SOPHOS

Security made simple.

Migration Guide

Cyberoam to Sophos Firewall

For Customers with Cyberoam Appliances

Document Date: October 2016

Contents

Change Log

Revision Date	Description
17 November, 2015	Added: "Dynamic DNS" section under **Changes in Individual Features**
26 November, 2015	Removed: Point related to Custom SSL port in SSL VPN section under **Changes in Individual Features** Added: Note in Step 1 under **Steps to Migrate**.
14 December, 2015	Updated: First point related to Rollback under **Points to Note before Migration** 5th point related to AV Scanning of Web Servers under **Discontinued CR Features**
7th April, 2016	Added: Wireless point under **Changes in Individual Features** Updated: List of supported Appliance under Supported Cyberoam Appliances DHCP/PPPoE point under **Changes in Individual Features**
21st April, 2016	Added: Point for identity-based firewall rules under Transformation of Firewall Rules to Security Policies. Updated: List of supported Appliance under Supported Cyberoam Appliances
30th June, 2016	Added: Information for Internet Scheme Page under Transformation of Firewall Rules to Security Policies.
10th October, 2016	Updated entire guide for SFOS v16.

11th October, 2016	Renamed “Discontinued CR Features” section to “Important Notes for CR to SF Migration. Updated section with relevant points for SFOS v16.

Supported Cyberoam Appliances

The following Cyberoam (CR) Appliances can be upgraded to Sophos Firewall (SF) firmware:

- Cyberoam Virtual Appliances: All Virtual Appliances.
    - Virtual Trial Appliance (CRiV-TR) **CANNOT** be upgraded.

- Cyberoam iNG Series: All iNG Appliances.
    - Appliances that **CANNOT** be upgraded: Certain hardware versions of CR10iNG, CR10wiNG, CR15iNG/4P and CR15wiNG. For appliances with supported hardware, an upgrade link will be visible on the dashboard and the customer portal.

- Cyberoam i Series: CR200i and CR300i.
    - Appliances that **CANNOT** be upgraded: CR15i, CR15wi, CR25wi and CR35wi.

- Cyberoam ia Series: CR500ia and above.
    - Appliances that **CANNOT** be upgraded: CR25ia, CR35ia, CR50ia and CR100ia.

It is recommended for Cyberoam to have firmware version 10.6.3 MR4 or higher to upgrade to SF firmware.

- For Appliances running 10.6.2 MR1 and below, upgrade to SF firmware is a two-step process wherein they first upgrade to the latest release of 10.6.2 or 10.6.3 versions and then to the SF firmware.
- For Appliances running 10.6.3, upgrade to SF firmware is a two-step process wherein they first upgrade to the latest release of 10.6.3 version and then to the SF firmware.
- Appliances running 10.6.4 or higher can upgrade to SFOS v16 only. However, if appliance is upgraded to SFOS v15, it will boot up with factory default settings.

Note:

To upgrade, CR Appliance should be registered in Cyberoam Customer Portal and should have a valid support subscription.

Points to Note before Migration

1. If your CR Appliance is migrated to SF-OS firmware on a Full Guard Trial License, seamless rollback to CyberoamOS is possible. All you have to do is reboot the appliance and select CyberoamOS to boot it. All previous configurations, reports and subscriptions (except WAF) will be restored once the device is rebooted.

   Note:
    - Any new configuration (including features exclusive to SF-OS) will be lost once you roll back.
    - The downtime in this roll-back is similar to the time required for rebooting your system.
    - Rollback will not be possible after your existing CR Licenses have migrated to SF-OS licenses.

2. Appliances upgraded to SF firmware can no longer be managed by CCC. You will need Sophos Firewall Manager (SFM) to manage the upgraded appliances.

3. Appliances upgraded to SF firmware can no longer be integrated with Cyberoam iView. You will need Sophos iView (Version 2) for reporting of migrated appliances.
4. Once your Appliance is upgraded to SF firmware, the Warranty will be valid till 5 years from original date of Appliance registration on condition that you have an active Support License.
5. Once migrated, your Appliance will NOT be applicable for the Cyberoam Trade-Up schemes. However, you can opt for Sophos Firewall Hardware Refresh programs when it is launched.
6. Once migrated, a backup of the Cyberoam firmware cannot be restored on the SF firmware.

