Early Access Program (EAP) Evaluation Guide for XG Firewall v18

SOPHOS

XG Firewall v18 EAP 1 Feature List

Sl#	Features
1	NAT Enhancements – Decoupled NAT Rules and Linked NAT Rule
2	Firewall Rule Improvements
3	Xstream Architecture (DPI, SSL, FastPath)
4	Sandstorm Threat Intelligence Analysis
5	Sophos Central Firewall Reporting and Management
6	SD-WAN Policy-based Routing Enhancement
7	Interface Rename
8	DKIM and BATV Anti-Spam Protection
9	AD SSO Kerberos Authentication and NTLM
10	Radius Timeout with Two-Factor Authentication (2FA)
11	Use sAMAccount Name for AD Users
12	Wildcard domain Support in WAF
13	ECC Type Private Key Support for Certificate and CA
14	Upgrade to SFOS v18
15	Log Viewer Enhancements
16	Alerts and Notifications
17	SNMPv3
18	Improved Synchronized Application Control Verdict for Managed Endpoints
19	Enhanced DDNS Support

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
NAT Enhancements – Decoupled NAT Rules and Linked NAT Rule	XG Firewall's NAT configuration receives some major updates. NAT rules are now decoupled from firewall rules, enabling more powerful and flexible configuration options, including Source (SNAT) and Destination (DNAT) in a single rule. In addition, a new linked NAT rule feature follows the matching criteria of the Firewall Rule. Linked NAT Rule can also be added and edited in place while creating/editing firewall rules. Only the source translation configuration needs to be selected for Linked NAT Rule.	**Task:** Expose an internal resource intended for public consumption to the internet, (e.g., a web server, email server, etc.) 1) We'd like you to use the firewall rules along with the new NAT policies to create a policy that will inbound access from the internet to your specific resource (e.g., a webserver). The policy should have inbound NAT policy, and outbound, and a loopback NAT policy.	• Were you able to complete the task and verify that the public server is exposed to the internet? • Can you reach the public server from inside network with its external IP address? • If not, what problems did you face? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field>	

Notes:

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to Week2)	Feedback	Worked (Y/N/Free Text)
Firewall Rules Management Improvements	Firewall rules management includes a new 'Add Filter' option with several fields/conditions from which to choose. Adding a filter makes it easier to find firewall rules based on the selected filter criteria. Once selected, filters stay selected even when the administrator moves to other configuration screens. Administrators can manage multiple firewall rules at the same time (e.g. select multiple rules to delete, enable/disable, attach to a group, etc.). Movement of rules across screens is possible, providing ease of use and management for larger rule sets. Within the firewall rule there is an exclusion feature that provides a "negate" option in the matching criteria to reduce the management and ordering overhead of multiple rules. There's also a UI option to reset the data transfer counter for a firewall rule to improve troubleshooting.	**Task:** Expose firewall rule management with extended filtering option 1) We'd like you to use the firewall rules management with multiple scenario like select multiple rules to delete , enable/disable/attach to group	• Were you able to manage firewall rule seamlessly • were you able to delete/enable/disable multiple firewall seamlessly • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice, etc. <free text field>	

Notes:

