SOPHOS

XG Firewall v18 EAP 3 Refresh 1 Known Issues and Advice for Users

XG Firewall v18 EAP 3 Known Issues and Advice for Users

The following tables provide the latest information on known issues and their workarounds and advice for users for XG Firewall v18 EAP 3 Refresh 1 firmware.

Known Issues

Component	Known Issue with Explanation	Workaround
Base	QAT is enabled in new hardware revisions (XG 125/135 REV3, XG 750) → This was not working in v17.x QAT is not enabled in older hardware versions (XG 125/135 REV2) → This was working in v17.x	IPSes offload won't work regardless of CLI status for REV2 hardware
IPS-DAQ	The block page is not rendered correctly in Firefox. In some cases, when an HTTPS request is blocked, Firefox instead displays SSL_ERROR_RX_UNEXPECTED_APPLICATION_DATA.	No known workaround at this time.
HA	Starting with v18 EAP2, we have secure communication (SSH tunnel based) for configuration sync. This impacts our **"No downtime HA upgrade"** workflow when upgrading from v17.5 or v18 (i.e. <EAP2) as new secure communication keys aren't compatible with previous firmware versions. • There is no behavior change in the **"Upgrade Firmware Now and Reboot Later"** workflow as it is already **"Upgrade with Downtime."**	This behavior is expected.

	• The **"Upgrade Firmware and Reboot Now"** workflow is the **"No downtime"** upgrade. Due to previously mentioned improvement, there is a behavior change which will be **"Upgrade with Downtime."** **Note:** Customers will receive the following notification message in the user interface. "As the communication protocol for the HA cluster is upgraded in the new firmware, all the devices in the HA cluster will reboot simultaneously. Do you want to continue?"	
Web DPI / SSLx	When an HTTP connection is allowed by Web policy in DPI mode but not decrypted, it does not get logged in the Web Filter logs. This may impact Web traffic reporting.	If reporting of Web traffic is critical, use proxy mode for now.
Live Connection	In scale scenario of 1L+ contract entries in the system, it is seen that accesing the Live Connection page from two different session or starting Packet Capture while the Live Connection page is loading from another session, may show incorrect data or not be able to turn on Packet Capture.	Wait to start the packet capture until the Live Connection page loading is completed.
Web DPI / SSLx	When a client or server decides to terminate a TLS connection during the handshake but after the Client Hello and Server Hello, the connection is logged as successful. This means that the Log Viewer generally doesn't provide visibility into situations where the client rejects the re-signed site certificate.	No known workaround at this time.
SSLx	When a client terminates a TLS connection during the handshake, after the server certificate is received, it is a likely indication that the client considers the certificate invalid. For decrypted connections, this is a good indicator that either the client doesn't have the CA installed or that the connection is coming from an application that ignores added CAs, uses certificate pinning, or uses its own list of root CAs. We want to log and report on these errors separately from other types of terminations and expose them in the SSL remediation workflow on the Control Center.	No known workaround at this time.
IPS-DAQ/VFP	IPS fails to load on XG 550 if jumbo (>1500) MTU is configured on interfaces. Packet buffer allocation for IPS is using too much memory when buffers are jumbo-sized. On XG 550 this is preventing IPS from loading properly.	It is possible to work around with script/conf file changes (TBD - still testing)

NAT Rule	With default SNAT rule introduction, it's possible that WAN-bounded traffic will automatically start getting MASQ. In some scenarios such as MPLS-VPN failover/failback, it's not desirable to MASQ such traffic. This issue will be seen for v17.5.x to v18-EAP3-Refresh1 migration only (Not applicable to v18 EAP1/2/3 to Refresh migration) .	Disable (don't delete) the default generated NAT rule.
Firewall / Web	When 'Use web proxy instead of DPI engine' is selected and web policy is 'None', 'Scan HTTP and decrypted HTTPS' is not selected and 'Decrypt HTTPS during web proxy filtering' is not selected, traffic on port 443 is not forwarded to the web proxy. This mainly impacts customers who are creating proxy rules to work around apparent issues with the DPI Engine for certain traffic. This may also impact some users migrating from v17.5 who have firewall rules that direct traffic via the proxy even though they're not doing any web policy enforcement.	Selecting 'Allow all' as the web policy will cause all traffic on port 80 and port 443 to use the proxy without blocking any traffic.
Xstream SSL / TLS	Using Synchronized Security (Sync Sec) applications in SSL/TLS rules is not working reliably. Because of timing issues between the Sync Sec/Heartbeat data exchange and the policy decision on a new SSL/TLS connection, information about the Sync Sec app ID for connections is often not available when making SSL/TLS policy decisions. The net effect is that rules that match on Sync Sec applications do not work reliably	No equivalent workaround available at this time. Do not use Sync Sec apps in SSL/TLS rule criteria.
Web DPI / Xstream SSL/TLS	Applications or IoT devices that send traffic that is not HTTP and not genuine SSL/TLS over port 443 may fail because these connections are not recognized as web traffic.	Log into the device console and enter `set http-proxy relay_invalid_http_traffic on` Or, for a more targeted workaround, create a firewall rule specific to that destination, with web policy 'Allow all' and with 'Use proxy' selected.
IPSec	Kernel panic observed on AUX when creating an XFRM tunnel interface. The impact is on HA setup, when an RBVPN tunnel is configured, the Auxiliary node is unaccessible and kernel panic is seen.	Use RBVPN Tunnel interface without HA config as work-around.

