SOPHOS
Security made simple.

Sophos XG Firewall v16.01.1

Contents

New Features & Issue Resolved in SFOS v16

NC-9657 :	API	Fixed the issue of firewall rules imported using API not getting edited
NC-12227 :	API	Fixed the issue where user is unable to use more than 6 characters as TLD in Notification Settings
NC-89 :	Authentication	SFOS will act as an OTP Server and provide OTP based authentication to clients
NC-5457 :	Authentication	To enhance security and privacy of Local user created on appliance, SFOS will have their password stored in database in encrypted format.
NC-7071 :	Authentication	Unable to filter SSO users in Live User list is now fixed.
NC-10511 :	Authentication	Simplified dropdown list objects “Connection Security” while adding Authentication Server
NC-7151 :	Authentication	Fixed the issue of "Search Query" in authentication server not getting validated and resulting in authentication failure
NC-5186 :	Authentication	Fixed the issue of SSL VPN not getting connected with Long Domain Name
NC-6284 :	Authentication	Added some additional attributes in radius test connection request
NC-11347 :	Authentication	Fixed the issue of User Settings not getting edited in case user is authenticated through Active Directory
NC-2806 :	Authentication	Fixed the issue where user name with special characters are not getting in Live
NC-11581 :	Authentication	Fixed the issue with API import/export of users
NC-12162 :	Authentication	Fixed the issue where user with @ in username is not able to login to User Portal
NC-8623 :	Authentication	Fixed the spelling mistake on Add LDAP server page
NC-11584 :	Authentication	Fixed the issue where live users got disconnected due to Segmentation Fault in Authentication Service
NC-11847 :	Authentication	"show encrypted password" Option is removed from UI
NC-12113 :	Authentication	Fixed the issue where Remote Users page is not loading in Internet Explorer 11
NC-12260 :	Authentication	Fixed the issue where Importing local users through CSV was getting failed
NC-12552 :	Authentication	Fixed the issue where user is unable to import groups containing Apostrophe (‘) in their names
NC-12730 :	Authentication	Fixed the issue where AD users were taking long time to authenticate using Captive Portal
NC-12824 :	Authentication	Fixed the issue where admin couldn’t revert CCL for OTP feature from SFM
NC-12876 :	Authentication	Fixed the issue where User Portal was showing Auto-generated token for OTP only if Auto-creation is ON in OTP settings
NC-13233 :	Authentication	Fixed the issue where Enterprise Authentication was not working for remote AP
NC-12697 :	Authentication	Fixed the issue where Authentication title was missing on Authentication → STAS page
NC-12844 :	Authentication	Fixed the issue where importing local users through exported CSV doesn’t respect groups
NC-5236 :	Base System	Secure shell access with Public Key authentication Support
NC-5593 :	Base System	Improved "Interface" widget, clicking on interface widget will take you to new flip-card label i.e. "Connection & Interfaces" which contains all interface status along with the gateway as well as respective appliance static image.
NC-5594 :	Base System	Graph Enhancement in Control Center, clicking on Graph data in Traffic Insight widget will redirect to respective filtered report in “Report” section. E.g. "Allowed App Category" graph is linked with “Application Reports" for ease of admin.

NC-5595 :	Base System	Separate option to view and Download Reports, individual options available in 'Report' section • Download pre-generated PDF Report • Open filtered Report in report section.
NC-6264 :	Base System	S/W ISO installation on Hardware appliances is now supported
NC-6655 :	Base System	Cloning support VM on EsXi / VMWare without stopping vmtool service.
NC-6946 :	Base System	Performance Improvement for IPsec using Quick-assist on board chips available on XG750, XG135, XG125. This will work when hardware acceleration is enabled from CLI using below command "***system hardware_ acceleration enable"***
NC-6962 :	Base System	Device Access Security Strengthened • Telnet access is disabled and converted into SSH access; User can still enable Telnet and use it, user will see appropriate alert on the device access page. • HTTP is removed from device access page • HTTP requests will be redirected onto HTTPS
NC-7262 :	Base System	Configurable Host Name and Description Support
NC-8869 :	Base System	Fixed the issue of CA certificates containing ' (Apostrophe) not getting imported in SFOS
NC-8138 :	Base System	Fixed the issue with Default Certificate Authority due to Special characters in Registration details
NC-8825 :	Base System	Fixed the issue of Local subnets not reachable through IPsec Tunnel if multiple NATed tunnel are configured
NC-8869 :	Base System	Fixed the issue of CA certificate not getting imported if it has special characters
NC-10435 :	Base System	Fixed the issue where after reboot it took more time to prompt for login screen
NC-12374 :	Base System	Fixed the error message shown on UI when clicked on Check for new firmware from Auxiliary in HA (A-A)
NC-13180 :	Base System	Fixed the issue where certificate is not accepted in IE 11 due to SHA1 while using client less VPN
NC-10504 :	Certificates	Fixed the issue of OPENVPN failing to connect to XG due to certificates getting generated with invalid date format by XG
NC-1958 :	Certificates	Fixed the issue where admin is unable to upload PEM or DER type certificate if there is no .der or .pem at end of file name
NC-6628 :	Certificates	Fixed the issue where admin is unable to upload PFX Certificate if passphrase has special character
NC-10135 :	Certificates	Fixed the issue where Default CA is generated with wrong value of certificate field containing special characters
NC-11278 :	Certificates	Fixed the issue where Self-singed certificate generated with name as "Key" shows numeric value when applying it on Hotspot page.
NC-8627 :	Clientless SSL VPN	Fixed the issue of bookmarks being not accessible with case sensitive username
NC-8579 :	Clientless SSL VPN	Fixed the issue of SMB bookmark failing to connect if user's password contains "@" symbol
NC-11179 :	Clientless SSL VPN	Fixed the issue of accent mark not working in Clientless RDP bookmarks
NC-12726 :	Clientless SSL VPN	Fixed the issue where the browser Page is blank after file download in Safari in Clientless Access mode