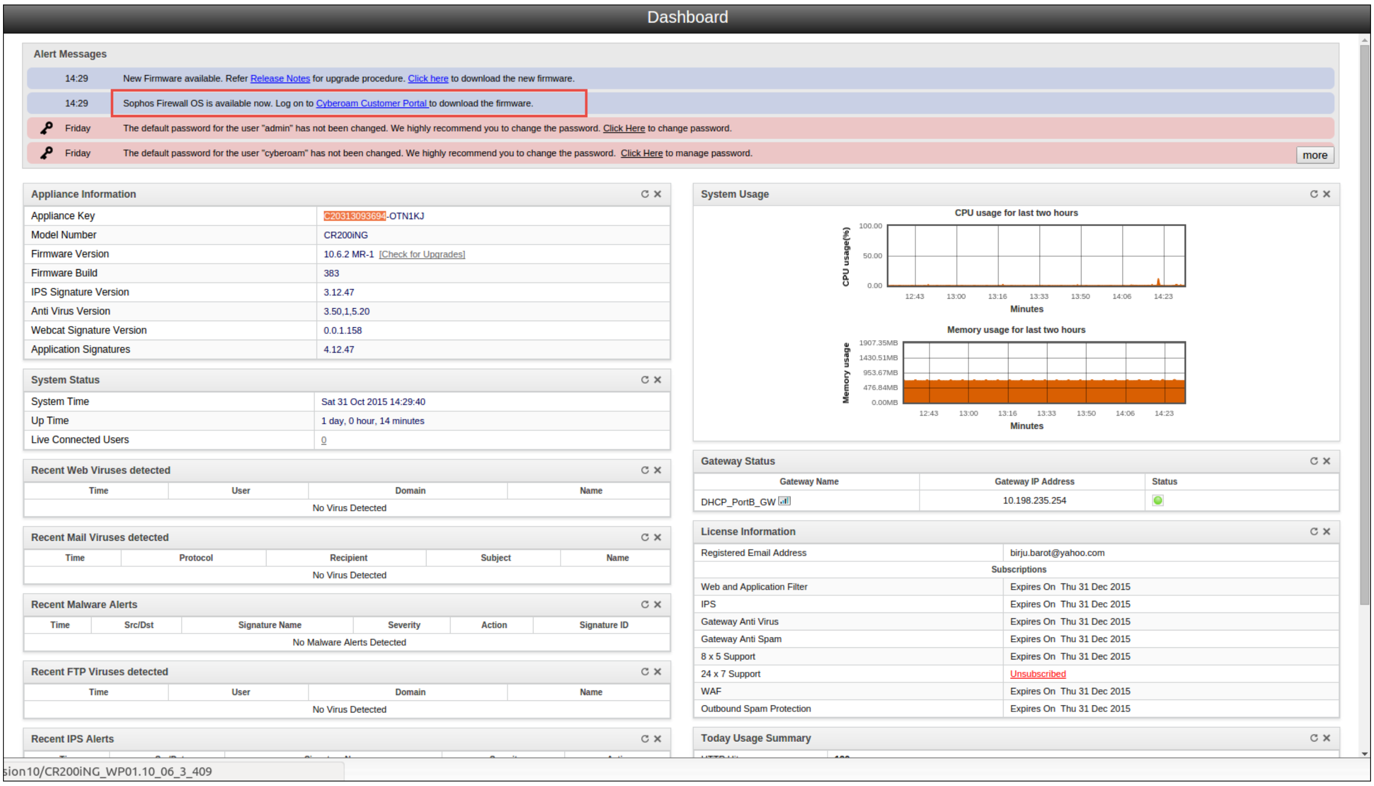
Also refer to the **Known Issues – Cyberoam to Sophos Firewall Migration**.

Steps to Migrate

You can migrate your Cyberoam appliance to Sophos Firewall by following the steps given below.

Step 1

Once the SF firmware is available, an alert is displayed on your dashboard. Click the link.



Dashboard

Alert Messages

14:29	New Firmware available. Refer Release Notes for upgrade procedure. Click here to download the new firmware.
14:29	Sophos Firewall OS is available now. Log on to Cyberoam Customer Portal to download the firmware.
Friday	The default password for the user "admin" has not been changed. We highly recommend you to change the password. Click Here to change password.
Friday	The default password for the user "cyberoam" has not been changed. We highly recommend you to change the password. Click Here to manage password.

Appliance Information

Appliance Key	C20313093694-OTN1KJ
Model Number	CR200iNG
Firmware Version	10.6.2 MR-1 [Check for Upgrades]
Firmware Build	383
IPS Signature Version	3.12.47
Anti Virus Version	3.50,1,5.20
Webcat Signature Version	0.0.1.158
Application Signatures	4.12.47

System Status

System Time	Sat 31 Oct 2015 14:29:40
Up Time	1 day, 0 hour, 14 minutes
Live Connected Users	0

Recent Web Viruses detected

Time	User	Domain	Name
No Virus Detected			

Recent Mail Viruses detected

Time	Protocol	Recipient	Subject	Name
No Virus Detected				

Recent Malware Alerts

Time	Src/Dst	Signature Name	Severity	Action	Signature ID
No Malware Alerts Detected					

Recent FTP Viruses detected

Time	User	Domain	Name
No Virus Detected			

Recent IPS Alerts

System Usage

Gateway Status

Gateway Name	Gateway IP Address	Status
DHCP_PortB_GW	10.198.235.254	●

License Information

Registered Email Address	birju.barot@yahoo.com
Subscriptions	
Web and Application Filter	Expires On Thu 31 Dec 2015
IPS	Expires On Thu 31 Dec 2015
Gateway Anti Virus	Expires On Thu 31 Dec 2015
Gateway Anti Spam	Expires On Thu 31 Dec 2015
8 x 5 Support	Expires On Thu 31 Dec 2015
24 x 7 Support	Unsubscribed
WAF	Expires On Thu 31 Dec 2015
Outbound Spam Protection	Expires On Thu 31 Dec 2015

Today Usage Summary

sion10/CR200iNG_WP01.10_06_3_409

Note:

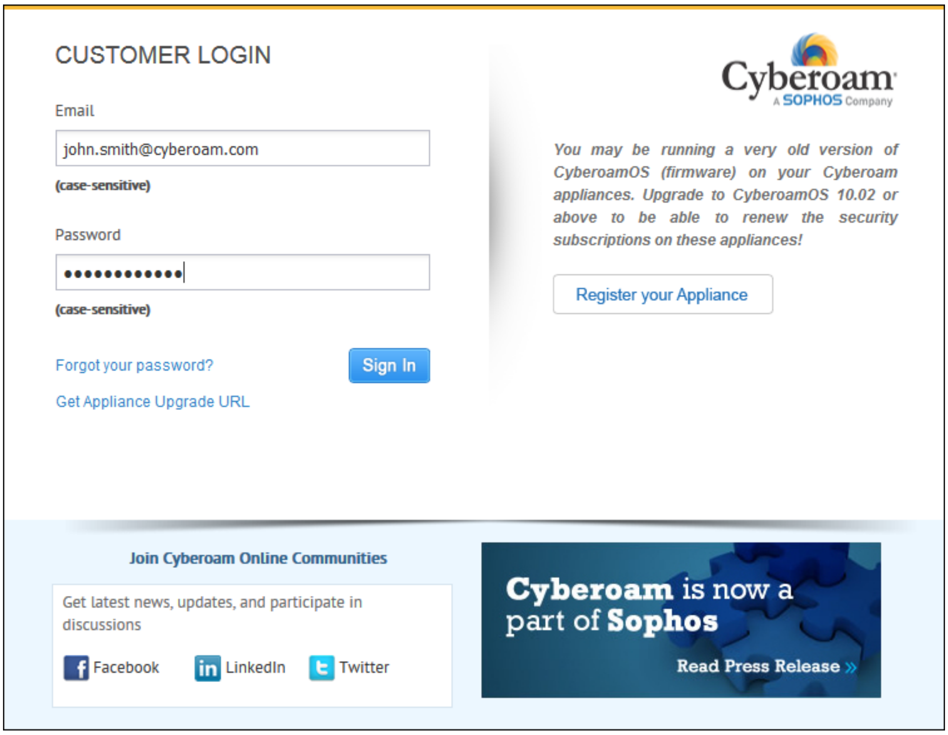
The SF firmware will be available ONLY to Cyberoam Appliances in which all subscriptions are valid till 1st January, 2016 and after. If any or all of your subscriptions expire before 1st January, 2016, you may first renew them and then upgrade your Appliance. Refer to the following articles for more details:

- How do I view my Registration and Subscription details on Cyberoam?

- How do I renew Subscription of Modules?

Step 2

On clicking the link, you will be redirected to Cyberoam Customer Portal. Login to the Portal.



CUSTOMER LOGIN

Email: john.smith@cyberoam.com
(case-sensitive)

Password: ••••••••••••
(case-sensitive)

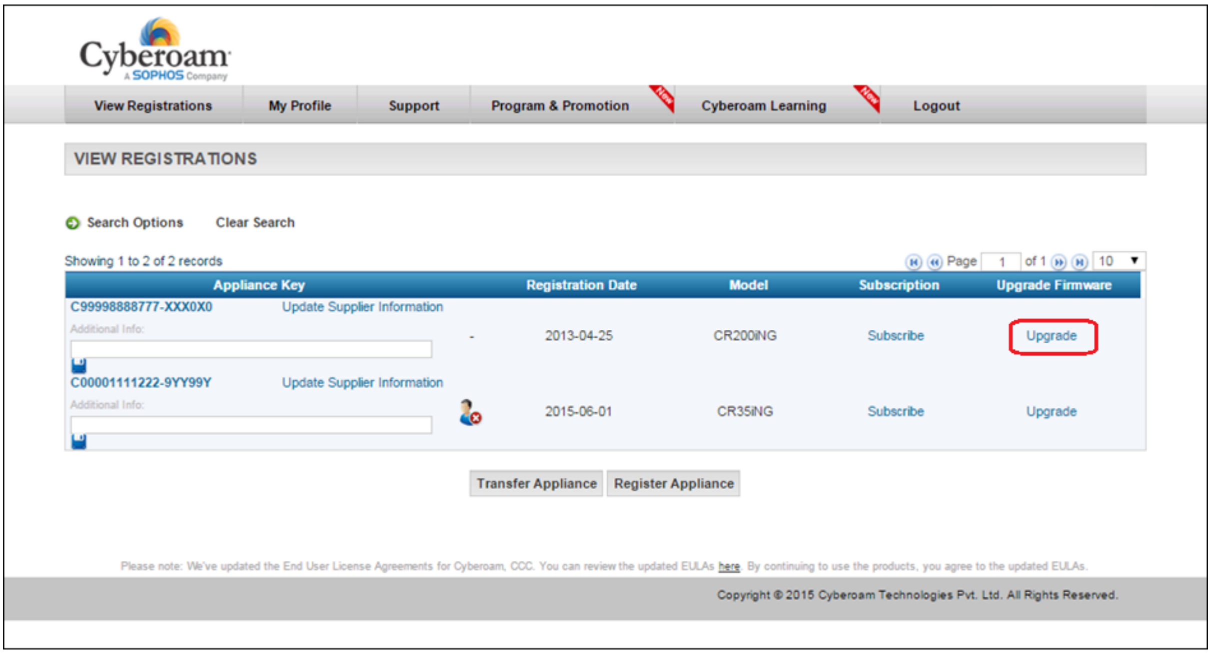
You may be running a very old version of CyberoamOS (firmware) on your Cyberoam appliances. Upgrade to CyberoamOS 10.02 or above to be able to renew the security subscriptions on these appliances!

