STP configuration, etc. More information will be provided upon release of EAP 3 and after launch.

Q. Logs: Currently the log files are overwritten if they reach a specific file size. Are there plans to change this?

We are planning to replace the legacy 'garner' logging service with a more modern syslog-ng implementation in a future release.

General (cont'd)

Q. Logs: When will we see the ability to review/search raw log files?

The new log viewer is equipped with very comprehensive search and filtering capabilities. You can either search based on free text or filter all logs using structured filters. We have both the simple column view plus the more detailed view for raw logs.

Q. HA: Are virtual MACs still used or is it a completely new implementation?

It is a new implementation. We are eliminating the challenges with existing VMAC and will provide further information on this at a later date.

Q. Migration: Is there anything new to report about the migration tool to move from Sophos UTM to XG?

There have been no changes to the tool. We would recommend working with your local Sophos team as there are a few scenarios where the migration tool may not be recommended, and if you match one of those, the Sophos Professional Services team is setup to help with more challenging migrations.

Q. WAF: When will Site Path Routing be configurable?

It is labelled path-specific routing in XG, and is available as part of the WAF rule. Path rules may be created by enabling the mentioned option.

Xstream SSL Inspection, New DPI Engine, FastPath

Q. Are all TLS versions supported?

All TLS versions are supported, including TLS 1.3. SSL versions 2 and 3 are not supported for decryption.

Q. How is it possible for the firewall to decrypt SSL and see traffic? Isn't the whole point of secured traffic that it can't be looked at?

SSL/TLS interception has been possible for a long time, including on previous versions of XG.

The point of SSL/TLS is that it can't be intercepted and decrypted without being detectable by the end-user. It is done by replacing the keys and certificates used by the server with locally trusted certificates. It is necessary for any end-user devices to add and trust these certificates on their devices. For managed devices, this can be done automatically through methods such as AD Group policies.

Q. Doesn't the implementation of SSL Inspection lead to a considerable performance hit?

SSL inspection of course does have a performance toll on any network appliance. However, the new Xstream SSL Inspection engine is not based on a traditional HTTPS application proxy. It is a lightweight TCP layer proxy with additional optimizations as the process is integrated in the new DPI engine.

Xstream SSL Inspection, New DPI Engine, FastPath (cont'd)

Q. Will the Xstream Architecture provide the ability to inspect HTTPS sites without a certificate on the firewall or installed on the user's browser?

No. It is still necessary to install a root certificate in the client devices that will be used on the firewall to replace the site certificates, as with any SSL/HTTPS interception technology.

Q. Are there any plans to integrate the TLS/SSL inspection rules with the firewall rule system?

We do not intend to couple SSL policies with firewall policies. Organizations need to control what they decrypt as a separate policy model to what they enforce with a firewall rule. In many ways, it simplifies the experience as you can decide what needs to be decrypted or bypassed from decryption without having to worry about any dependency on firewall rules, ordering of rules, and how exceptions are handled.

Q. With Web Filtering using TLS interception rather than the proxy, will SafeSearch be possible in the future?

SafeSearch, depending on the content provider, does still require the proxy. We are looking to add specific hosts in XG to make it easy to define proxy policies for those specific sites. In that way, you can rely on DPI and TLS for everything else, and use the proxy for the specific SafeSearch sites. For Google at least, there are safe search enforcement alternatives which do not require the firewall, e.g. inserting a DNS record into your DNS server.

Q. With SSL inspection, can I block or allow specific videos on platforms such as YouTube and would I need to use the DPI engine or the proxy to achieve this?

If you have URL-based rules to block or allow specific videos, you will be able to enforce that with the DPI engine. If you rely on Google's methods (enforce restricted mode or use GSuite authorization with domain login restrictions) you will need to continue using the proxy.

Q. If an application does end-to-end trust checks or only allows connections to a trusted root certificate store which it manages, connections could fail. Are there plans to add to v18 to support this and get better visibility into failed connections when using the TLS interception architecture?

We are improving the visibility of such issues in v18 with the new view of failed connections in the Control Center, along with the ability to quickly add such sites to exclusion lists. However, we are also looking at trying to find more automated ways to back off these kinds of connections when failures are seen. This is something that will continue to improve over following releases.

Q. Wireless and BYOD have introduced a number of challenges, e.g. proxy avoidance apps such as X-VPN, Psiphon, etc. The Sophos application filters currently do list these but do not seem to block them. Will this be different in v18?

We have a KBA that describes the settings that we would recommend today to help you block evasive applications, such as Psiphon https://community.sophos.com/kb/en-us/132436 which are based upon v17.5. Please work with your local Sophos SE on this and have them escalate to the product team if the KB doesn't resolve it for you.

