Cyberoam OS to Sophos Firewall OS (SFOS) Upgrade Guide

Product: Cyberoam
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Log</td>
<td>3</td>
</tr>
<tr>
<td>Overview</td>
<td>5</td>
</tr>
<tr>
<td>Supported Cyberoam Appliances</td>
<td>5</td>
</tr>
<tr>
<td>Supported Firmware</td>
<td>6</td>
</tr>
<tr>
<td>Points to Note before Upgrade</td>
<td>7</td>
</tr>
<tr>
<td>Sophos Partner Portal (For Partners only)</td>
<td>8</td>
</tr>
<tr>
<td>Sophos Central Firewall Manager (For Partners only)</td>
<td>8</td>
</tr>
<tr>
<td>Steps to Upgrade</td>
<td>9</td>
</tr>
<tr>
<td>Login to SFOS</td>
<td>14</td>
</tr>
<tr>
<td>Navigation in SFOS</td>
<td>15</td>
</tr>
<tr>
<td>License Migration</td>
<td>15</td>
</tr>
<tr>
<td>Transformation from CR Firewall Rules to SFOS Firewall Rules</td>
<td>15</td>
</tr>
<tr>
<td>Changes in Individual Features</td>
<td>20</td>
</tr>
<tr>
<td>Licensed Features</td>
<td>20</td>
</tr>
<tr>
<td>Wireless</td>
<td>20</td>
</tr>
<tr>
<td>Web Application Firewall (WAF)</td>
<td>20</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>20</td>
</tr>
<tr>
<td>General Authentication Client</td>
<td>20</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>21</td>
</tr>
<tr>
<td>Web and Application Filtering</td>
<td>21</td>
</tr>
<tr>
<td>Identity</td>
<td>21</td>
</tr>
<tr>
<td>High Availability (HA)</td>
<td>22</td>
</tr>
<tr>
<td>Certificates</td>
<td>22</td>
</tr>
<tr>
<td>DHCP/PPPoE</td>
<td>22</td>
</tr>
<tr>
<td>SNMP</td>
<td>22</td>
</tr>
<tr>
<td>Country Host</td>
<td>22</td>
</tr>
<tr>
<td>Custom Zones</td>
<td>22</td>
</tr>
<tr>
<td>HTTP Redirection</td>
<td>23</td>
</tr>
<tr>
<td>Telnet Access</td>
<td>23</td>
</tr>
<tr>
<td>Web Proxy</td>
<td>23</td>
</tr>
<tr>
<td>Important Notes for Cyberoam to SFOS Upgrade</td>
<td>23</td>
</tr>
<tr>
<td>Renamed CR Features</td>
<td>24</td>
</tr>
<tr>
<td>Copyright Notice</td>
<td>25</td>
</tr>
</tbody>
</table>
# Change Log