NC-10737 :	Cyberoam to Copernicus Migration	Fixed the issue of Route through Gateway not getting updated in respective created Business Application rule on migration from Cyberoam 10.6.3 MR-4
NC-11128 :	Documentation	Amendments in Online Help with respect to downloading CA certificate
NC-5279	Firewall	Purpose based Application Filter Policy: Based on the generic requirement few templates are added which can be used for more meaningful application grouping under firewall policy. Below temples are added: • Block Generally unwanted apps (p2p, risk 4&5 file sharing, proxy tunnel, Loss of productivity) • Block highest risk apps(risk 5) • Block High risk apps (4&5) • Block filter avoidance apps (proxy, can bypass firewall policy)
NC-5290 :	Firewall	Improved country host creation work flow , now predefined country group based on continents are available and can be used directly in security policy
NC-5607 : & NC-8644 :	Firewall	Heartbeat Policy Enhancement: • Destination based HB Policy: Firewall will maintain heartbeat status for the destination and based on the destination heartbeat policy traffic will be served. Till v15 firewall was only monitoring source IP endpoint health which is now enhanced to support for the destination endpoint system as well. • Support for Missing Heartbeat (Source only): Firewall can detect the missing heartbeat from the endpoint and drop traffic.
NC-5780 :	Firewall	Added support to enable SNMP service on required zone and can support SNMP servers located on WAN side.
NC-7256 :	Firewall	Live Packet Capture can be opened as a Pop-window from Log Viewer
NC-7733 :	Firewall	DOS Protection Enhancement: • Enhanced dos protection limits for TCP, UDP, SYN and ICMP traffic for Zones, Interfaces and IPs instead of Global Limit. • As of now this feature is supported by CLI command ***"system dos-config add dos-policy policy-name <name>"*** and ***"system dos-config add dos-rule rule-name"***
NC-8643 :	Firewall	Support for Missing Heartbeat: • SFOS can detect endpoints that have been sending a heartbeat message earlier but are no longer sending Heartbeat message.
NC-8645 :	Firewall	Enhanced Live Connection view with Application information from Endpoint.
NC-8646 :	Firewall	Enhanced Application classification in connection list (Diagnostics->connection List): If system is not able to classify application then one link will be available in Live connection list page. Clicking on link will retrieve the application information from endpoint. System will use the Heartbeat to query the endpoint for the extended application classification. (Heartbeat should be configured at Protect → Advanced Threat → Security Heartbeat)
NC-10490 :	Firewall	Fixed the issue of Local Service ACL Exception rule not getting created for SNMP Services
NC-10361 :	Firewall	Fixed the ambiguity with services in MTA auto firewall rule
NC-8897 :	Firewall	Fixed the issue of ICMP Unreachable messages taking wrong path in case of IPsec VPN tunnel

NC-6922 :	Firewall	Fixed the ambiguity with Business Application Rule - Showing any host on UI even if a specific host is used
NC-5515 :	Firewall	Fixed the issue of traffic not passing from LAN to VPN or VPN to VPN rule if MASQ is enabled
NC-6755 :	Firewall	Fixed the issue of SMTP & SMTP(S) scanning option disappearing from business application policy if it's disabled once
NC-10351 :	Firewall	UDP timeout can now be configured from CLI using "set advanced firewall command"
NC-11640 :	Firewall	Fixed the issue where connections are dropped if XG Firewall is deployed in Direct Proxy mode.
NC-11147 :	Firewall	Fixed the issue where Open PCAP option from log viewer did not retained filtered settings
NC-12029 :	Firewall	Fixed the issue of Packet capture not started automatically if clicked on Open PCAP link from log viewer
NC-12044 :	Firewall	Fixed the Kernel Panic issue seen with HA (A-A) mode in MR3
NC-6568 :	Firewall	Fixed the error message thrown on enabling HA while dedicated interface is down
NC-11470 :	Firewall	Fixed the Kernel dump issue observed in SFOS 15.01.0 – MR3
NC-11701 :	Firewall	Fixed the error message on accessing the UI page with under privileged administrator user
NC-11873 :	Firewall	Fixed the issue where space missing between "Middle East" in Description of Country Group
NC-11929 :	Firewall	Fixed the issue where no error message was displayed when user enters decimal values in Rule ID Filter
NC-12298 :	Firewall	Fixed the issue where user based firewall rules are ignored with SATC (Sophos Authentication for Thin Client)
NC-12455 :	Firewall	Fixed the error message thrown when user imports the trusted mac csv file when no trusted mac added
NC-12611 :	Firewall	Fixed the issue where user gets logged off if authenticating through CAA and corresponding Firewall rule is turned off, but below that rule there is host based rule.
NC-4544 :	Firewall	Fixed the issue where admin can create a host with Invalid IP Range
NC-8079 :	Firewall	Fixed the issue where admin is unable to update Business Application Rule if rule name ends with space
NC-11694 :	Firewall	Fixed the issue where IPv6 Family Host were showing up in create new NAT policy list in Business Application Rule
NC-11841 :	Firewall	Fixed the issue where user is unable to disable firewall rule using API
NC-12714 :	Firewall	Fixed the TCP Vulnerability CVE-2016-5696
NC-13261 :	Firewall	Fixed the issue where after migration from Cyberoam 10.6.3 to V15 to V16, LOCAL zone was visible in zone page.
NC-13543:	Firewall	Fixed the issue where Business Application policy using Email Server(SMTP) template was not working
NC-7048 :	Galileo Heartbeat	Fixed the issue of SFOS regularly losing heartbeat registration with cloud.
NC-7145 :	Galileo Heartbeat	Fixed Network connectivity loss issue with Sophos Cloud
NC-7146 :	Galileo Heartbeat	Enhanced Cloud Communication Logs: Cloud connectivity logs are enhanced and added in hbtrust.log which will help in identifying the reason for the connection failure with cloud server.
NC-10385 :	Galileo Heartbeat	Fixed the issue of Cloud registration failing for security heartbeat due to string size limitation

