SOPHOS

Security made simple.

Sophos XG Firewall v16.05

Contents

New Features & Issue Resolved in SFOS v16

- Sandstorm Analysis for Web Downloads
    - Sandstorm is a Cloud service that provides in-depth analysis of potentially malicious files and it enhances SF Web Security to quickly and accurately detect evasive threats
    - With SF 16.05 release Admin can configure SF to securely send suspicious files to a Sandstorm server before downloading them from any website to more closely inspect them and have better protection against Zero Day Threats
    - Admin can get detailed reports of analysis done by the Sandstorm server on the Sandstorm Activity Page
    - There is also an option for Admin to release a file before the Sandstorm server sends the result or create exceptions for certain domains or file types
- Sandstorm Analysis for Email Attachments
    - With SF 16.05, SF supports Sandstorm Analysis for Email attachments in MTA mode
    - SF will send suspicious attachments to Sandstorm server for further analysis and to closely inspect them and have better protection against Zero Day Threats
    - Admin can configure Sandstorm Protection while configuring SMTP policy
    - Apart from Sandstorm activity, Admin can view status of Emails waiting for Sandstorm results in Email Spool
    - Sandstorm will not be supported in Legacy Mode and for Outbound emails
- Hovering the mouse over objects in Firewall Policies will now show a tool tip displaying the details about the object
    - This feature will further enhance the ease of configuring Firewall Policies by showing the underlying values of the objects in Tool Tip to Admin which will in turn save Admin's time to configure policies

NC-11437	Base System	Added the support for Soft Shutdown (Graceful) through Power Button on hardware having Power Button
NC-14100	Authentication	Fixed the issue wherein SF IP was not appearing on General Tab of STAS suite
NC-13930	Authentication	Fixed the issue wherein Authentication service was restarting frequently
NC-14160	Authentication	Fixed the issue wherein NetBios requests were sent out via WAN interface
NC-14140	Base System	Fixed the issue wherein if the IPsec VPN tunnel name matched an existing log file then that tunnel's logs were placed in that existing log file
NC-14123	Base System	Fixed the issue wherein IPsec tunnels configured on IPv6 interfaces were not reconnected on updating the interface
NC-3820	Certificates	Fixed an issue wherein Start Date/End Date were not validated before uploading CRL file
NC-14227	Certificates	Improved the error message thrown on uploading expired CRL
NC-13394	Clientless Access (HTTP/HTTPS)	Fixed the issue wherein Japanese characters were getting distorted while accessing google.co.jp through HTTPS Clientless SSL VPN Bookmark
NC-13665	Firewall	Fixed the issue wherein Missing EP traffic was not getting dropped in HA Active-Active Deployment
NC-13702	Firewall	Fixed the issue wherein Captive Portal was not thrown directly to unauthenticated users when "Show Captive Portal" was enabled in Firewall Policy

NC-13987	Firewall	Fixed the issue wherein Configuration Wizard from Dashboard was not running after configuring Source based DoS rule in CLI
NC-14137	Firewall	Fixed the issue wherein “Internet Scheme” page was not loading properly on UI
NC-13014	Firewall Datapath	Fixed the issue wherein traffic was not passing from LAN zone to DMZ zone with IPsec site to site configured and Firewall acceleration enabled
NC-8116	Framework(UI)	Disabled TLS1.0/TLS1.1 protocols for Web Admin and User Portal
NC-13858	Framework(UI)	Added Horizontal interval Data in Dashboard Graphs to get precise view
NC-14995	Galileo Heartbeat	Fixed the issue wherein Heartbeat Service was restarting frequently
NC-13610	IDS + AppControl	Fixed the issue wherein Psiphon Proxy was not getting blocked
NC-13496	IPS	Fixed the issue wherein wrong IP address was displayed in Web Filter logs in Log Viewer when SF is deployed in TAP mode
NC-14231	IPS	Fixed the issue wherein Internet Traffic was dropped by IPS if network subscription was not subscribed but Web protection was subscribed
NC-12228	Mail Proxy	Improved Mime Whitelist Box to display the entire text
NC-14093	Mail Proxy	Fixed the issue wherein Email traffic processing was stopped if IP reputation was enabled with Action Reject
NC-14098	Mail Proxy	Fixed the issue wherein Delivery Failure Notification was not sent if sender or recipient email address contained space
NC-14178	Mail Proxy	Fixed the issue wherein SMTP Proxy service was stopped due to specific characters in return path of delivery failure notification
NC-14213	Mail Proxy	Fixed the issue wherein Read Only Profile had read-write access of Email Protection Page in HA
NC-13448	Network Services	Fixed the issue wherein DHCP service was stopped while binding custom option to DHCP Server
NC-13449	Network Services	Fixed the issue wherein on deleting DHCP option its bind was not getting deleted
NC-12966	Networking	Fixed the issue wherein Huawei E3372 USB dongle was not connecting after rebooting the SF
NC-12214	Networking	Improved Warning Message on Unbinding any interface
NC-13599	RED	Fixed the issue wherein admin was able to configure 3G Failover in Transparent Split Mode
NC-14164	RED	Implemented support wherein admin can choose to use only TLS 1.2 for RED Tunnel
NC-13257	Reporting	Fixed the issue wherein pagination was not working for Executive Report of Interfaces
NC-11769	Reporting	Fixed the issue wherein Event Type was shown “Not Available” for some entries in Admin Events report
NC-6345	Reporting	Fixed the issue wherein Search Filter in Reports was not working for some reports
NC-12472	Reporting	Fixed the issue wherein in exported PDF Reports server time was shown incorrect at 2nd Page
NC-12969	SSLVPN	Fixed the issue wherein permitted resources were not accessible through SSL VPN when connected via OpenVPN for iOS
NC-13945	UI	Fixed the issue wherein Log Viewer link on Control Center window was not working
NC-6589	VPN	Fixed the issue wherein IPsec connection was not reconnected if configured on IPv6 interface with DHCPv6 IP assignment when IPv4 address of the same interface is changed