Join Cyberoam Online Communities

Get latest news, updates, and participate in discussions

Step 3

Click **Upgrade** against the hardware or virtual appliance you want to upgrade.



VIEW REGISTRATIONS

Showing 1 to 2 of 2 records

Page 1 of 1 10

Appliance Key			Registration Date	Model	Subscription	Upgrade Firmware
C99998888777-XXX0X0 Additional Info:	Update Supplier Information	-	2013-04-25	CR200iNG	Subscribe	Upgrade
C00001111222-9YY99Y Additional Info:	Update Supplier Information		2015-06-01	CR35iNG	Subscribe	Upgrade

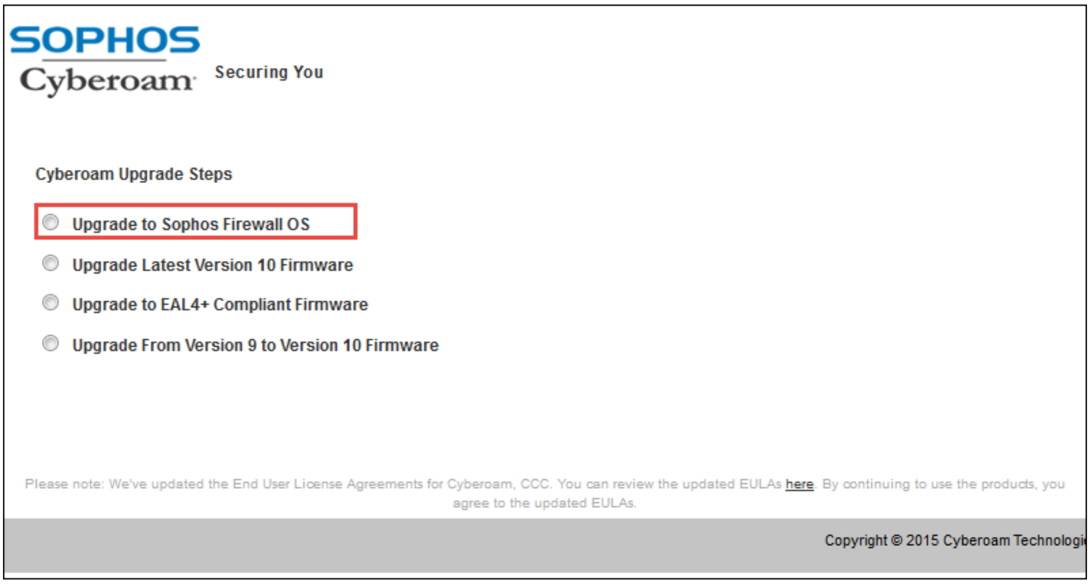
Please note: We've updated the End User License Agreements for Cyberoam, CCC. You can review the updated EULAs here. By continuing to use the products, you agree to the updated EULAs.

Copyright © 2015 Cyberoam Technologies Pvt. Ltd. All Rights Reserved.

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 Sophos Firewall firmware only if your 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.



Cyberoam Upgrade Steps

○ Upgrade to Sophos Firewall OS

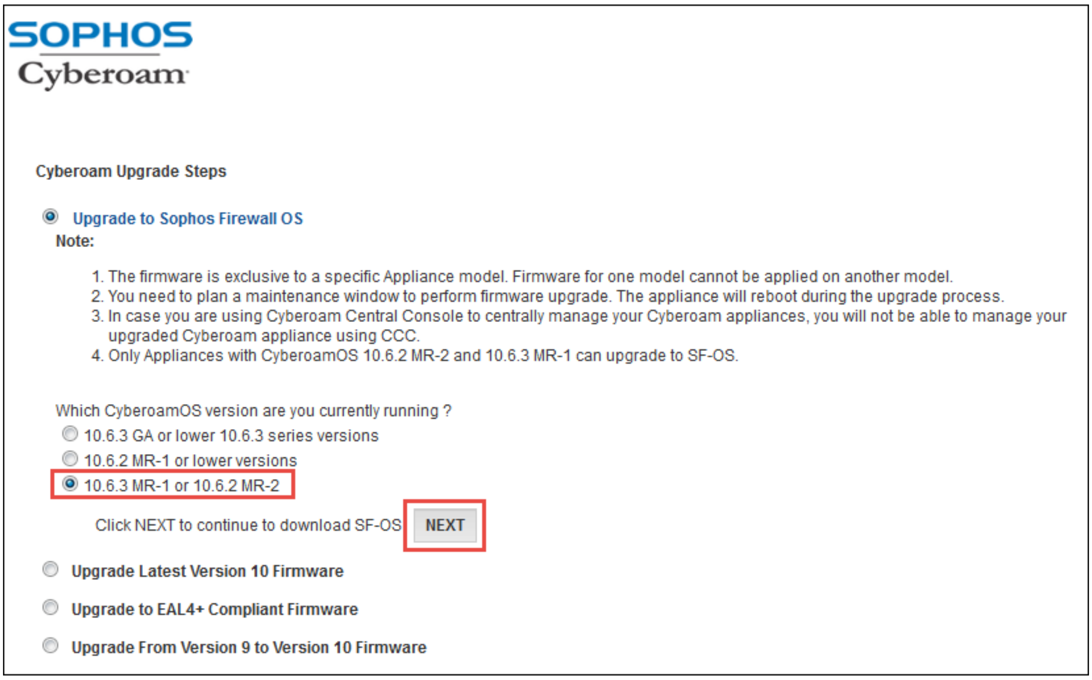
○ Upgrade Latest Version 10 Firmware

○ Upgrade to EAL4+ Compliant Firmware

○ Upgrade From Version 9 to Version 10 Firmware

Please note: We've updated the End User License Agreements for Cyberoam, CCC. You can review the updated EULAs here. By continuing to use the products, you agree to the updated EULAs.