Advice for Users

Component	Advice
SSL Inspection	**Deployment of SSL/TLS signing certificates is required for decrypted connections to be trusted by endpoint devices.** SSL Inspection offers significant improvements in decrypting and scanning SSL/TLS traffic over previous versions of SFOS. However, it still has to replace the original site's certificate with one created dynamically on the device. Copies of the re-signing certificates configured for use in Rules and Policies > SSL/TLS Inspection Rules > SSL/TLS Inspection settings should be installed on all endpoints whose traffic is to be decrypted. Failure to do so will result in browsers displaying certificate warnings, potentially preventing access to some sites. If you configure different re-signing certificates to use for certain profiles, copies of those certificates will need to be deployed to endpoints whose traffic is impacted by those profiles. Certificates can be deployed to managed Windows endpoint using Active Directory GPOs. **Even so, not all applications running on endpoints will trust the added certificates.** Although browsers will generally trust additional CAs, other applications may be written or configured to be stricter about checking the certificates. Some applications may have their own certificate trust stores, which cannot easily be updated other than by the app publishers. Some applications may use certificate pinning, where they check for specific known certificates, or that the certificate presented by the server is signed by a specific certificate authority. When enabling SSL inspection for a wide range of destinations and ports, some applications may experience difficulties. You will need to create new rules or modify existing rules to exclude such traffic from decryption. SFOS includes a range of exclusions for domains that we know to be associated with applications that do not respond well to SSL inspection. At this early stage in the release and live testing of SFOS we are still learning about how we can do a better job of detecting when applications drop connections because they do not trust our certificates. It is our goal before final release to provide better visibility of these situations in the SSL/TLS area in the Control Center so that users can more easily understand and remedy these issues.

	SSLVPN SSLVPN client apps, such as Cisco's AnyConnect, are known to fail when their SSL/TLS connections are being decrypted. When users behind a firewall are expected to connect to VPNs over SSL/TLS, the destinations should be excluded. It may be possible to do this by adding the VPN hostname to the 'Local TLS exclusion list' URL group, or by creating a new SSL/TLS inspection rule set to 'Do not decrypt' for the destination IP addresses of the VPN servers. **Recommended key types** With SFOS v18 you can create and use RSA or Elliptic Curve certificates. When configuring SSL/TLS inspection, we allow you to specify to different signing CAs. Which one is used depends on the type of certificate used to sign the original server certificate. In most situations, it is not necessary to provide both an RSA and an Elliptic Curve. All browsers and most other applications can handle both types of cryptographic algorithms and the protocols generally support the mixing of key types in certificate signing chains. However, there may be some situations where legacy or poorly-implemented applications cannot handle the mixing of algorithm types. Therefore, we allow you to choose to specify different re-signing CAs. Please note that although SFOS supports creating CSRs and certificates using three different Elliptic Curve parameters, only two are supported by all browsers. When creating CSRs for use as re-signing CAs, or as the server certificate for the SFOS Web Administration interface, we recommend to select only one of the following: secp265r1 (also known as prime256v1) secp384r1 Don't forget that if you choose to use two different re-signing CAs you will need to ensure that both are deployed to and trusted by all endpoints.
Bridge	XG Firewall v18 has a feature that allows configuring of the bridge without an associated IP address. When configuring a bridge interface without an IP address, features that require an IP address such as NAT rules and web filtering won't function.
SNMP	In the XG v18 implementation of SNMP, standard traps (aka well-known traps in RFC3418 and RFC2863) such as coldstart, warmstart, and link up/down traps), will be generated when there is an SNMP configuration update in SFOS.