NC-4874 :	Galileo Heartbeat	Fixed the issue of Special Characters not getting displayed correctly on heartbeat widget at dashboard under Heartbeat Flipside
NC-9723 :	Galileo Heartbeat	Fixed the issue of heartbeat registration with cloud getting lost
NC-11304 :	Galileo Heartbeat	Missing heartbeat can be enabled on specific zones for handling managed/unmanaged endpoint traffic
NC-5324 :	HA	Dynamic Interface support in HA • Supports DHCP and PPPoE interfaces in Active-Passive Scenario
NC-6581 :	HA	In case of HA , Primary appliance gets rebooted when trying to import AD groups ,when AD server is reachable over IPsec tunnel
NC-12277 :	HA	Fixed the issue where traffic is not getting passed through with HA (A-A) and load balancing ON
NC-13015 :	HA	Fixed the Kernel Panic issue observed while enabling 6in4 tunnel
NC-8333 :	HA	Fixed the issue where IPv6 address is not visible in aux appliance after HA (A-A) is disabled and peer administration interface is in WAN zone.
NC-6694 :	Hotspot	Added support of Space in Hotspot Name
NC-11323 :	Hotspot	Fixed the issue where import of Hotspots is failed when hotspot created using type as voucher & password of the day
NC-12957 :	Hotspot	Fixed the issue with alignment of added hotspots and their description on Hotspot Page
NC-13271 :	Hotspot	Fixed the issue where users were not able to connect to SSID unless hotspot is disabled
NC-6196 :	IDS	Fix for application filter policy showing all applications instead of selected risk level from application filter criteria.
NC-9466 :	IPS	Fixed the issue of Legitimate website traffic getting dropped due to IPS Signature
NC-11507 :	IPS	IPS Pre-processer alerts are now disabled
NC-8463 :	IPS	Fixed the issue where backup restore from appliance having 4 Core CPU to 2 Core CPU fails if IPS instance is configured manually
NC-11551 :	IPS	Fixed the issue where custom signature gets disappear in UI
NC-12904 :	IPS	Fixed the issue where ATP Threat Exceptions were not bypassed
NC-13377 :	IPS	Fixed the issue where IPS Service gets dead on rollback from V16 BETA-5 to BETA-3
NC-13447 :	IPS	Fixed the issue where after Bypass Session action for IPS Policy was not working as expected and changes made to the policy were not reflected
NC-13453 :	IPS	Fixed the issue where IPS service caused network outage in rare and very high load scenario
NC-8445 :	Licensing	Fixed License sync issue with HA (A-P)
NC-12306 :	Licensing	Fixed the issue where Control center page was shown on a de-registered appliance on login after logout session.
NC-11331 :	Localization	Fixed the issue of Wrong Success message shown while updating Web Filter Policy in French Language
NC-4953 :	Mail Proxy	MTA Mode Support: • SFOS supports email protection in MTA (Mail Transfer Agent) mode. • SFOS will be able to support both Transparent Proxy mode (known as Legacy Mode) and MTA mode deployment for the email protection. • Cyberoam Customer will be migrated into Legacy mode with all the configuration working as it is and will be able to switch the mode manually. • Mail Logs: History mail logs are supported for the admin troubleshooting like UTM9.

NC-4954 :	Mail Proxy	Domain Based Routing(Relay Support) : • With MTA mode , SFOS can support Inbound and Outbound E-mail relay and can support mail routing based on MX record or Static Host entry. • This feature is not supported with Proxy Mode.
NC-4957 :	Mail Proxy	Support of SPX Reply Portal: • Recipient of SPX email can now reply from PDF file through SPX reply portal. • Reply button in PDF file will redirect to SPX reply portal where recipient can reply to SPX email sender. • Admin can also enable option by which recipient can view the actual mail content and compose reply directly from the encrypted PDF file. • SPX reply portal is not supported for mails having attachment.
NC-6876 :	Mail Proxy	Support for Mail Spool: • With MTA mode support, mail spool feature is supported for easy troubleshooting of mails handled by MTA. • Admin can filter the spool mails based on date, domain and action like (Queued, Failed, SPX Blocked and frozen). • Retry and delete action with multiple spool mail selection
NC-7135 :	Mail Proxy	Email protection- UI Regrouping: • Email protection is regrouped for the ease of admin configuration
NC-7352 :	Mail Proxy	HELO/RDNS (to MTA) Support • Validity of HELO • Reverse lookup for mail domain
NC-10526 :	Mail Proxy	Fixed the issue of SMTP Service getting restarted constantly due to assertion
NC-9607 :	Mail Proxy	Fixed the issue of connections getting rejected by SMTP Service when there is substantial mail traffic
NC-8033 :	Mail Proxy	Fixed the issue of SMTP Service dying if there is a '+' in the address group.
NC-10438 :	Mail Proxy	MTA auto created rule will now have reasonable name
NC-10443 :	Mail Proxy	Added renaming support in Address group configuration in E-mail protection
NC-10444 :	Mail Proxy	SMTP banner can be configured from UI
NC-10454 :	Mail Proxy	UI Enhancements in SMTP Profile Tab
NC-11464 :	Mail Proxy	Relay page in Email Protection is improved to have a single Apply button
NC-11465 :	Mail Proxy	MTA will be enabled by default in fresh appliance and on factory reset, appliance will be in proxy mode if migrated from Cyberoam
NC-10638 :	Mail Proxy	Fixed the issue of client getting blacklisted due to default hostname used in Email Protection
NC-11463 :	Mail Proxy	Domains are now shown by hovering the mouse on SMTP Profiles
NC-10604 :	Mail Proxy	Improvements in debugging E-mail MTA failed to send, failure reason can be seen by hovering mouse over those emails on UI
NC-10839 :	Mail Proxy	SPX reply portal is now having time configurable option. Specifying the maximum time (in days) in which recipient can securely reply to an SPX-Encrypted email using the SPX reply portal is possible now.
NC-11598 :	Mail Proxy	SFOS now offers a selection of mail server to send notifications (Administrator > Notification) it has two options available 1. External E-Mail server 2. Built-in mail server (SFOS MTA)
NC-11798 :	Mail Proxy	Fixed the issue where Status is shown as ‘Reject’ instead of ‘Bounce’ when server reject mail with error code 5xx