Copyright © 2015 Cyberoam Technologi



Cyberoam Upgrade Steps

● Upgrade to Sophos Firewall OS

Note:

1. The firmware is exclusive to a specific Appliance model. Firmware for one model cannot be applied on another model.
2. You need to plan a maintenance window to perform firmware upgrade. The appliance will reboot during the upgrade process.
3. In case you are using Cyberoam Central Console to centrally manage your Cyberoam appliances, you will not be able to manage your upgraded Cyberoam appliance using CCC.
4. Only Appliances with CyberoamOS 10.6.2 MR-2 and 10.6.3 MR-1 can upgrade to SF-OS.

Which CyberoamOS version are you currently running ?

○ 10.6.3 GA or lower 10.6.3 series versions

○ 10.6.2 MR-1 or lower versions

● 10.6.3 MR-1 or 10.6.2 MR-2

Click NEXT to continue to download SF-OS

○ Upgrade Latest Version 10 Firmware

○ Upgrade to EAL4+ Compliant Firmware

○ Upgrade From Version 9 to Version 10 Firmware

Note:

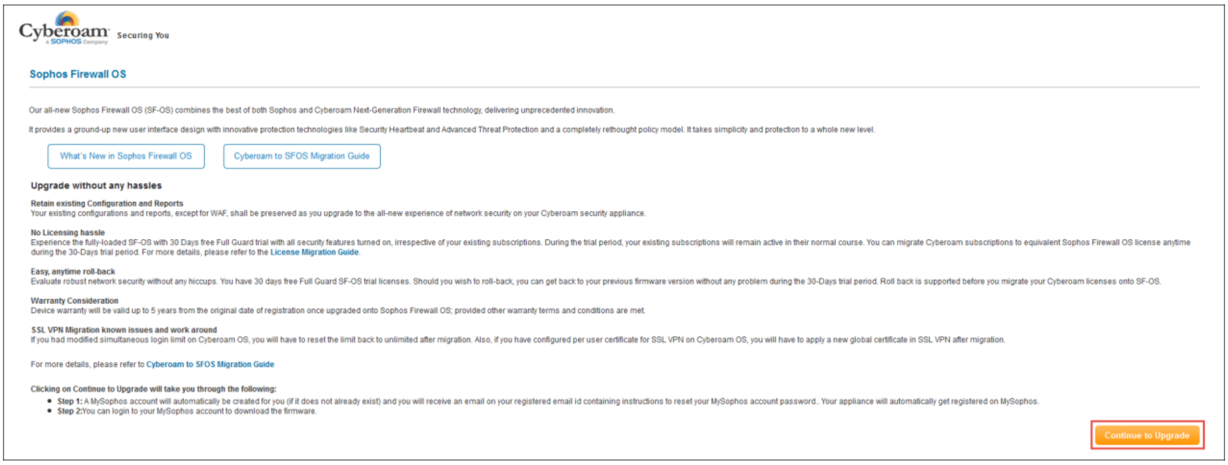
Appliances upgraded to Sophos Firewall firmware can no longer be managed by CCC. You will need Sophos Firewall Manager (SFM) to manage the upgraded appliances.

Step 5

Read the complete instructions and click **Continue to Upgrade**.

Note:

You can view the instructions for License Upgrade on the screen. Please note that if you select **Migrate License**, you will have to upgrade to SF-OS firmware within the next 30 days. The CyberoamOS will be automatically deactivated after 30 days.



Cyberoam
A SOPHOS Company
Securing You
What's New in Sophos Firewall OS
Cyberoam to SFOS Migration Guide
Continue to Upgrade

Sophos Firewall OS

Our all-new Sophos Firewall OS (SF-OS) combines the best of both Sophos and Cyberoam Next-Generation Firewall technology, delivering unprecedented innovation.

It provides a ground-up new user interface design with innovative protection technologies like Security Heartbeat and Advanced Threat Protection and a completely rethought policy model. It takes simplicity and protection to a whole new level.

Upgrade without any hassles

Retain existing Configuration and Reports
Your existing configurations and reports, except for WAF, shall be preserved as you upgrade to the all-new experience of network security on your Cyberoam security appliance.

No Licensing hassle
Experience the fully-loaded SF-OS with 30 Days free Full Guard trial with all security features turned on, irrespective of your existing subscriptions. During the trial period, your existing subscriptions will remain active in their normal course. You can migrate Cyberoam subscriptions to equivalent Sophos Firewall OS license anytime during the 30-Days trial period. For more details, please refer to the License Migration Guide.