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 November, 2015</td>
<td>Added: “Dynamic DNS” section under <a href="#">Changes in Individual Features</a>.</td>
</tr>
<tr>
<td>26 November, 2015</td>
<td>Removed: Point related to Custom SSL port in SSL VPN section under <a href="#">Changes in Individual Features</a>. Added: Note in Step 1 under <a href="#">Steps to Upgrade</a>.</td>
</tr>
<tr>
<td>14 December, 2015</td>
<td>Updated: First point related to Rollback under <a href="#">Points to Note before Upgrade</a>. 5th point related to AV Scanning of Web Servers under <a href="#">Important Notes for Cyberoam to SFOS Upgrade</a>.</td>
</tr>
<tr>
<td>7th April, 2016</td>
<td>Added: Wireless point under <a href="#">Changes in Individual Features</a>. Updated: List of supported Appliance under <a href="#">Supported Cyberoam Appliances</a>. DHCP/PPPoE point under <a href="#">Changes in Individual Features</a>.</td>
</tr>
<tr>
<td>21st April, 2016</td>
<td>Added: Point for identity-based firewall rules under <a href="#">Transformation of Cyberoam Firewall Rules to SFOS Firewall Rules</a>. Updated: List of supported Appliance under <a href="#">Supported Cyberoam Appliances</a>.</td>
</tr>
<tr>
<td>30th June, 2016</td>
<td>Added: Information for Internet Scheme Page under <a href="#">Transformation of Cyberoam Firewall Rules to SFOS Firewall Rules</a>.</td>
</tr>
<tr>
<td>10th October, 2016</td>
<td>Updated entire guide for SFOS v16.</td>
</tr>
<tr>
<td>11th October, 2016</td>
<td>Renamed “Discontinued CR Features” section to “Important Notes for CR to SFOS Upgrade”.</td>
</tr>
<tr>
<td>26th October, 2016</td>
<td>Language and formatting changes in various sections.</td>
</tr>
<tr>
<td>9th November, 2016</td>
<td>Updated <a href="#">Steps to Upgrade</a> section.</td>
</tr>
<tr>
<td>Date</td>
<td>Changes</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>23rd November, 2016</td>
<td>Added <a href="#">Overview</a> Section. Updated <a href="#">Supported Cyberoam Appliances</a>.</td>
</tr>
<tr>
<td>20th February, 2017</td>
<td>Updated the title and all relevant references in content from Migration Guide to Upgrade Guide.</td>
</tr>
<tr>
<td>24th May, 2017</td>
<td>Updated <a href="#">Supported Firmware</a> section. Added sections: <a href="#">Sophos Partner Portal</a> &amp; <a href="#">Sophos Central Firewall Manager</a>.</td>
</tr>
<tr>
<td>29th November, 2017</td>
<td>Added 5th &amp; 6th point and updated 4th point under <a href="#">Points to Note before Upgrade</a>. Updated <a href="#">License Migration</a>.</td>
</tr>
<tr>
<td>3rd January, 2018</td>
<td>Updated <a href="#">High Availability (HA)</a> under <a href="#">Changes in Individual Features</a>.</td>
</tr>
</tbody>
</table>
Overview

This guide walks you through the steps of upgrading Cyberoam OS to Sophos Firewall OS (SFOS), and the changes in behavior of the various features and functionality in SFOS.

Before upgrade:
- Check if your Cyberoam model and firmware can be upgraded.
- Check how your licenses can be migrated.
- Go through this guide to see known behavior changes in features, and which Cyberoam features are renamed or discontinued.

Supported Cyberoam Appliances

The following Cyberoam Models can be upgraded:

<table>
<thead>
<tr>
<th>Model</th>
<th>Hardware Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>CR10iNG</td>
<td>AM04</td>
</tr>
<tr>
<td>CR10wiNG</td>
<td>AM04</td>
</tr>
<tr>
<td>CR15iNG</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR15iNG-4P</td>
<td>All</td>
</tr>
<tr>
<td>CR15wiNG</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR25iNG</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR25iNG-6P</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR25wiNG</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR25wiNG-6P</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR35iNG</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR35wiNG</td>
<td>AM02, AM03</td>
</tr>
<tr>
<td>CR50iNG</td>
<td>All</td>
</tr>
<tr>
<td>CR100iNG</td>
<td>All</td>
</tr>
<tr>
<td>CR200iNG /XP</td>
<td>All</td>
</tr>
<tr>
<td>Model</td>
<td>Compatibility</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CR300iNG/XP</td>
<td>All</td>
</tr>
<tr>
<td>CR500ia/1F/10F/RP</td>
<td>All</td>
</tr>
<tr>
<td>CR500iNG-XP</td>
<td>All</td>
</tr>
<tr>
<td>CR750ia/1F/10F</td>
<td>All</td>
</tr>
<tr>
<td>CR750iNG-XP</td>
<td>All</td>
</tr>
<tr>
<td>CR1000ia/10F</td>
<td>All</td>
</tr>
<tr>
<td>CR1000iNG-XP</td>
<td>All</td>
</tr>
<tr>
<td>CR1500ia/10F</td>
<td>All</td>
</tr>
<tr>
<td>CR1500iNG-XP</td>
<td>All</td>
</tr>
<tr>
<td>CR2500iNG</td>
<td>All</td>
</tr>
<tr>
<td>CR2500iNG-XP</td>
<td>All</td>
</tr>
<tr>
<td>Cyberoam Virtual Appliances</td>
<td>All</td>
</tr>
</tbody>
</table>