XG Firewall v18 EAP1 Evaluation Guide

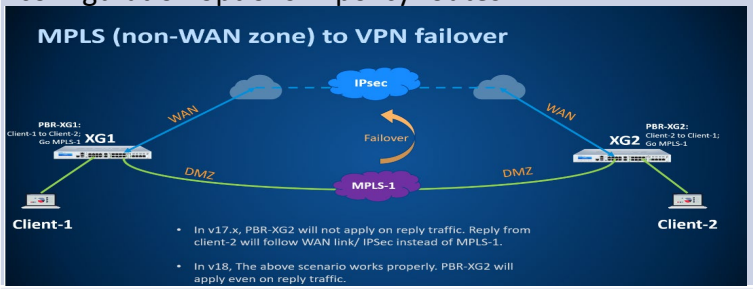
Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Xsrream Architecture	Sophos is pleased to introduce the new Xstream Architecture for XG Firewall , a new streaming packet processing architecture that provides extreme levels of protection and performance. The new architecture includes: • **Xstream SSL Inspection** – Organizations can enable SSL inspection on their networks without compromising network performance or the user experience. It delivers high-performance, high-connection-capacity support for TLS 1.3 and all modern cipher suites providing extreme SSL inspection performance across all ports, protocols, and applications. It also comes equipped with enterprise-grade controls to optimize security, privacy, and performance. • **Xstream DPI Engine** – Enables comprehensive threat protection in a single high-performance streaming DPI engine with proxyless scanning of all traffic for AV, IPS, and web threats as well as providing Application Control and SSL Inspection. Pattern matching on decrypted traffic makes patterns more effective and provides increased protection from hash/pattern changing applications such as Psiphon proxy. • **Xstream Network Flow FastPath** – Provides the ultimate in performance by intelligently offloading traffic processing to transfer trusted traffic at wire speeds. FastPath offloading can be controlled through policy to accelerate important cloud application traffic, or intelligently by the DPI engine based on traffic characteristics.	**Task#1:** Allow internet access for internal users with a DPI policy set to protect the internal network. 1) We encourage you to use different types of applications, voice and video communication. Access different websites, etc. through the DPI policy. 2) We would like you to explore the performance experience with Network Fast Path (NFP).	• Did you encounter any issues with the traffic/applications, (e.g., websites blocked or streaming stuck)? • Did websites/files get blocked as expected and did you get feedback, why a website/file was inaccessible/blocked? • Did you experience any improved performance with certain traffic or when accessing any application?	
		Task#2: Allow internet access for internal users through an SSL Policy (Deep SSL inspection). 1) We would like you to explore the SSL Policy advanced configuration with different combinations such as traffic decryption on/off, allowed TLS versions/ciphers, etc... and access different websites with different SSL/TLS versions/ciphers.	• Did you experience any unexpected drop in legitimate SSL traffic? • Did you notice any improvement in blocking configured/unwanted applications? • Did you encounter any issues with non-browsers applications that use SSL? • Did you see any behavioural differences with different browsers such as Chrome, Firefox, Safari?	

Notes:

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Sandstorm Threat Intelligence Analysis	Sophos Sandstorm gains an added layer of artificial intelligence protection. All suspicious files are now subject to threat intelligence analysis in parallel with full sandbox analysis. Files are checked against SophosLabs' massive threat intelligence database and subjected to our industry-leading deep learning, which identifies new and unknown malware quickly and efficiently – often rendering a verdict in seconds – to stop the latest zero-day threats before they get on the network.	**Task:** Allow internet access to internal users using Sandstorm protection for web and email traffic. Please download different files in the internet to evaluate the improved Sandstorm activity view.	• Did you see any delays in file downloads, unexpected blocks or false positive detection? • Did you find it easier to get information on files that were submitted to Sandstorm?	
Sophos Central Firewall Reporting and Management	This release includes support for new firewall reporting and management capabilities being launched simultaneously on Sophos Central including a rich, powerful new reporting suite and group firewall management tools.	**Task:** Integrate your XG firewall Reporting with Sophos Central and explore your XG Firewall reporting available on Sophos Central.	• Were you able to complete the workflow? • Please share your experience on ease and efficient report customization on Sophos Central.	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
SD-WAN Policy-based Routing Enhancement	Policy-based routing gains added SD-WAN flexibility and more granular control. Routing can be defined through either the primary or a backup gateway WAN connection and can be configured for replay direction. Additionally, routing decisions are now decoupled from firewall rules and merged with SD-WAN policy-based routes, enabling more powerful and flexible configuration options in policy routes. 	**Task:** Allow internal resources access on different sites of premise connected using VPN tunnel having failover-failback configuration, and also the sites are connected via links such as MPLS and backup link is secure tunnel VPN/RED. Explore the routing rule using given granularity and on non-WAN zone based route policy.	• Were you able to complete the task and access the network resource in-between the sites? • Were you able to achieve your network resource access on a non-WAN zone based route policy?	
Interface Rename	Interfaces can be renamed, making networking configuration easier and more intuitive.	**Task:** Change the interface display name to one that is more logical and familiar according to your network topology and consume it in various subsystems.	• Ease of use using Interface name?	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
DKIM and BATV Anti-Spam Protection	Anti-spam protection is improved with support for Domain Keys Identified Mail (DKIM) which detects forged sender addresses and Bounce Address Tag Validation (BATV) to determine, whether the bounce address specified in the received email is valid and reject backscatter spam.	**Task:** Configure DKIM signing for your domains to sign the outbound mails. Also, enable DKIM verification to validate the inbound messages received by the XG Firewall. Configure BATV secret and enable BATV via SMTP profile to validate the bounce messages received by XG Firewall. Also, explore the exception policy which allows you to skip the DKIM signing, DKIM verification and BATV based on the source hosts, sender address and recipient address.	• Provide input on the general understanding of the feature, and its usability. • Also, provide your input on how simple is to set up this deployment scenario.	