NC-12734 :	Mail Proxy	Improvements in Default Standard RBL Service Address Group
NC-12739 :	Mail Proxy	Fixed the issue where MTA service is getting restarted frequently if there are more than 150 recipients in mail.
NC-12820 :	Mail Proxy	Fixed the issue where user is unable to download mails from mail spool of aux appliance(HA active-active)
NC-6740 :	Mail Proxy	Fixed the issue where MTA service gets dead if all is selected in Block File Types
NC-6847 :	Mail Proxy	Fixed the SQL injection vulnerability in User Portal
NC-6857 :	Mail Proxy	Fixed the vulnerability allowing low privileged user to view Quarantine Email of other users in user portal
NC-11338 :	Mail Proxy	Fixed the issue where E-mail gets scrambled on iOS 9.3.3 and inbuilt iOS E-mail client if scanned by IMAP
NC-12973 :	Mail Proxy	Fixed the issue where Email quarantined due to un-scannable content (due to AV failure or AV service not responding) were never allowed to release again from quarantine in MTA
NC-13007 :	Mail Proxy	Fixed the issue where no E-mails were listed in SMTP Quarantine if User is having more than one E-Mail address
NC-13275 :	Mail Proxy	Fixed the issue where clear Button in SMTP Quarantine page under User Portal is not working
NC-13320 :	Mail Proxy	Fixed the issue where MTA service was taking high CPU in HA Cluster
NC-10574 :	Network Services	Fixed the issue of ports showing status as NA, regardless of the possibility that it's already connected
NC-6830 :	Network Services	Added support of simultaneous configuration of DHCP Server and DHCP relay.
NC-9235 :	Network Services	Fixed the issue of Full configuration import getting fail
NC-10319 :	Network Services	Fixed the issue where updating interface of flexi port cause entire flexi mode to go disabled state
NC-10295 :	Network Services	Fixed the issue where XG was unable to do name lookup from appliance if URLs / server is sending PDU larger than 512 Bytes
NC-12197 :	Network Services	Fixed the issue where Wireless Interface is not updated if DHCP server static IP MAC binding is enabled and device is migrated from V15 MR3
NC-8082 :	Network Services	Fixed the issue where VLAN over Alias is getting removed on HA (A-A) failover
NC-11216 :	Network Services	Fixed the error message shown on CLI after updating IP of DHCP pool
NC-12558 :	Network Services	Fixed the issue where Line Splitting is not proper on Interface Page
NC-12899 :	Network Services	Fixed the issue where user is unable to update Gateway Host which is bound to WWAN interface when WWAN interface is disconnected
NC-12906 :	Network Services	Fixed the issue where Policy Route was not working properly with Cellular WAN connect / Disconnect
NC-13025 :	Network Services	Fixed the issue where Cellular WAN setting cannot be saved when there is another WAN GW of SFOS which is down
NCR-1025 :	On Premise Reporting	Improvements in Exported PDF Reports: • Exported PDF reports will now have Inline graphs in it and Risk number formatting for better view of reports.
NCR-1745 :	On Premise Reporting	Added Reports for Destination Heartbeat Restriction

NC-10616 :	Pattern Update	Included two new Intervals for Up2Date (Every 15 Minutes & Every 30 Minutes)
NC-11117 :	Pattern Update	Improvements in Up2Date pattern update. Patterns will now start update in case of first boot if gateway is up and live.
NC-5417 :	QoS	Purpose Based Traffic Shaping (QoS) Policy : Optimize business traffic priority needs by using Purpose based traffic shaping polices
NC-4908 :	RED	RED Site to Site Tunnel is supported from this release, between SFOS to SFOS and SFOS to UTM9 as well
NC-6579 :	RED	RED 15W is supported now
NC-8073 :	RED	Fixed the issue of RED tunnel not getting established properly after migration from V15 to V16
NC-11326 :	RED	Fixed the issue where RED site-to-site tunnel restarts frequently if Firewall RED Server has two or more WAN links
NC-12370 :	RED	Fixed the issue where SF device gets un sync to SFM when deleting RED server/client
NC-12920 :	RED	Fixed the issue where interface update was failing after deleting bridge interface
NC-13146 :	RED	Fixed the issue where RED 10 was not working with SFOS
NC-12417 :	RED	Fixed the issue where API import failed for RED Server device
NC-10122 :	RED	Added RED Site-to-Site tunnel support between UTM9 and SFOS
NC-7401 :	Reporting	Added MAC address details along with IP lease information into logs of System in Log viewer
NC-7666 :	Reporting	SAR Reports Improvements : • Report will not display NA or equivalent labels as a part of regular tables but have separate statement for un-categorized traffic • Report will show only critical and major IPS attacks • SAR report will be generated on the appliance and not sent to Cloud for report generation • Included Blocked reports and Hide reports that do not generate any data (including ones in summary)
NC-7668 :	Reporting	Added Activity based Web Reports
NC-9144 :	Reporting	Added Top IP Addresses by Web Server Usage Report
NC-11033 :	Reporting	Fixed the issue of Reports being unavailable on migration from Cyberoam to V16
NC-9176 :	Reporting	Fixed the issue of Drill down reports of application category shown blank
NC-12208 :	Reporting	Fixed the issue where Search Function is not working for "Source IP" in FTP Usage at Custom FTP Report.
NC-12632 :	Reporting	Fixed the corrupted file error coming in excel reader while opening Custom Web Reports
NC-12740 :	Reporting	Fixed the issue where deleting Report Bookmark automatically deletes custom view created for that bookmark
NC-6735 :	Routing	Policy Routing: Supports advanced routing scenarios. • Gateway can be configured on non-WAN zone type of interfaces and can be monitored using health check probing. • Policy Routing allows to define routing based on different traffic criteria like incoming interface, source network, destination network, layer 4 services, and Diffserv code points to route through desired and configured gateway. • Policy base routing will be overridden by Security policy if primary or backup gateway is configured in Security Policy • Various MPLS/VPN fail-over / fail-back scenario can be achieved by using this feature.
NC-10627 :	Routing	Fixed the issue of routing preferences getting overridden and traffic being passed through VPN instead of MPLS