**Note:**
- Execute the following command on Cyberoam CLI to view the hardware revision of your appliance: console> cyberoam diagnostics show version-info.
- The minimum hardware requirement for upgrading Cyberoam Virtual Appliances is:
  - One vCPU
  - 2GB vRAM
  - 2 vNIC
  - Primary Disk with a minimum of 4 GB size
  - Report Disk with a minimum of 80 GB size

**Supported Firmware**
To upgrade your CR Appliance to SFOS v16.x, your appliance should be at CyberoamOS 10.6.3 MR1 or above.
The appliance should be registered in [Cyberoam Customer Portal](#) and should have a valid support subscription.
If your appliance is running on CyberoamOS 10.6.3 MR1 or above, you can upgrade it to the latest SFOS 16.01 version.
If your appliance is running on CyberoamOS 10.6.5 or above, you can upgrade it to the latest SFOS 16.05 version.
Points to Note before Upgrade

1. When upgrading to SFOS from the Customer Portal, you get a 30-Day Full Guard Trial License (refer to License Migration Guide for more details). During the trial period, seamless rollback to CyberoamOS is possible. All you have to do is reboot the appliance and select CyberoamOS to boot it. All previous configuration, reports and subscriptions (except) will be restored once the device is rebooted.

   Note:
   - Any new configuration (especially features exclusive to SFOS) will be lost once you roll back.
   - Rollback time is the same as the time required to reboot your device.
   - Rollback will not be possible after your existing CR Licenses have permanently migrated to SFOS licenses.

2. Appliances upgraded to SFOS can no longer be managed by Cyberoam Central Console [CCC]. You will need Sophos Firewall Manager [SFM] to manage the upgraded appliances.

3. Appliances upgraded to SFOS can no longer be integrated with Cyberoam iView. You will need Sophos iView (Version 2) for reporting of upgraded appliances.

4. Once your Appliance is upgraded to SF firmware, the warranty expiry will be determined by SF warranty rules. The warranty expiry date will coincide with the expiry of the Enhanced Support subscription [which can be renewed]. However, the Warranty Expiry is capped at a maximum of 5 years from the original invoice date.

   Note: After warranty expires, customer will not be eligible for RMA.

   Example: If the appliance invoice date is 28-May-2017, bought with 3 years of TVS and is migrated on 15-Dec-2017, the Warranty Start date would be 28-May-2017 and the Warranty Expiry date would be 27-May-2020. In 2020 if the FullGuard subscription is renewed for 3 years, the subscription expiry date would be 27-May-2023 and the Warranty Expiry date would be 27-May-2022 [i.e. capped at 5 year from invoice date].

5. Once you have fully migrated your license using the Migrate License option to SF firmware, if you want to purchase additional subscriptions or renew your migrated subscriptions then you must order subscriptions for SFOS.

6. If you want to activate license keys for your appliance running on SF firmware then you must ensure:
   - You have migrated your Cyberoam OS license to SFOS
   - You are not using the 30 day FullGuard trial license
Note: If you are using the FullGuard 30 day trial license, go to System > Administration > Licensing and complete a full migration by clicking ‘Migrate’.

7. Once upgraded, your Appliance will NOT be applicable for the Cyberoam Trade-Up schemes. However, you can opt for Sophos Firewall Hardware Refresh programs.
8. Once upgraded, a backup of the Cyberoam firmware cannot be restored on the SFOS.

Sophos Partner Portal (For Partners only)

1. Once the Cyberoam appliance is upgraded to SFOS, it will not be managed from Cyberoam Partner Portal.
2. In order to add those devices to your Sophos Partner Portal, drop an email to GlobalSEDesk@sophos.com with the serial number of the devices and along with Sophos partner details (such as registered email address, Partner's company name and partner portal username).
3. Global SE Desk will take this up with licensing team to get the migrated devices added to Sophos Partner Portal.
4. All the migrated units should have valid subscription, applied in order to get the devices added to Sophos Partner Portal.
5. Devices running under evaluation licenses will not appear on Sophos Partner portal.