Easy, anytime roll-back
Evaluate robust network security without any hiccups. You have 30 days free Full Guard SF-OS trial licenses. Should you wish to roll-back, you can get back to your previous firmware version without any problem during the 30-Days trial period. Roll back is supported before you migrate your Cyberoam licenses onto SF-OS.

Warranty Consideration
Device warranty will be valid up to 5 years from the original date of registration once upgraded onto Sophos Firewall OS; provided other warranty terms and conditions are met.

SSL VPN Migration known issues and work around
If you had modified simultaneous login limit on Cyberoam OS, you will have to reset the limit back to unlimited after migration. Also, if you have configured per user certificate for SSL VPN on Cyberoam OS, you will have to apply a new global certificate in SSL VPN after migration.

For more details, please refer to Cyberoam to SFOS Migration Guide

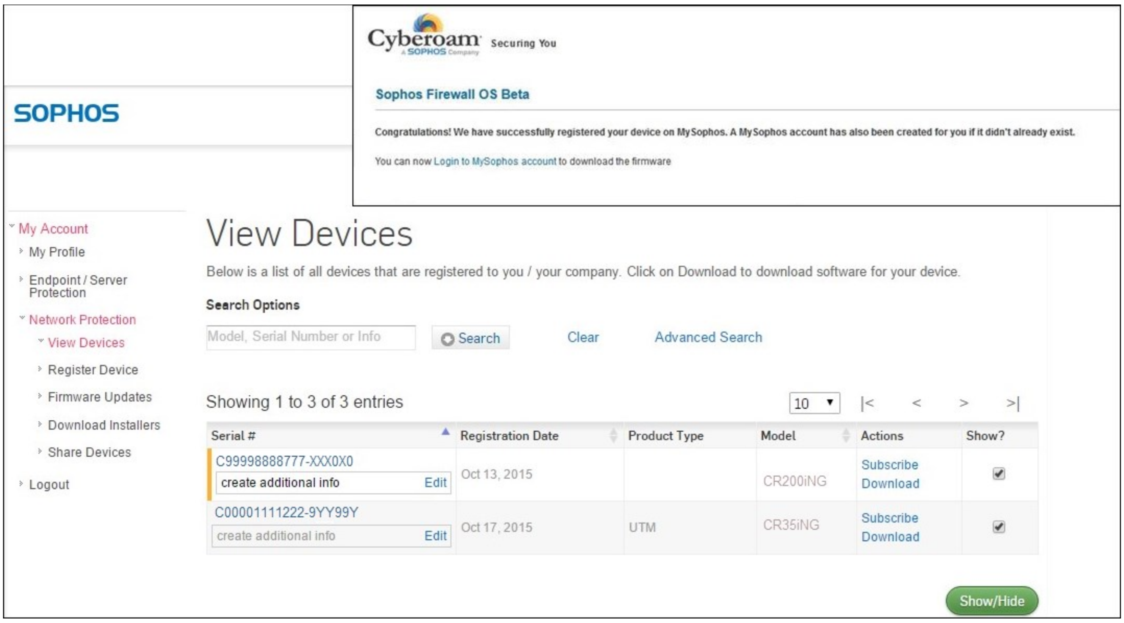
Clicking on Continue to Upgrade will take you through the following:

- **Step 1:** A MySophos account will automatically be created for you (if it does not already exist) and you will receive an email on your registered email id containing instructions to reset your MySophos account password.. Your appliance will automatically get registered on MySophos.
- **Step 2:**You can login to your MySophos account to download the firmware.

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) and 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.
2. You can login to your MySophos account to download the firmware.



Sophos Firewall OS Beta

Congratulations! We have successfully registered your device on MySophos. A MySophos account has also been created for you if it didn't already exist.

You can now Login to MySophos account to download the firmware

View Devices

Below is a list of all devices that are registered to you / your company. Click on Download to download software for your device.

