SOPHOS

XG Firewall v18 EAP 2 Known Issues, Advice for Users and Incomplete Features

XG Firewall v18 EAP 2 Known Issues, Advice for Users and Incomplete Features

The following tables provide the latest information on known issues and their workarounds, advice for users and incomplete features for XG Firewall v18 EAP 2 firmware.

Known Issues

Component	Known Issue with Explanation	Workaround
Web / Sandstorm	The Sandstorm dashboard widget does NOT include new statuses introduced in EAP 1 (e.g. likely clean, suspicious) which results in misleading count results. Please ignore these widget readings in EAP 1 since the issue is scheduled to be updated with EAP 3 enhanced reporting.	Use the new Threat Intelligence page to determine the current count of jobs and statuses. GUI: Advanced Threat → Threat Intelligence
QoS (Quality of Service)	QoS will not work for traffic originating from or destined to a WiFi/3G/4G interface.	No known workaround at this time.
AppFilter/AppClass	Several SSL apps won't be classified.	Disable SSL/TLS inspection from the UI (Advanced settings under SSL/TLS Inspection settings).
Base	Upgrading the firmware from EAP 0 to EAP 1 fails on XG 125, XG 135, and XG 750.	Disable Intel QuickAssist. cish> system hardware-acceleration disable Reboot the appliance. Upload the firmware again.
Base	The QAT driver is not enabled.	IPSec offload won't work regardless of CLI status. This may affect IPSEC throughput.

IPS-DAQ	The block page is not rendered correctly in Firefox. In some cases, when an HTTPS request is blocked, Firefox displays SSL_ERROR_RX_UNEXPECTED_APPLICATION_DATA instead.	No known workaround at this time.
Web / SSLx	Failed session resumption attempts are included in the SSL/TLS remediation workflow in the Control Center, but do not necessarily indicate fatal problems that require a website to be excluded. SFOS keeps a cache of TLS session information so that it can successfully detect and re-establish TLS connections that are resumed by the client. That cache has a finite lifetime, and sometimes browsers will attempt to resume sessions that have been expired from our cache. This can be particularly noticeable when coming back to a browser that has been left open or asleep overnight. In this case, the firewall rejects the resumption attempt and the browser will usually transparently retry by establishing a brand new cryptographic session. The user experiences nothing except for possibly a very small delay. Firefox can be more sensitive to these issues and sometimes will display user error pages.	Before excluding traffic because it's listed as an error, check the detailed logs to see if it has session="1". If it does, this is an indication that the connection was an attempted session resumption.
IPS-DAQ	With SSL decryption, there is a chance that we run out of NSEI Ds. If this happens, no further decryption will occur. This can arise after the device has been running for a long period of time.	Reboot the system.
SNMP	MIB files for SFOS in v18.0 are referencing an incorrect enterprise number 2064. Sophos' IANA enterprise number is 2604. When using an enterprise MIB-based query this will map to an organisation for 2064 known as Aware, Inc.	Continue to use enterprise MIB-based queries with 2064 as the enterprise number. Change it to 2604 when the issue is fixed in the next refresh/rebuild.
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?"	
Logging Framework	Unable to start packet capture in the user interface on the following two pages: Diagnostics->packetcapture (Full page functionalites) Diagnostics->connectionlist (masterconnection id) The issue is seen intermittantly.	No known workaround at this time.

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.