Notes:

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Kerberos Authentication and NTLM	This release adds Kerberos authentication alongside the existing NTLM support for Microsoft Active Directory SSO, extending the range of authentication tools available.	**Task:** Integrate XG Firewall user authentication with Active Directory, where SSO Authentication would be done using Kerberos Authentication and NTLM.	• Were users be able to authenticate successfully and reach the internet? • Did users get presented with the Captive Portal in case of failure to authenticate? • Did you experience any difference with NTLM and Kerberos Authentication? • Did you experience any issues with certain browsers?	
Radius Timeout with Two-Factor Authentication (2FA)	For customers using 2FA with Radius Server Authentication, the timeout value is now configurable, allowing additional time to finish the authentication flow when necessary.	**Task:** Integrate your XG firewall using 2FA with a Radius Authentication server. Verify your remote access user could authenticate with that server. You are encouraged to use Sophos connect, our SSL VPN client on XG as a remoter user.	• Could you successfully log in and access the resource(s)?	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Use sAMAccount Name for AD Users	For organizations with user names that differ by character with a diacritic mark. For example - John and John can be only treated as single user now in XG Firewall. With this support, we are implementing Microsoft Windows logon behaviour. If the user's name contains characters that have accents or other diacritical marks, he/she would be treated as single user only in XG.	**Task:** Integrate XG Firewall User authentication with Active Directory. Log in as normal with the diacritical user's name. For example, Rana and Rana.	• Did you see both users logged in on XG Firewall?	
Wildcard Domain Support in WAF	Wildcard domain support in Web Sever Protection (WAF) added for ease of use for XG's Admin. Say, for example, you are adding domain in single Web Server Protection (WAF) like a.sophos.com and b.sophos.com so now you can add *.sophos.com and access from external world as you access earlier.	**Task:** Protect your internal web servers having same domain name (sales.sophos.com, marketing.sophos.com) with WAF using wildcard domain (*.sophos.com) support. You are encouraged to try WAF with multiple domains in the same rule.	• Could you complete the task and access all domains publicly?	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
ECC Type Private Key Support for Certificate and CA	ECC (Elliptic Curve Cryptography) Type private key support for certificate and CA added to user latest encryption method. ECC promises stronger security, increased performance, yet shorter key lengths. Again ECC is FIPS-certified, like DSA, and endorsed by the National Security Agency.	**Task:** Deploy a web proxy with ECC type CA certificate. Let users access SSL-based web traffic. You are encouraged to configure different type curves and secure hashes.	• Were you able to complete the task and can users access the websites?	
Upgrade to SFOS v18	Upgrade from SFOS v17.5 MR6+ to SFOS v18	**Task:** Upgrade XG firewall to SFOSv18 from SFOSv17.MR6 (KBA link to be added) **You should experience a seamless transition switching to v18 from v17.**	• Please share your experience after upgrading to v18, for firewall rule management, NAT and SD-WAN policy route. • Did the firmware upgrade and switch to v18 work seamlessly?	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Log Viewer Enhancements	The log viewer has a number of enhancements with one-click actions available right from the logs to narrow search results, filter log entries or create or modify polices on the fly. Options include the choice to disable signatures, block a source IP address, edit interfaces, and modify IPS, App Control, or web filtering policies.	**Task:** Click any log parameter's value (most values are clickable) on log viewer standard or advanced view – add value on filter and free text search field. Click any log parameter's value (example – Src IP, Signature Id, IPS/App/Web Policy Id, Website, URL) on log viewer standard or advanced view – Take action directly from the logviewer	• Were you able to block the Src IP with local ACL exception rule with just one click from the log viewer? • Were you able to disable this SID into the same IPS policy, edit app/ web/IPS policy, create custom URL group, create acceptable or objectionable website category with just one click from the log viewer? • Please provide additional feedback on the overall experience, considering ease of use, intuitiveness, configuration choice.	
Alerts and Notifications	There is a new option to choose from dozens of system and threat-related alerts and have notifications sent via email or SNMP. Now, the XG admin will have the option to enable the management interface through which email is sent.	**Task:** Explore XG Firewall's system and threat-related Alerts and Notifications via email or SNMP trap.	• Could you get Email notification for configured critical events of XG Firewall?	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
SNMPv3	SNMPv3 support is added to provide more flexibility and security over SNMPv2.	**Task:** Explore SNMPv3 walk and trap functionality with XG Firewall using new MIB.	• Could you get SNMP trap over SNMPv3? • We would encourage you to use SNMPv3 with different types of encryption and authentication algorithms. • Which SNMP server did you use for SNMPv3? (Subjective/Text input)	
Improved Synchronized Application Control Verdict for Managed Endpoints	In case of pattern based match conflict, Sync App Control Verdict will be adhered for more accurate application control.	**Task:** Deploy Sync App Control and upgrade to v18 on XG where Sync App Ctrl has already been configured.	• Have you observed more granular application classification with managed endpoints? • Did you experience any issue with Sophos endpoint?	
Notes:				