NC-11856 :	Routing	Fixed the issue where no error message was thrown on entering duplicate condition for link monitoring
NC-11219 :	SSL VPN	Fixed the issue of SSLVPN policy not visible under user details when applied on a group of which user is member
NC-11475 :	SSL VPN	Fixed the issue where User could use a revoked certificate to connect SSL VPN
NC-11869 :	SSL VPN	Fixed the issue where currently selected networks are removed from list if user edits any of them
NC-13168 :	SSL VPN	Fixed the issue where SSL VPN service dies after migration from CR 10.6.3-838 MR5 to SF 16.01.0.174
NC-5293 :	UI	Cloning Support - Security policy (FW Rule) can be cloned and add to above or below selected policy/rule
NC-5425 :	UI	Improved UI Performance and responsiveness
NC-7418 :	UI	Menu Component and UX Revamp • Re-organized all Menu Items • New Tab support for easy navigation • Repeated options removed • UI Terminology Change. e.g.: Security Policy → Firewall & Wireless WAN → Cellular WAN
NC-7419 :	UI	Security Policy Configuration form UI Revamp • Reduced efforts of UI scrolling as compared to V1 • In line Configuration Summary of Security Policy while creating it. • More organized structure of security policy creation page.
NC-7672 :	UI	Log Viewer Enhancement • Pop out Log Viewer to full screen for improved user experience • Easy Identification logs by Color • Added faster refresh interval up to 5 Seconds.
NC-8980 :	UI	Fixed the issue of UI getting stuck with no response while editing IPS policy
NC-11137 :	UI	Fixed the issue of Administrator User failing to login to User Portal in case of Login Disclaimer is enabled
NC-10770 :	UI	Fixed the issue of UI becoming unresponsive on Safari Browser if refresh interval of Log viewer is set to 5 seconds
NC-10624 :	UI	Fixed the issue of firewall rules not being able to drag and drop in Safari Browser
NC-9605 :	UI	Fixed the issue of Users not getting logged out, when logged in through captive portal on Mozilla Firefox with Windows 8
NC-10289 :	UI	Revamped some icons to remove the inconsistent experience with icons
NC-10687 :	UI	Fixed the issue of support access not working if login disclaimer is enabled
NC-10728 :	UI	Fixed the issue of External domain receiving bounce back mail from Unknown Sender in case of XG Email protection policy has notify sender option selected
NC-11276 :	UI	Fixed the issue of sorting data in live connections once filter is applied
NC-11391 :	UI	Fixed the issue where admin gets logged out while using display filter in connection list
NC-11171 :	UI	Fixed the issue of Report links getting mismatch in control center Report Widget
NC-12111 :	UI	Fixed the issue where RDP bookmark using clientless VPN is not accessible if login disclaimer is enabled
NC-8687 :	UI	Fixed the issue where large number of groups are not getting imported
NC-11432 :	UI	Fixed the issue where UI becomes unresponsive while doing URL category lookup with space in Domain name.
NC-11628 :	UI	Fixed the issue where IPS rule cannot be edited in custom IPS Policy before saving the policy.

NC-12148 :	UI	Fixed the issue where user is unable to open Manage access points page via Control Center or Wireless protection
NC-12663 :	UI	Fixed the issue where user portal link displayed in captive portal even if it's disabled while using custom HTML template for captive portal.
NC-12712 :	UI	Fixed the issue where User Threat Quotient link is not opening from Control Center
NC-12713 :	UI	Fixed the issue where administrator user is not able to login in User Portal if User Portal port is set to 8443 and login disclaimer is enabled.
NC-5064 :	UI	Fixed the issue where multiple blank pop-up window opens and UI gets distorted on pressing space bar on any popped up page of UI
NC-11645 :	UI	Provided Help link on Log Viewer Page
NC-11779 :	UI	Fixed the issue where Email journaling page gets scrolled up automatically after canceling filter on recipient
NC-11803 :	UI	Fixed the issue where no error was thrown while giving non-numeric value for validity of Guest user under Authentication.
NC-11843 :	UI	Fixed the issue where user is unable to clear filter in Application → Traffic Shaping Defaults unless page is refreshed
NC-11867 :	UI	Fixed the issue where Multiple Popped windows were not shown separately
NC-11871 :	UI	Fixed the issue where Gateway page hangs when while adding gateway space bar is pressed
NC-11874 :	UI	Improvements in alert message on dashboard in case of scheduled local backup is failed
NC-11896 :	UI	Fixed the issue where Control Center was visible to Admin user who didn't had privilege for any entity
NC-12404 :	UI	Fixed the issue where Web filter logs in Log Viewer failed to load if POST request contains file name in UTF-8 Encoded header
NC-12595 :	UI	Fixed the issue where De-anonymize Pop-up was not showing up in log viewer
NC-6326 :	VPN	Fixed Super NAT issues in IPsec VPN Configuration
NC-7932 :	VPN	Fixed the issue with IPsec tunnel failover when multiple IPsec tunnels are configured between HO & BO and HO & BO has two WAN links.
NC-11540 :	VPN	Fixed some compatibility issues with other firewall for IPsec VPN connections
NC-11967 :	VPN	Fixed the issue where iOS VPN client profile downloaded from user portal shows profile name as 'Cyberoam Profile'
NC-5048 :	WAF	Added support for Slow HTTP Attack Protection.
NC-5959 :	WAF	Support of Web Server Protection (WAF) on bridge, LAN and Alias on LAN interface
NC-9478 :	WAF	Fixed the issue of WAF service restarting frequently when application protection policy has Anti-Virus scanning enabled
NC-11313:	WAF	Fixed the issue of IP based Web Server not getting added in Web Server Protection
NC-12542 :	WAF	Fixed the issue where user is unable to add IP address in Domains under Hosted Server Section in Business application policy if last octet of IP address is equal or less than "9"
NC-13022 :	WAF	Fixed the issue where user is unable to open login form for website in Google Chrome and Firefox if default form template is used in Web Server protection
NC-12372 :	WAF	Fixed the issue where admin is unable to publish sites via WAF due to incorrect path to WAF signature files.
NC-3542 :	Web	Support to specify a warning action for categories in web filter policy. When user browses a site falling in that category, they should see a customizable warning page that advises them to not visit the site, they can override it if they want to proceed and visit that site.