Sophos Central Firewall Manager (For Partners only)

1. A Cyberoam appliance managed by Partner using Cyberoam’s on-Cloud Management Service (CCMS) cannot be managed using CCMS once it's upgraded to SFOS. The Partner can choose to manage the firewall using Sophos Central Firewall Manager (CFM) by following the steps in the CFM guide for partners.
2. First step is to make device visible in Sophos Central Partner dashboard [please click here for CFM and Sophos Central Partner dashboard guide].
3. If the firewalls (on SFOS) sold by you are not visible on Sophos Central Partner Dashboard, drop an email to GlobalSEDesk@sophos.com with the serial number of the devices along with Sophos partner portal details (such as registered email address, Partner’s company name and partner portal username).
4. Global SE Desk will take this up with licensing team to get the migrated devices added to Sophos Central Partner Dashboard.
5. CR devices on SFOS with licenses migrated can be managed via CFM.
Steps to Upgrade

You can upgrade your Cyberoam appliance to SFOS by following the steps given below.

Step 1
Once SFOS is available, an alert is displayed on your dashboard. Click the link. You will be redirected to Cyberoam Customer Portal.

Step 2
Login to the Portal.
Step 3
Click **Upgrade** against the hardware or virtual appliance you want to upgrade.

Step 4
Select **Upgrade to Sophos Firewall OS** and select the CyberoamOS firmware version your appliance is running on currently. Click **Next**.

You can upgrade to SFOS only if the current CyberoamOS firmware is 10.6.2 MR2 or 10.6.3 MR1 onwards. If not, you will have to first upgrade your appliance to 10.6.2 MR2 or 10.6.3 MR1 and then to the Sophos Firewall firmware.
Step 5
Learn about SFOS, upgrade and known issues.
- You retain all your current configuration and reports.
- On upgrade to SFOS, you get a 30-Day Full Guard Trial License. At any point during that 30-day period, you can permanently migrate your Cyberoam Licenses to SFOS Licenses. (For details, refer to [License Migration Guide](#)).
- Device warranty will be valid up to 5 years from date of registration after you have upgraded to SFOS.

Click **Continue** to Upgrade.
Step 6
On clicking Continue to Upgrade:
1. A Sophos ID and MySophos account will automatically be created for you [if it does not already exist].
2. You will receive an email on your registered email address containing instructions to reset your Sophos account password. Your appliance will automatically get registered on MySophos.
3. You can login to your MySophos account to download the firmware.
Step 7
Once the firmware is downloaded:

- Login to Cyberoam Web Admin Console and go to **System > Maintenance > Firmware**.
- Click Upload icon and upload the downloaded .gpg file, that is, downloaded firmware.
- Click **Upload and Boot**.

Step 8
Once the device boots up, login using your administrator credentials.
Login to SFOS

After upgrade, your CR Hardware Appliance’s Model number and Serial Key will remain the same. Virtual Appliances will be renamed to their corresponding XG Models.
Navigation in SFOS
The navigation bar on the Admin Console consists of menus and tabs. The menus are grouped into 4 headings and contain the following modules:

Monitor & Analyze: Menu contains:

- Control Center which acts as a dashboard to provide overall information about the system health, traffic insights, user-related and connected device related insights, usage and status of active security policies, most useful reports and alert messages.
- Reports that provide organizations with visibility into their networks while meeting the requirements of regulatory compliance.
- Current Activities that provides information about the live IPsec, SSL, IP and wireless connections to the device.
- Diagnostics that allow checking the health of your device in a single shot.

Protect: Protect group contains all related tabs under Firewall, Intrusion Prevention, Web Applications, Wireless, Email, Web Server and Advanced Threat Protection sub-menus.

System: System group contains menus which enable overall administration of the SF device like Profiles, Hosts and Services, Administration, Backup & Firmware and Certificates.

Configure: Configure Group contains menus which allow administrator to configure how the SF device is connected to the organization’s network like Network, VPN, Routing, Authentication and System Services.

License Migration

On upgrading to SFOS, a 30-day Full Guard License with all feature licenses will be applied to the Appliance for 30 days. You can then permanently migrate Licenses from CyberoamOS to SFOS from System > Administration > Licensing > Click on Migrate Cyberoam Licenses. For details on migration of licenses, refer to the License Migration Guide and Sophos XG Firewall: Frequently Asked Questions for Cyberoam customers.