Xstream SSL Inspection, New DPI Engine, FastPath (cont'd)

Q. With the new Xstream Architecture, if something is inspected through the DPI engine and validated as OK and then allowed to use the FastPath, is there a risk that something malicious could be added to the traffic at that point?

Intelligent Offloading is done on a per-connection basis facilitated by data from Sophos Labs. The decision to offload is always made in a way that is appropriate for the kind of traffic and for the risks associated with that traffic. Administrators have the choice to inspect all content or to only inspect traffic that Sophos Labs considered untrusted.

Authentication, VPN

Q. Will it be possible to import users?

This is already possible today.

Q.VPN: is it possible to bind SSL VPN (e.g. port 443) to specific IP/interfaces?

You can control which IPs it will answer on by creating an ACL rule under Device Access settings.

Q. Are there any enhancements to STAS and AD authentication?

We are working on some improvements for the STAS agent. This will not be ready at the same time as the v18 release, but we hope to be able to release it not long afterwards.

Q. Do you plan to have authentication before VPN for clients?

Sophos Connect supports running logon scripts after logon, which is the primary reason users ask for a client that connects before logon.

Q. Can users be synced to Azure AD?

XG provides integration with traditional Active Directory/LDAP servers. XG does not provide a mechanism to sync users to Azure. Microsoft does provide a service to sync users from traditional active directory to Azure, although, XG does not integrate with Azure natively.

NAT

As there were a number of very similar questions regarding the decoupling of NAT rules from firewall rules, and as this is a topic which has seen much debate on the XG Community, the response to those questions is summarized here.

Q. Why are NAT rules decoupled from firewall rules?

With v18, XG firewall has moved towards the more standardized NGFW NAT design in which network translation configuration is now decoupled from firewalling configuration for better manageability in many deployments.

We have found that by binding everything together in a single policy it severely hampered deployments with anything beyond basic networks. In some cases, partners have found it literally impossible to migrate to XG from competing firewall vendors. For example, there are cases where NAT is required without impacting firewall ordering processing or security policies. The intersection of NAT and FW is clear in environments with basic requirements but less so in larger environments. Decoupling these items provides a greater degree of flexibility and is a requirement for supporting customers with more complex requirements.

From v18, NAT is now a separate rule table that will be traversed as a top to bottom prioritized rule set for network translation decisions.

For further details, please refer to the Recommended Reads in the v18 EAP section of the XG Community https://community.sophos.com/products/xg-firewall/sfos-eap/sfos-v18-early-access-program/f/recommended-reads/116102/understanding-new-decoupled-nat-and-firewall-changes-in-v18

Q. Will there be grouping of NAT rules?

We are not planning to group NAT policies today, but if there is a scenario where you see this as a requirement, we are interested to hear more details.

Q. Is NAT translation handled entirely in wire speed FastPath?

Yes, this will be the case once a NAT decision is made and the connection is marketed as trusted/eligible to go via FastPath.

Management in Sophos Central

Q. When will Central Firewall Management be equivalent to SFM/SUM/CFM in terms of rules, categories, policies, etc.?

We are constantly adding to the functionality of Central Management and are placing our focus on this platform to eventually replace SFM and CFM and make it into a more capable platform to manage firewalls.

Q. Will we be able to create templates in Sophos Central as we can in SFM?

Templates are not necessary in Sophos Central. The group that you assign a firewall to becomes the template that is assigned to it. As you make changes to the group policy, the changes are updated on all group members. Nested group support will also be added later in the EAP.

Management in Sophos Central (cont'd)

Q. How can I manage licenses via Sophos Central?

Firewall licenses are not yet manageable in Sophos Central but we are planning to add support after group management is released.

Q. Are there plans to allow multi-tenant support for synchronized security? We have a number of sites that have multiple Sophos Central tenants sharing a single hardware firewall. At the moment, we can't enable synchronized security since the XG can only talk to one Central tenant at a time.

Yes, we are planning to integrate into the Sophos Central Partner and Enterprise dashboards next year, after group management is launched.

Q. Is it possible to add custom roles to allow firewall management only in Sophos Central?

This functionality is on the Sophos Central near-term roadmap for Central Admin and has been added to the Central Partner and Enterprise dashboards for use with some products. We would suggest keeping an eye on the Sophos Central release notes blog https://community.sophos.com/products/sophos-central/b/blog and will certainly inform you once this functionality is available for XG Firewall.

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

© Copyright 2019. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.
191126 EN (PMM_BLH)

SOPHOS