NC-3547 :	Web	Support to specify action to block or allow downloading of files which are encrypted and/or could not be scanned properly by virus engine.
NC-3551 :	Web	Google Apps Control Support, specify one or more comma-separated Google App Domains (which are hosted over Google) so that firewall can tell Google Apps only to allow access for those domains.
NC-3553 :	Web	Creative Commons Filter: extend safe search enforcement by also telling search engines to only display images with an open use creative commons license, which will provide further insurance that image search results will not return inappropriate images, Web Proxy provides domain restriction for Google, Yahoo and Bing. This feature is supported in both proxy mode, standard & transparent.
NC-3554 :	Web	Support for 'External URL Database' containing third-party URL lists: To comply with government, local or industry requirements for internet access control. By defining HTTP/FTP URL to download a third-party URL lists, extensions supported are .tar, .bz, .bz2 or plain text files. Text files should contain a list of URLs with one URL on each line. .tar, .tar.bz or .tar.bz2 files can contain a directory structure with a text file in each sub directory. Note: Firewall will not use the directory structure to separate URLs into multiple categories.
NC-4865 :	Web	Heartbeat-specific block-page: When a HTTP/HTTPS request is blocked by the heartbeat, the appliance should return a new block page with heartbeat specific message. So end user can understand that his/her HTTP/HTTPS request is blocked because of heartbeat rules. • Customization of this blocked page is not supported yet. • **Note:** Users might get certificate warning when HTTPS request is blocked, because proxy will handshake with its own CA certificate to send a blocked page and that CA may not be trusted in End User's Browser

NC-7097 :	Web	Activity Control to manage web browsing policies: • This is a key enhancement for web filter policy page, this feature deals with the user/group base restriction of web controls. So Admin can create a single web policy and in that he/she can define an action of allow/warn/block of web categories over user/group base. • As with version 15, the Firewall rule selects which policy applies to web traffic, based on source and destination zone, network address and user/group matching. But with version 16, a Web Policy can provide an additional layer of filters based on users and group. • This allows customers to create simple Firewall rules that use a single Web policy for an entire network, while still providing different levels of Web access for different groups of users. • To speed up the creation of policies a new look and feel is adapted that avoids the need to navigate back and forth between the policies list, policy pages and individual rule definition pages. All policies can be viewed in a single page, and all rule criteria can be edited inline. Rules can also be turned on and off, which makes troubleshooting much easier. Finally, properties of policies and rules that were previously static and required deletion or re-creation of elements, such as the category for a rule, or the default action for a policy, can now be modified. • We have reorganized the Global Web Protection settings, making the product easier to navigate and making it easier to find and modify the settings you need.
NC-7184 :	Web	Added support for more complex exception rules that apply globally for Web Filtering across all Activity Control provisions: • Exceptions provide a way to exclude certain traffic from specific parts of the Web Protection process. They are a powerful way to deal with problematic sites or applications that don't behave well. • In version 16, Exceptions replace the HTTP Scanning Rules and HTTPS Scanning Exceptions that existed in version 15. Note that this imposes a slight limitation on migration from version 15, because HTTP Scanning Rules could be used to enforce or skip virus scanning, whereas version 16 assumes virus scanning is always on and only allows exceptions to bypass it. • Admin can create and enable/disable exception rule base on Source IP, Destination IP, Regex for URL matching and Categories. Remember here, all rules are applied globally. • Admin can create a maximum of 200 exception rules.
NC-7965 :	Web	CLI option added to show and set relay_invalid_http_traffic and core_dump settings
NC-9142 :	Web	Fixed the issue of SSL2 connection handshakes getting failed through Proxy
NC-10505 :	Web	Fixed the issue of NTLM Authentication getting failed
NC-9027 :	Web	Fixed the broken Denied message in case of HTTPS redirection enabled
NC-6217 :	Web	Fixed the issue of Block page images not getting displayed on Microsoft Edge Browser

NC-7297 :	Web	Added support for Block Page for unauthenticated users with link to login instead of Captive Portal
NC-7925 :	Web	Fixed the issue of Web Categories not getting blocked according to policy when XG firewall is placed as direct proxy and respective firewall rule has only allowed some particular services.
NC-7927 :	Web	Fixed the Certificate error thrown while accessing Outlook with Web Protection policy as Allow All
NC-10637 :	Web	Fixed the issue with Facebook and other sites using Brotli compression not getting open with Web Protection enabled
NC-10655 :	Web	Fixed the issue where Custom logo with space in name can't be uploaded in denied message under general configuration of Web Content filter.
NC-11056 :	Web	Improvements in Web Protection debug logs from advanced shell for ACL or Exception match.
NC-11348 :	Web	Fixed the issue where Web Protection service dies due to all connection of Database service is occupied
NC-12256 :	Web	Fixed the issue where Web Proxy service was taking high CPU, resulting in slow browsing
NC-12363 :	Web	Fixed the issue where web Proxy service gets dead if restoring backup from appliance having more than 128 rules. Note: This release supports up to 128 rules in a single policy. If you are migrating policies or restoring backup from a previous release that contain more than 128 rules, only the first 128 rules will be used.
NC-12494 :	Web	Fixed the issue where Facebook commenting is not blocked using micro app enabled in SFSO 15.01.0 –MR3
NC-12621 :	Web	Fixed the issue where Web Proxy Service was getting stopped
NC-12884 :	Web	Fixed the issue where Web Proxy service was restarting
NC-13376 :	Web	Fixed the issue where HTTP Websites are categorized under IP address category if Pharming Protection is disabled
NC-13397 :	Web	Fixed the issue where downloading files through FTP in direct proxy deployment changed MD5 SUM of file being downloaded
NC-7367 :	Wireless	Adapt encryption settings for WPA2 to have the one with highest performance as default
NC-10371 :	Wireless	Fixed the issue of pending access point tab getting stuck on "Loading"
NC-8964 :	Wireless	Fixed the MTU mismatch between UI and CLI
NC-7801 :	Wireless	Fixed the issue of wireless network accepting more than 32 characters Passphrase /PSK but shows only 32
NC-6238 :	Wireless	XG Firewall now recognize all AP models to be added as Root or Mesh nodes in Mesh Network
NC-5235 :	Wireless	Fixed the message shown while changing Wireless Network from "Bridge to AP LAN" to "Bridge to VLAN"
NC-7663 :	Wireless	Fixed the issue where clients are not able to connect to SSID
NC-11446 :	Wireless	Fixed the issue where few mobile applications are failed to load with Separate Zone
NC-11863 :	Wireless	Fixed the issue where Access Point Groups status is getting reverted while sorting the records by Status
NC-12265 :	Wireless	Fixed the issue where SSID stops broadcasting with Dynamic Channel & Time based scanning enabled
NC-13374 :	Wireless	Fixed the issue where Wireless Controller service was taking high CPU