Search Options

Model, Serial Number or Info

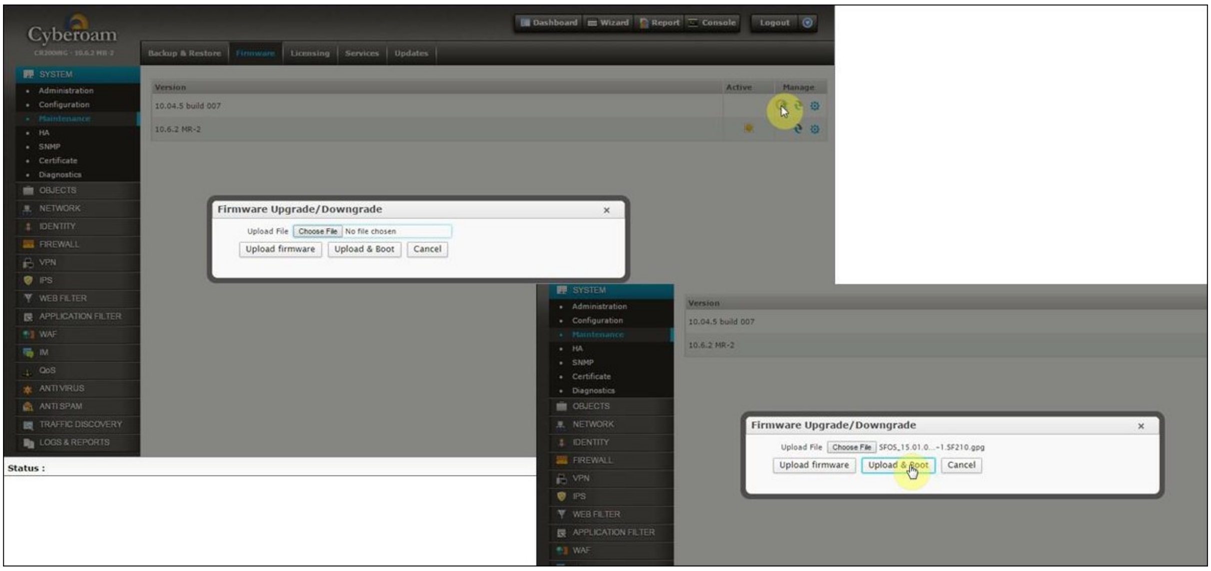
Showing 1 to 3 of 3 entries

Serial #	Registration Date	Product Type	Model	Actions	Show?
C99998888777-XXX0X0 create additional info Edit	Oct 13, 2015		CR200iNG	Subscribe Download	☑
C00001111222-9YY99Y create additional info Edit	Oct 17, 2015	UTM	CR35iNG	Subscribe Download	☑

Step 7

Once firmware is downloaded, follow instructions below:

- 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**.



Version
10.04.5 build 007
10.6.2 MR-2

Firmware Upgrade/Downgrade

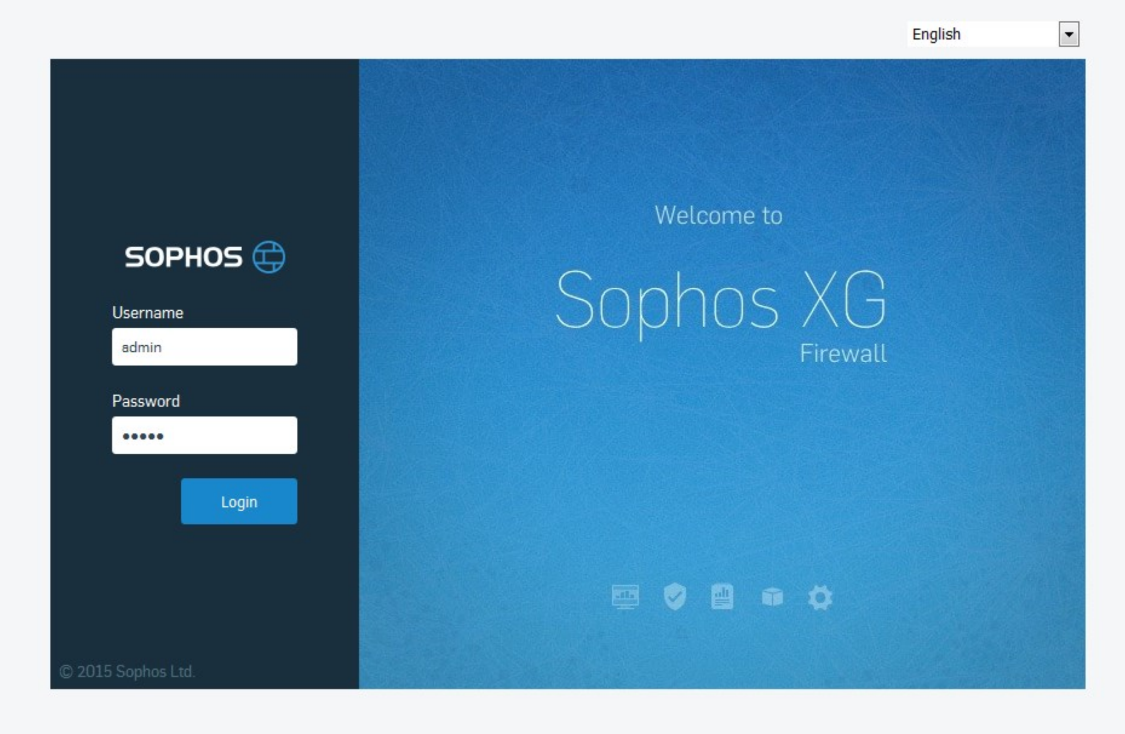
Upload File: Choose File No file chosen

Firmware Upgrade/Downgrade

Upload File: Choose File SFOS_15.01.0...-1.SF210.gpg

Step 8

Once the device boots up, login using your administrator credentials.