Transformation from CR Firewall Rules to SFOS Firewall Rules

Your firewall rules will be migrated to SFOS as per following guidelines:
1. WAF-related rules will NOT be migrated.
2. For rules related to LOCAL Zone:
   a. If Action in source rule is marked ‘Reject’ or ‘Drop’, Action in migrated rule will be ‘Drop’.
   b. Log Firewall Traffic parameter will be disabled for all migrated rules.
c. Identity will be disabled for all migrated rules.
d. Destination Host will always be “Any” in migrated rule. Rules with specific Destination Host will not be migrated.
e. All service-specific rules will be migrated as is. However, if the service specified in the Cyberoam rule is not present in SFOS, the rule will not be migrated.

3. For non-identity based rules:
   a. Rules having Identity disabled will be migrated to SFOS as Network Rules.
   b. Rules which have Email scanning enabled will be migrated to SFOS as Business Application Rules. Rules with SMTP and/or SMTPS scanning enabled will be migrated as policy with Email Server template, while rules with POP, POPS and/or IMAP will be migrated as policy with Email Client Template.
   c. For Rules with Email Scanning and HTTP/HTTPS/FTP scanning enabled, Two [2] corresponding rules will be created in SFOS: One [1] Business Application Rule with Email Client or Email Server template (as applicable) and One [1] Network Rule with corresponding Web Filter, Application Filter and HTTP/HTTPS/FTP scanning configuration [if any].

4. For Virtual Host based Rules:
   a. Rules with Action as ‘Drop’ or ‘Reject’ will be migrated as respective User/Network rule containing external information of the source rule.
   b. Rules with Action as ‘Accept’ will be migrated to SFOS as Business Application Rules with Non-HTTP based template. The corresponding Web Filter, Application Filter, Multi-Link Management [MLM] and HTTP/HTTPS/FTP/IMAP/POP scanning configuration [if any] will NOT be carried over.
   c. Loopback rules will be migrated to SFOS as Business Application Rules with Non-HTTP based template. The corresponding Web Filter, Application Filter, Multi-Link Management [MLM] and HTTP/HTTPS/FTP/IMAP/POP scanning configuration [if any] will NOT be carried over.
   d. Reflexive Rules will be migrated as is to User/Network Rules. Rules with SMTP and/or SMTPS scanning enabled will be migrated as policy with Email Server template, while rules with POP, POPS and/or IMAP will be migrated as policy with Email Client template.
   e. Virtual host rules using #vhost as a service will be migrated as is.
   f. For rules with Destination as ‘Any’ and no Virtual Host Rules, a corresponding Virtual Host rule will be created along with a Network Rule as per the source and destination zones.
   g. Rules which have Destination host as ‘Any’ will be migrated to SFOS as a Business Application Rules with Non-HTTP based template. Rules with SMTP and/or SMTPS scanning enabled will be migrated as policy with Email Server template, while rules with POP, POPS and/or IMAP will be migrated as policy with Email Client template. The corresponding Web Filter, Application Filter,
Multi-Link Management (MLM) and HTTP/HTTPS/FTP scanning configuration (if any) will be carried over in a separate Network rule.

5. For identity-based rules [applicable when migrated from CR 10.6.3 MR3 or below to SFOS GA, MR1]:
   a. Rules in which Web and Application Filter policies are defined, are migrated as is to User Rules. If Destination Zone in the rule is zone other than WAN, the Web and Application Filter values are not carried over to migrated rule.
   b. Rules where specific users are specified, are migrated as User Rules. The user-specific Web and Application Filter policies are carried over as corresponding configuration in the rule. However, if the CR rule itself has Web and Application Filter parameters defined, the rule is migrated as is.
   c. The group-specific Web and Application Filter policies are carried over as corresponding configuration in the rule. However, if the CR rule itself has Web and Application Filter parameters defined, the rule is migrated as is.
   d. Rules where specific groups or “Any” is specified, are migrated as User Rules.
   e. If the user-specific policies are different than those in the group, a separate User Rule is created for the user-specific policies as per method described in the point 5 b.
   f. If Email scanning is enabled in in CR Rule, a corresponding Business Application Rule with Email Client template is also created along with this rule.