Known Issues / Limitations

- **Firewall**
  - NC-11848 : Firewall Rule re-order is working if all the rules are in expanded state
  - NC-12150: https://cloud.sophos.com is not opening using SF IP as a Direct Proxy in browser.
- **Base System & Framework**
  - Hostname cannot be used for resolving IP, Certificate, and Captive Portal etc.
  - NC-13510: If default admin user's password has space in V15, on migration the text before space would become the password of the admin user, text after the space would be discarded.
  - NC-12367 : Up2date status on Auxiliary are not syncing with Primary
- **UI / UX**
  - NC-13538 Control Center page is not displayed properly in IE11 browser
  - NC-13555 Users containing UTF-8 special characters in their usernames are not able to login into Captive Portal
- **Network Protection**
  - Cellular WAN is not supported in HA
  - Policy Routing will not be applicable for System originated traffic. Static routing for system originated traffic will work as it is.
  - Gateway Host is not supported for IPsec, GRE, IP tunnels and SSL VPN site to site Tunnel Interface. Dynamic and IPsec tunnel routing will work as it is to support deployment scenario over VPN.
  - NC-6756 : Static Route Redistribution in OSPF is not working
  - NC-9469 : Wireless interfaces is not showing on Network configuration wizard if admin has configured a wireless network with name consisting of word 'WLAN'
  - NC-13590 : Route Precedence configured in CLI is not followed in case of Policy Based Route and RED Site to Site Tunnel
- **Authentication**
  - NPM-186 - Google Authenticator is not supported for OTP as Authenticator Program
  - NC-13530: RADIUS Server add/update fail if NAS-Port-Type is empty
  - User MAC binding is not supported
  - Cyberoam and UTM Authentication client is not supported
  - SATC is not supported for IE11 with Protective Mode enabled.
  - SATC will not work if any AV is installed on the Windows Server 2012, AV has to be disabled to make SATC work
- **RED**
  - NC-13592 Unable to do offline provisioning of RED 50 using USB device
- **Web Protection**
  - When upstream proxy is configured in SFOS or SFOS IP is used as proxy in browser, Destination based Firewall rule action will not be followed.

- NC-13496: Log viewer logs shows wrong IP for web filter logs when appliance is deployed under Discover Mode.
- NC-13081 : AV Scanning is not supported for the streaming applications which are using 'Range' HTTP header, for example, Netflix, Windows Update, YouTube for iOS.

- **Web Server Protection**
  - No logging of requests dropped due to SlowHTTP Attack Protection
  - SlowHTTP Attack Protection settings are Global so specific server can't be included/excluded from it
  - SFOS only monitors HTTP headers for SlowHTTP attack protection
- **Galileo Heartbeat**
  - NC-12079: No heartbeat status is displayed on control center for MAC End point
  - NC-13480:Heartbeat service taking High CPU due to same UUID coming from multiple End point
- **Wireless Protection**
  - NC-13282: AP deployment over IPsec VPN is not working
  - NC-12390 : Not able to configure mesh network using AP55C
  - NC-11738 : AP will be in inactive state after Backup-Restore, and administrator has to delete and add the AP again to make it active.
  - NC-10688: All advanced settings for AP won't be shown on UI before accepting the AP.
- **VPN**
  - NC-6315: Script based Web Forms of Web Server are not accessible through HTTP/S Clientless SSL VPN Bookmark
  - NC-8915 :SFOS Web Admin Console will not be accessible through HTTPS Clientless SSL VPN Bookmark
  - NC-13014: If IPsec connection is configured with remote as 0.0.0.0/0, then internal zone traffic will be impacted if firewall acceleration is enabled.
  - NC-13603:L2TP connection using Pre-shared Key is not supported for Mobile Devices
  - NC-13394:Japanese characters are distorted when accessing google.co.jp through HTTPS Clientless SSL VPN Bookmark
  - NC-12969: SSL Remote-Access VPN client is connected through Apple iPhone. But traffic is not pass through to that SSL VPN tunnel.
  - NPM-93: Not able to support Cyberoam and UTM9 VPN clients for IPsec and SSLVPN.
  - NC-12065 : Unable to create VPN on IPv6 interface which is configured as RA client
  - NC-13573: Clientless SSL VPN Bookmark will not work in IE11 with compatibility setting turned ON.