NC-13995	VPN	Fixed the issue wherein VPN Failover Group probing was stopped after couple of minutes
NC-14118	WAF	Fixed the issue wherein WAF configurations were not getting pushed from SFM to SF
NC-11111	Web	Fixed an issue wherein Captive Portal was not thrown to Unauthenticated Users
NC-14000	Wireless	Fixed the issue wherein DHCP Option Code 234 was not working for RED15w
NC-13340	Wireless	Fixed the issue wherein vendor name was shown Unknown for connected wireless clients
NC-13326	Wireless	Fixed the issue wherein DHCP service was having high CPU utilization
NC-10629	Wireless	Fixed the issue wherein “wifiauth” service status was shown Dead on UI
NC-9469	Wireless	Fixed the issue where Wireless Interfaces were not shown on Network Configuration Wizard if admin has configured a wireless network with name consisting of word 'WLAN'
NC-13207	Wireless	Fixed the issue wherein hostapd service was getting dead on updating Radius Server in Wireless Global setting
NC-13940	Wireless	Fixed the issue wherein RED 15w was not getting detected by SF

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.
- UI / UX
    - 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-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
    - 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
    - NC-7216 : Users authenticated through SATC/STAS are not shown on Live Users Page after HA failover
- 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-13081 : AV Scanning is not supported for the streaming applications which are using ‘Range’ HTTP header, for example, Netflix, Windows Update, YouTube for iOS.
    - NC-15080: Guest User registration Portal is not opening if “Captive Portal uses HTTPS“ is unchecked under Authentication > Services> Captive Portal
- 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
- Galileo Heartbeat
    - NC-12079: No heartbeat status is displayed on control center for MAC End point
- Wireless Protection
    - 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-13603:L2TP connection using Pre-shared Key is not supported for Mobile Devices
  - NC-13573: Clientless SSL VPN Bookmark will not work in IE11 with compatibility setting turned ON.
  - NC-15203: Permitted resources are not accessible through SSLVPN Remote Access if both IPv4 & IPv6 are enabled in SSL VPN Global Option and Use as Default Gateway setting is selected
- Sandstorm
  - NC-14948 : Sandstorm Pending emails can't be released from Auxiliary Appliance in HA Active-Active deployment
  - NC-15210 : API Import/Export is not working
  - There is an issue with the Sandstorm licensing if user tries to initiate the 30 day evaluation via Control Center. After clicking the 30 days trial button, user will be redirected to the MySophos portal where after finishing the subscription process user will see a HTTP 404 error page, because the redirect URL is not correct.
    - As a workaround, user needs to synchronize the licenses from System →Administration -→ Licensing →Synchronize
      This issue does not appear if user initiates the process via MySophos instead of Control Center

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
  - NC-14124: Apple & Microsoft Web Exceptions will be turned ON by default in case of Fresh installation or Factory Reset, however on migration the status of these exceptions will remain unchanged.
  - NC-11111 : Captive Portal Redirection behavior from this release will be
    - No Captive Portal will be thrown to Unauthenticated Users ,if “Show captive portal to unknown users” checkbox is unchecked
    - If “Show captive portal to unknown users” is checked and under Authentication > Services> Captive Portal - Login Prompt Method “Link to Captive Portal “ is selected, then Captive Portal will be thrown to unauthenticated users
    - If “Show captive portal to unknown users” is checked and under Authentication > Services> Captive Portal - Login Prompt Method “Custom Message “ is selected, then Custom message will be thrown to unauthenticated users with No Captive Portal Link embedded to it.
    - If Match known users checkbox is unchecked and under Authentication > Services> Captive Portal - Login Prompt Method “Link to Captive Portal “ is selected , and user accesses a blocked site then a block page with captive portal link will be displayed to user
    - If Match known users checkbox is unchecked and under Authentication > Services> Captive Portal - Login Prompt Method “Custom Message” is selected, and user accesses a blocked site then a custom message with no captive portal link will be displayed to user
    - If Match known users checkbox is unchecked and under Authentication > Services> Captive Portal - Login Prompt Method “Link to Captive Portal “ is selected , and user accesses a warned site then a warn page with captive portal link will be displayed to user and if the setting under Authentication > Services> Captive Portal - Login Prompt Method is “Custom Message” then a warn page with no captive portal link will be displayed
- 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.