6. For identity-based rules [applicable when migrated from CR 10.6.3 MR4 to SFOS MR2]:
   a. Rules in which User’s Policy is applied for web/app filter, are migrated with ‘Internet Scheme’ applied to the migrated Rules. In the Internet Scheme* page in SFOS [Web > Internet Scheme] all the users/groups from Cyberoam are listed along with the specific web and app filter policies that are applied to each.
   b. User or Group based rules in which User’s Policy is applied for web/app filter, are migrated with ‘Internet Scheme’ applied to the migrated Policies. In the Internet Scheme* page in SFOS [Web > Internet Scheme] the users/groups affected by the rule are listed along with the specific web and app filter policies that are applied to each.
   c. User or Group based rules in which app filter is set as User’s Policy and web filter is set as ‘CIPA’, are migrated with its app filter set to ‘Internet Scheme’ and web filter set to ‘CIPA’.
   d. User or Group based rules in which app filter is set as Custom Policy and web filter is set as User’s Policy, are migrated with its app filter set to Custom Policy and web filter is set to Internet Scheme.
   e. If user or group is not present in the Internet Scheme* page, the Default web and app filter policies are applied on the users.
7. Rules containing Discover (TAP) zone will not be migrated.

Internet Scheme Page
*The Internet Scheme page is displayed after migration from CR 10.6.3 MR4 to SFOS MR2. It displays the list of all users and groups affected by migrated firewall rules, listing out the corresponding web and app filter policies applied to them.
Example:
Cyberoam Firewall Rules in which User’s Policy is applied for web/app filter are migrated with ‘Internet Scheme’ applied to the migrated Firewall Rules.

![Image of Internet Scheme Page]

In the Internet Scheme* page in SFOS [Web > Internet Scheme] all the users/groups from Cyberoam are listed along with the specific web and app filter policies that are applied to each.

![Image of Policies Page]
Behavior Difference
Once migrated, difference of behavior between Cyberoam Firewall Rules and Sophos Firewall Rules:
- Administrator will not be able to configure Email Scanning, WAF & Virtual Host on network/user rules.
- Web and Application Filter Policies are no longer associated with individual users or groups. They will have to be applied using Firewall Rules.
- AV/AS scanning, web/application filter policy and MLM are not available in Non-HTTP (Virtual Host) Business Application Rules.
- Web / Application filter policies are not available in Email Client and Email Server Templates.
- Multi-Link Management is not available on Email Server Template.
- Destination Host “Any” will not cover all the virtual hosts.
- For Business Application Rules, corresponding Reflexive Firewall Rules will be created but will not be visible on the Firewall Rule page. The Reflexive Rule inherits its properties from the rule to which it is associated.
Changes in Individual Features

Licensed Features
For features related to Web, Email and Network Protection, if the respective license is not subscribed, SFOS will allow you to configure the feature, but will not do the corresponding scanning and logging. For example, if your Network Protection module is not subscribed, SFOS will allow you to create custom IPS signatures, policies, etc. but will not scan or log traffic.
Similarly, if any license expires, SFOS will stop scanning and logging of traffic related to that module without disrupting the network traffic.
However, for security reasons, this behavior does not hold true for Web Server Protection Module. You need a valid License of the module for SFOS to allow any traffic from your Web Server[s].

Wireless
If the Security Mode of any Wireless Network is set as WEP Open, on migration, the Wi-Fi Key of that network[s] will be regenerated. This is applicable to Cyberoam firmware version 10.6.3 MR4 onwards.
If Wireless Protection in Cyberoam is disabled, on migration the Access Point and DHCP configuration is not carried over to SFOS.

Web Application Firewall (WAF)
The WAF configuration of the Cyberoam Appliance will not be migrated to the SFOS Firmware. You will have to re-configure WAF-related policies in the SFOS firmware.

Dynamic DNS
In CR, if you used Cyberoam [<host name>, ddns.cyberoam.com] as your Dynamic DNS service provider, it will be migrated to SFOS as a non-editable entity. To continue using DDNS services smoothly, it is recommended to either register with and use a third-party DDNS service provider, or use Sophos [<host name>.myfirewall.co] as your provider.