Behavior Changes / Known Behavior

- **Base System & Framework**
    - Certificate passphrase has been strengthened in SFOS v16, it is recommended to administrator regenerate the SSL CA certificate to use the strengthened passphrase on upgrading to SFOS v16 from v15. After regenerating the SSL CA, administrator will have to reinstall the new SSL CA in all client browser to avoid Certificate Error.
    - Web Admin HTTP access selection is removed from Device Access Page
        - Web Admin HTTP Port selection is removed from Admin settings, in case of fresh installation
        - Web Admin HTTP Port selection will be available in case of firmware migration if it is enabled in previous firmware. But requesting on HTTP will be redirected on HTTPS in that case.
        - If HTTP Access is enabled in previous firmware for Device Access, after SFOS v16 migration on requesting Web Admin via HTTP, it will get redirected to HTTPS.
    - If Telnet is enabled in previous firmware, after migration to SFOS v16 it will be disabled and SSH will be enabled
        - If someone is going to enable Telnet in SFOS v16, then SFOS will give warning message "Telnet service will be discontinued from next release so we recommend that you use SSH service."
    -
- **Network Protection**
    - Cyberoam and SFOS V15 Source based route configuration will be migrated under Policy Routing rule.
    - V16 will no longer support separate UI configuration for the source routing and admin can use the Policy routing rule to achieve same configuration.
- **Authentication**
    - SFM authentication not working when OTP is enabled for Web Admin
    - SFOS OTP implementation is a tOTP (time-based OTP) so users can only use Authenticators or hardware tokens which are designed for tOTP. Recommended Authenticator program for smart-phones and tables are “Sophos Authenticator”
    - Typing in an incorrect pass-code will cause the generated token to become invalid until the next time step is reached - OTP passwords are only valid once per time step.
- **Web Protection**
    - Behavior Change while creating/editing web policy:
        - There have been some minor changes in how policies are applied, particularly regarding file type rules. This was done primarily to address inconsistencies in how policies worked depending on whether file type was determined based on extension (in the HTTP request) or actual file type/mime type (in the HTTP response). In short, an 'allow' rule for a file type will no longer override a 'block' rule for URL or category, even if the file type allow rule comes above the category block.
        - File type exceptions for individual rules have been removed. Customers who make extensive use of file types in their policies may need to review policies after upgrading. Some marginal use cases

may no longer be supported (the only ones we could think of is where an Admin wants to allow ONLY a certain file type from a given site, but block everything else on the site) file type base exception is not supported in web control ACL rules. So this won't be migrated if configured previously.

- 'Deny' has been replaced with 'Block'
- Configuration of web action to allow/block for HTTP/HTTPS has changed. The UI provides one place to configure action, and assumes the same for HTTP and HTTPS. There is an optional setting allowing the Admin to choose a different action for HTTPS per-rule if required.

- Reorganize Web Settings UI pages
  - Most **Web Content Filter** settings have moved to a new page **Protection**
  - **Notifications** are moved to a new configuration page of their own
  - Primary malware scan engine preference is now accessed via a link on the main **Protection** page alongside the other malware scanning settings
  - Some settings have been renamed and some have changed behavior. For example:
    - 'Download File Size Restriction' becomes 'Prevent downloading of large files'. There is a checkbox to enable/disable this option. If enabled, the Admin can enter a numerical maximum file size value. In v15 this was a single edit box, and entering a '0' meant 'No restriction'. On migration, it will be disabled if previously configured '0' or enabled with a size same as configured previously.
    - 'Deny Unknown Protocol' becomes 'Block unrecognized SSL protocols'
    - 'Allow invalid certificate' becomes 'Block invalid certificates' and is enabled (block) by default.
    - Web Proxy moves to a new **advanced** page along with Caching configuration. 'Trusted Ports' becomes 'Allowed Destination Ports'
- NC-12363 : Migrating Policies from Previous Releases
  - This release supports up to 128 rules in a single policy. If you are migrating policies from a previous release that contain more than 128 rules, only the first 128 rules will be used.
  - Web policy rules now support combined activities. These include user activities, categories, URL groups, file types, and dynamic categories. To maintain the overall functionality of the policy, replace blocks of adjacent rules for different activities with a single rule that contains a group of activities. Please delete or consolidate rules as required.

- NC-11979: Unauthenticated users will get a Block Message with Captive Portal link instead of direct Captive Portal.
  - With this version of SFOS, if 'Show Captive Portal' option in the Firewall rule is enabled, SFOS will throw a Block Message with Captive Portal link at the bottom.

- **E-Mail Protection**
  - MTA mode will not be supported in lower end flash appliances.
  - NC-12099: SPX Add-in will not be available for download if Email Subscription is not subscribed
  - NC-12022: Remove and Deliver action configured in Legacy Mode will remove the body of Email Message also

- **Wireless Protection**
    - AES will be default encryption for WPA2 authentication, user will get deprecation + speed warning when choosing TKIP or TKIP+AES

Important Notes for Cyberoam Migration

- HTTP access of SFOS is not allowed
  - HTTP settings from device access page has been removed
  - Admin port settings for HTTP will be preserved in case http access is enabled before migration
  - HTTP request for device access will be redirected to HTTPS for the cases where HTTP access was enabled before V16 migration
  - Admin port settings for HTTP will be removed from admin port settings in case of
    - Fresh installation
    - Factory reset
    - HTTP disabled before migration
- TELNET access of SFOS is deprecated
  - If Telnet access is enabled before migration it will be converted to SSH access after migration
  - Warning message will be displayed on the device access page if admin enables telnet access for any zone
- ICAP will not be supported
- Web Proxy DOS Setting is not available
- Support of AV Scanning on Virtual Host without active Webserver Protection (WAF) subscription
- Ability to create all service based rule for ACL(local) rule
- FTP scanning is only supported for User/Network rule
- JavaScript emulation for URLs/Cookies will not be supported in Webserver Protection (WAF)
- Auto-learning of added exceptions in WAF is not supported
- Instant Messaging (IM) Proxy is not supported
- Route based VPN is not supported
- Nested Group Support in NTLM is not supported
- Overriding Organizational Web Filter Policy Restrictions is not available
- User MAC binding is not supported
- SSLVPN Port configuration is not supported
- Not able to support Cyberoam General Authentication and SSLVPN Client, user has to install SFOS Client Authentication Agent and SFOS SSLVPN client.
- On migration all self-sign certificates and certificate authority will be regenerated, admin and end users have to reimport this certificate wherever it is used.
- Reflexive Rule for Business Rules will not be displayed on UI on Firewall Page and all the policies will be inherited from the Business Rule including SNAT.
- If there are Identity Attached Rules for “Any Zone to Local” created in Cyberoam, then on migration they will be converted into Local ACL rules with Action as Drop.