Logging Framework (Central Firewall Reporting)	Central Firewall Reporting is not supported for the XG 86W which is a smaller flash-based device that do not support onboard logging. **Use an XG 115 or higher for the Central Firewall Reporting feature.**
SSLx	Prior to EAP 2, TLS session data was not being cleaned up on a regular basis, resulting in many files being stored in directories under /var/tmp. Over time, this may cause the /var partition to run out of disk space. In NC-42844 (merged in EAP 2), a job has been added to clean up these files on a regular basis. However, a one-time cleanup operation was required and has been added to the migration script for EAP 2. This process may take some time (depending on the number of TLS session data files that are stored on the device) and the device will be inaccessible during this portion of the upgrade. For most devices, this migration takes less than 10 minutes. The following steps can be used to perform this cleanup manually. Progress will be printed on the terminal so that the admin has an idea how long the process will take): `service -ds nosync ips:stop` `perl -e '$|=1; print "\nCalculating"; my $total = 0; for my $d (@ARGV) { print "."; opendir D, $d; @files = readdir D; closedir D; $total += scalar(@files); } print "\r0% "; my $pct = int($total/100); for my $d (@ARGV) { for my $f (<$d/*>) { unlink $f; if (--$total % $pct == 0) { printf "\r%d%% ", 100 - ($total / $pct) } } } print "\rDone\n"' /var/tmp/resumption_session /var/tmp/resumption_ticket /var/tmp/modified_cache /var/tmp/original_cache`  `rm -rf /var/tmp/resumption_session /var/tmp/resumption_ticket /var/tmp/modified_cache /var/tmp/original_cache`  `mkdir /var/tmp/resumption_session /var/tmp/resumption_ticket /var/tmp/modified_cache /var/tmp/original_cache`  `service -ds nosync ips:start`

Incomplete Features

Component	Feature	Missing Capabilities
Web / Sandstorm	Enhanced Sandstorm with Sophos Labs static analysis and improved reporting	Enhanced Threat Intelligence reporting is planned for EAP 3. With this build, you will see a simple report containing only the information that was available in v17.x, but delivered in a separate tab with a cleaner layout. Files detected as malware by on-box malware scanning are not yet sent to SLAP for analysis. The main Control Center view still shows the old counters for Sandstorm.
Web / SSLx	Web filtering in the DPI Engine (instead of proxy)	Handling of multi-part MIME HTTP request bodies. This may impact the ability to detect and report on HTTP Uploads and uploaded file names. Block pages for IPv6 connections may not appear correctly. HTTPS connections blocked by web policy are not logged to the Web Filter log. Undecryptable traffic using TLS compression is logged incorrectly. Web exceptions that specify 'Do not decrypt' will not match when the domain name has a trailing '/'. See above. Block pages may not work if the original page URL has multiple query parameters. When using AD SSO authentication (NTLM/Kerberos), user identity changes at an IP address may be missed for longer than expected. SSL/HTTPS inspection may not be completely port-agnostic. Logged server certificate fingerprint is truncated.
Web / SSLx	DPI engine uses NSE for decryption	SSL/TLS log lines with ID 19010 have no content fields. Some undecryptable traffic cannot be skipped without decrypting if it matches a SSL/TLS rule that says 'Decrypt'. This affects connections using SSLv3, unsupported cipher suites and TLS compression. See above.

		NPN extension is not removed on decrypted flows. This may result in the client and server negotiating HTTP/2 which will result in a parser error and dropped connection. Note: NPN was replaced by ALPN. This issue should not be seen unless you are running old versions of browsers or other older client software.
Web / SSLx	SSLx policy controls decryption features	SSLx does not yet remove unsupported cipher suites from the client hello, which can increase the chance that the client and server will negotiate a cipher suite that SFOS cannot decrypt. Bandwidth counters on SSL/TLS inspection rules will always show zero. Policy tester does not link SSL/TLS rule ID in results to the SSL/TLS rule editor. Cannot filter SSL/TLS rules. The policy configuration for exceeding the max SSL/TLS connection limit is not implemented. Use of FQDN objects in SSL/TLS rules is not yet supported. The content of read-only Decryption Profiles cannot be viewed. Control Center connection counts may not be accurate.
VFP	Jumbo frame support	VFP will not load if an MTU greater than 1500 is configured on any interface. Error logs showing this will be present in syslog and applog. The device will otherwise still be functional without VFP loaded, but traffic will not be offloaded.