General Authentication Client
The behavior changes are:
- Users will NOT be able to login to SFOS using Cyberoam General Authentication Client (GAC). They will have to download and install new instances called Client Authentication Agents (CAA) from User Portal.
- User-MAC binding will not be supported after migration to SFOS.
- After migration, each agent will be bound to the XG Firewall through the appliance certificate and communication will take place over a secure channel. Hence, an agent authenticating to one XG Firewall cannot be bound to another XG Firewall.
- In SFOS, user will be logged out from CAA once they connect to the Device using VPN.
SSL VPN
The behavior changes are:
- SSL VPN users will NOT be able to connect to SFOS using Cyberoam SSL VPN Client. They will have to install new instances of SSL VPN Client for SF which can be obtained from the User Portal.
- The SSL VPN Portal [accessed by browsing to https://<Cyberoam WAN IP Address>:8443] will be a part of the SFOS User Portal. After migration, the User Portal can be accessed by browsing to https://< Cyberoam LAN IP Address>:8443.
- The SSL VPN port can no longer be configured in SFOS.
- SSL VPN Bookmarks of Type IBM Server Terminal will be converted to TELNET Bookmark type after migration.
- If you have customized the Simultaneous Login SSL VPN Users, after migration, reset the limit to unlimited to prevent the “Maximum Login Limit” error displayed to users.
- If you have configured per user certificate for SSL VPN, after migration you will have to delete the user certificates from your Appliance. Then, the user[s] need to download and import a new SSL VPN Client bundle for SFOS from the User Portal.

Following SSL VPN related commands are discontinued:
console> set sslvpn proxy-sslv3
console> set sslvpn web-access
console> show sslvpn log
console> show sslvpn proxy-sslv3
console> show sslvpn web-access

Web and Application Filtering
The Web Categorization Database in SFOS will contain a different set of categories than Cyberoam.
If Web Protection License is not subscribed, you will be allowed to configure web and application settings, but the traffic will not be scanned or logged.
Web Filter Policy page [Web > Policies] has been revamped to allow inline configuration of policies.
Further, as compared to Cyberoam, SFOS does not support:
- Selective upstream proxy [CLI Command: console> set service-param HTTPS ssl_upstream_tunnel]
- ICAP [CLI Command: console> set icap edit]
- Proxy DoS Settings [CLI Command: set http_proxy dos]

Identity
For integration with an Active Directory [AD] Server, Integration Type ‘Loose Integration’ has been discontinued. By default, XG Firewall will integrate with an AD Server with Tight Integration. If you have configured your AD Server with Loose Integration, on migration it will be converted to Tight Integration.
Web and Application Filter policies cannot be assigned to users/groups directly in SFOS. If you want to apply any Web or Application Filter policies on a user/group, do it using Firewall Rules.

**High Availability (HA)**
Specification of a Passphrase will be compulsory for HA configuration in SFOS. Existing Cyberoam HA setups will be migrated to SFOS with a unique random passphrase. You can check and update the HA configuration from Configure > System Services > High Availability in SFOS firmware.

**Certificates**
Cyberoam Certificates will be carried over to SFOS firmware with the following changes:
- Default CA will be unchanged.
- Cyberoam Self signed CA will be renamed to SecurityApplianceSelfSignedCA, contents will remain same.
- Cyberoam_SSL_CA will be renamed to SecurityAppliance_SSL_CA, and will be regenerated with default values.
- Appliance Certificate will remain same and will remain signed by SecurityApplianceSelfSignedCA.
- Behavior of SSLVPN per user certificate will remain same as in Cyberoam.

**DHCP/PPPoE**
In SF firmware, DHCP and PPPoE can be configured on interfaces of all zones except of VPN. In Cyberoam, it was only available in WAN Zone.
If Two [2] Cyberoam Appliances in HA are migrated to SFOS, the DHCP Service in the Auxiliary Appliance may stop running. You need to remove the existing DHCP configuration to restart the DHCP service.

**SNMP**
You no longer require to create a firewall rule in SFOS to allow SNMP traffic when SNMP is configured. The related Firewall Rule created in Cyberoam will NOT be migrated as is.

**Country Host**
- Country Hosts will be migrated to SFOS as Country Names. You no longer need to create Country Host explicitly and can directly use list of countries available for Country group creation.
- IP Hosts having Hostname as Country name will be migrated to SFOS as Country name_Custom.

**Custom Zones**
By default, following services will be enabled for the migrated custom zones on the System > Administration > Device Access page:
- SNMP service will be enabled for custom LAN and DMZ zone.
• SMTP Relay service will be enabled for custom LAN zone.