XG Firewall v18 EAP1 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Enhanced DDNS Support	Provides support for enhanced DDC service HTTPS-based DDNS by adding five more DDNS providers – No-IP, DNS-O-Static, Google DNS, Namecheap, and FreeDNS.	**Task:** Configure different types of DDNS accounts and use them as web admin host, VPN host, etc. You are encouraged to configure new DDNS service providers.	• Were you able to complete the deployment with different types of DDNS? • Could you get appliance access using the new added DDNS account?	

Notes:

XG Firewall v18 EAP2 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
User-based SD-WAN Policy-based Routing Enhancement	Policy-based routing gains added SD-WAN flexibility and more granular control. Routing can be defined through either the primary or a backup gateway WAN connection and can be configured for replay direction. Additionally, routing decisions are now decoupled from firewall rules and merged with SD-WAN policy-based routes, enabling more powerful and flexible configuration options in policy routes. With EAP2 , we have added support of policy based route with User identification	**Task:** Allow external resources access using specific WAN uplink, having user identity attached in policy-based route	• Were you able to complete the task and access the network resource in-between the sites? • Were you able to achieve your network resource access as per user identity?	
Notes:				

XG Firewall v18 EAP2 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
VLAN Bridge Support	VLANs are now supported on bridge interfaces, enabling greater networking flexibility and support for advanced inter-VLAN routing and bridging deployments.	Task: 1. Add VLAN on bridge interface 2. Add VLAN interface as member of bridge 3. Apply VLAN filter (Caveats: VLAN filter is not applied on routed traffic)	1. Were you able to set up VLAN a on the bridge interface? • Was traffic between two VLANs flowing as expected ? 2. Did you find the VLAN worked as expected? 3. Provide input on the general understanding of the feature and its usability.	

Notes:

XG Firewall v18 EAP3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
SD-WAN Application Routing and Synchronized SD-WAN	Policy-based routing gains added SD-WAN flexibility and more granular control. Routing can be defined through either the primary or a backup gateway WAN connection and can be configured for replay direction. Additionally, routing decisions are now decoupled from firewall rules and merged with SD-WAN policy-based routes, enabling more powerful and flexible configuration options in policy routes.	Task: 1. Route some of the application you are using in your network with SD-WAN rule application-based routing	1. Were you able to set up an SD-WAN rule and route desired applications with application based routing? 2. In which deployment scenarios did you found application-based routing useful? 3. Provide input on the general understanding of the feature and its usability.	

Notes:

XG Firewall v18 EAP3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Sandstorm Threat Intelligence Reporting	Sandstorm Threat Intelligence Reporting adds a new Control Centre widget to highlight all suspicious file downloads. The widget enables one-click drill-down to detailed forensics reports on all suspicious file activity. A quick summary view for each file provides a traffic-light style (red, yellow, green) indication of the analysis after antivirus scanning, threat intelligence analysis, and sandboxing. Detailed reports provide an-depth view of the verdict, including illustrated analysis by multiple machine learning models, details and screenshots of behaviors seen during Sandstorm analysis, and an in-depth breakdown of the file's features and attributes, together with malware scan results and insight from VirusTotal.	**Task:**		

Notes:

XG Firewall v18 EAP3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Bridge Interface Enhancements	1. Bridge interfaces now supports: 2. ARP broadcasts 3. Spanning Tree Protocol (STP) traffic, 4. Non-IP protocols by specifying the Ethernet frame type 5. Non-IP bridge	1. We would like to use ARP broadcast functionality in your deployment 2. We would like you to set up a bridge network with redundant links with STP enabled 3. We would like you test non-IP protocols filter 4. We would like you to set up a no-IP bridge (Caveats: Add no NAT rule in case the bridge interface member matches any of the configured NAT rule, and the legacy proxy will not work with non-IP bridge)	1. Did the ARP broadcast functionality working as expected? 2. Were you able to complete the deployment having redundant links with STP enabled? • Was traffic flowing properly as expected? 3. Did the Non-IP protocol filter work as expected ? 4. Were you able to set up a no-IP bridge? • Was traffic flowing properly between the members of the non-IP bridge with Advance Firewall policies? 5. Provide input on the general understanding of the feature and its usability.	