**HTTP Redirection**
SFOS Web Admin Console will be accessible only via HTTPS after migration, even if you had configured Device Access through HTTP. Your HTTP requests will be automatically redirected to HTTPS. In SFOS, you will be allowed to enable and configure admin access through HTTPS only.
After migration, HTTP-related Local Service ACL Exception Rules with DROP action will be deleted, while those with ACCEPT action will be converted to HTTPS rules.

**Telnet Access**
CR Appliances that have Telnet access enabled for any zones will be converted to SSH access on migration. In SFOS, if you enable Telnet access, a warning message will be displayed advising to switch to SSH access.

**Web Proxy**
Web Proxy section has been moved to Web > Advanced. The parameter ‘Trusted Ports’ is renamed to ‘Allowed Destination Ports’.

**Important Notes for Cyberoam to SFOS Upgrade**
1. The SFOS Admin Console cannot be accessed by via HTTP.
   a. In SFOS, HTTP setting has been removed from the Device Access page.
   b. If HTTP access was enabled before upgrade, the admin port settings for HTTP will be preserved and any HTTP request for device access will be redirected to HTTPS.
   c. In case of fresh installation, factory reset configuration or if HTTP was disabled before upgrade, the HTTP admin port settings will be removed.
2. SFOS cannot be accessed over TELNET. Hence,
   a. All TELNET requests will be converted to SSH.
   b. A warning message will be displayed on the Device Access page if admin enables telnet access for any zone.
3. ICAP will not be supported.
4. Web Proxy DOS Setting will not be available.
5. AV Scanning on Virtual Host will not be supported without active Webserver Protection (WAF) subscription.
6. SFOS will not create ‘All’ service based rule for ACL [local] rule.
7. FTP Scanning will only be supported for User/Network rule.
8. JavaScript emulation for URLs/Cookies will not be supported in Webserver Protection (WAF).
9. Auto-learning of added exceptions in WAF will not be supported.
10. Instant Messaging [IM] will not be supported.
11. Route based VPN will not be supported.
12. Nested Group Support in NTLM will not be supported.
13. Overriding Organizational Web Filter Policy Restrictions will not be available.
14. User MAC binding will not be supported.
15. SSLVPN Port Configuration will not be supported.
16. All Self-signed Certificates and Certificate Authorities will be regenerated on upgrade. You will have to re-import the certificate for all services that use them.
17. Reflexive Rule for Business Application Rules will not be displayed on the Firewall page. All the policies of the Reflexive Rule will be inherited from the Business Application Rule [including SNAT].
18. Cyberoam allowed AV scanning of Web Servers [Virtual Hosts] if AV Module is subscribed and WAF module is NOT subscribed. However, in SFOS, admin needs an active Web Server Protection subscription for AV scanning of Web Servers.

**Renamed CR Features**

1. My Account is renamed to User Portal. The User Portal displays user information and facilitates SSL VPN, Hotspot and downloading of clients. It is accessible by browsing to https://<SF IP Address> and is enabled by default from the WAN Zone.
2. QoS is renamed to Traffic Shaping.
3. Network > Gateway is renamed to WAN Link Manager.
4. Parent Proxy is renamed to Upstream Proxy.
5. Appliance Access is renamed to Device Access.
6. 4-eye Authentication is renamed to Data Anonymization.
7. Data Transfer Policies is renamed to Network Traffic Quota.
9. Wireless WAN is renamed to Cellular WAN.
10. In **Web > Protection**, Deny Unknown Protocols is renamed to Block unrecognized SSL protocols.
11. In **Web > Protection**, Allow Invalid Certificates is renamed to Block invalid certificates (behavior is changed as the name suggests).
Copyright Notice

Copyright 2016-2017 Sophos Limited. All rights reserved.
Sophos is registered trademark of Sophos Limited and Sophos Group. All other product
and company names mentioned are trademarks or registered trademarks of their
respective owners.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted,
in any form or by any means, electronic, mechanical, photocopying, recording or otherwise
unless you are either a valid licensee where the documentation can be reproduced in
accordance with the license terms or you otherwise have the prior permission in writing of
the copyright owner.