Notes:

XG Firewall v18 EAP3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Route-based VPN	Route-based VPN makes VPN setup easier to manage as it separates the VPN policy configurations from network topology configuration. In addition, it adds greater flexibility to how traffic is routed and how routes propagate over a VPN connection. Route-based VPN is the preferred choice in many deployments because it doesn't require the VPN policy to be reconfigured with changing networks.	Task: 1. We'd like you to use Route-based VPN to establish connectivity between your sites (Branch / HO static) 2. Explore various routing methods such as Static, Dynamic, and Policy-based with RBVPN 3. We encourage you to test the interop capabilities by establishing VPN connectivity with any third-party device (Router / Firewall)	1. Were you able to complete the task and set up VPN connectivity between your sites using RBVPN ? 2. Were you able to achieve routing over VPN with different routing methods (Static/Dynamic and Policy-based)? 3. Were you able to set up RBVPN with a third-party device ? 4. Provide overall input on the general understanding of the feature and its usability.	

Notes:

XG Firewall v18 EAP3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
NAT Enhancement	Based on feedback we received from community and insiders we have made following enhancements in NAT: 1. Support of DNAT wizard – easy workflow to configure NAT and Firewall rule 2. SNAT auto create for WAN Interface – auto-masquerading in place 3. More consistent NAT UI flow	1. Expose an internal resource intended for public consumption to the internet, (e.g., a web server, email server, etc.) using Server Access Assistant (DNAT) 2. Explore enhanced NAT rule creation UI	1. Please share your experience on ease of DNAT rule creation with Server Access Assistant (DNAT) 2. Have you found the default SNAT rule useful in your deployment scenario (does it saved your time)? 3. Have you found Manual NAT rule creation UI more consistent and easy to use/set up a rule compared to previous EAP versions?	

Notes:

XG Firewall v18 EAP3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
Flow Monitoring Improvements	The new real-time flow monitor provides at-a-glance insights into active applications, users, and hosts along with current bandwidth utilization and other important information with convenient drill-down capabilities. Administrators can now analyze bandwidth in real time via the Live connections screen. Also, they can add users, source IP, and applications under a single view, all of which equips admins to analyze live bandwidth utilization from different pivots.	Task: • Explore the live connection page for network traffic visibility	• Please share your experience with the enhancement we made in live monitoring.	

Notes:

XG Firewall v18 EAP2/3 Evaluation Guide

Feature List	Brief Introduction	Task List (Week1 to WeekN)	Feedback	Worked (Y/N/Free Text)
High Availability (HA) Enhancements	New enhancements enable plug-and-play high availability deployments with greater flexibility and business redundancy. A preconfigured HA port on every device enables quick and easy HA deployments by simply connecting the two ports together and then acknowledging and activating HA. HA configurations also include a configurable failback strategy, ideal for remote-site HA deployments, with options for manual synchronization and time out tuning. It is now possible to perform firmware updates, rollbacks, and other tasks such as port monitoring lists and assigning multiple IP addresses to primary and auxiliary appliances while HA is active. In addition, deploying more than one HA pair in a single network is easier due to the elimination of conflicts arising from any dependency on a virtual MAC address HA architecture.	Task: 1. We'd like you to set up HA using Quick HA mode 2. We'd like you to test the Update functionality and update any/combination of the following parameters: I. Keepalive timer II. Peer admin port III. Failback to primary IV. VMAC 3. We'd like you to use Rollback functionality	1. Please share your experience on the ease of configuring HA with Quick HA Mode 2. Were run-time 'updates' made to HA worked/synced as expected? 3. Did Quick HA reduce your overall set up/configuration time? 4. Were you able to seamlessly roll back to a previous version (without disabling HA)? 5. Provide overall input on the general understanding of the feature and its usability.	

Notes:

SOPHOS

Security made simple.