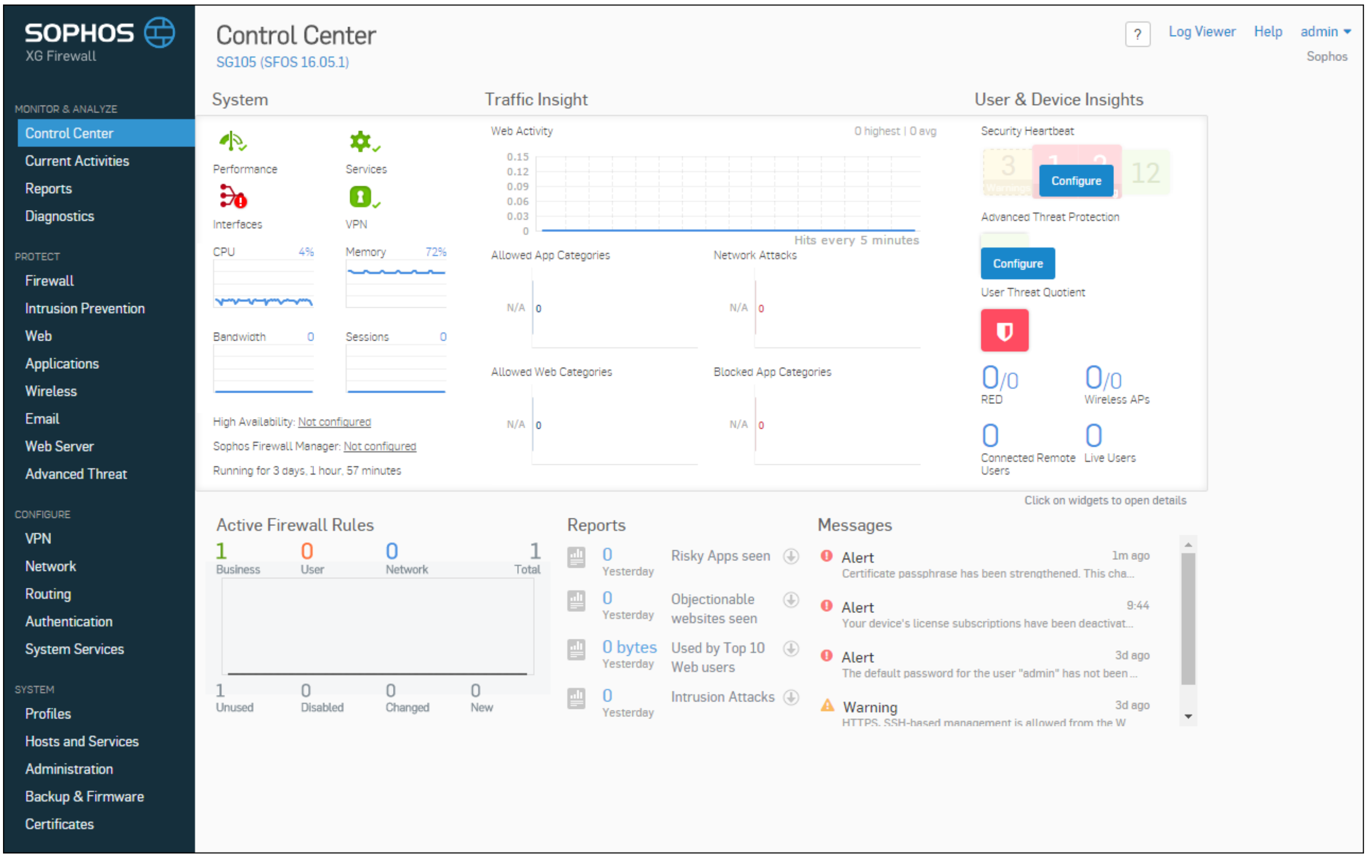


Username: admin

Password: •••••

Login to Sophos Firewall

After upgrade, your CR Hardware Appliance's Model number and Serial Key will remain the same. Virtual Appliances will be renamed to their corresponding SF Models.



Certificate passphrase has been strengthened. This cha...

Your device's license subscriptions have been deactivat...

The default password for the "admin" has not been ...

HTTPS, SSH-based management is allowed from the W

Navigation in Sophos Firewall

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 allows 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 enables overall administration of the SF device like Profiles, Hosts and Services, Administration, Backup & Firmware and Certificates.

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

License Migration

You can migrate Licenses from CyberoamOS to Sophos Firewall OS (SFOS) from:

- Customer Portal
- **System > Administration> Licensing** at the time of migration

For details on migration of licenses, refer to the **License Migration Guide**.

Transformation from CR Firewall Rules to SF Firewall Rules

Your firewall rules will be migrated to SF 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 SF, the rule will not be migrated.
3. For non-identity based rules:
    a. Rules having Identity disabled will be migrated to SF as Network Rules.
    b. Rules which have Email scanning enabled will be migrated to SF 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 SF: 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 SF 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 SF 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 SF as 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 SF 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 SF 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 SF (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 SF (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.

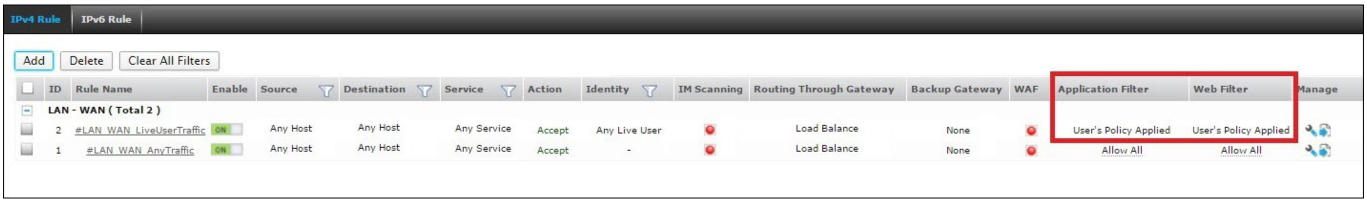
e. If user or group is not present in the Internet Scheme* page, the Default web and app filter policies are applied on the users.

Internet Scheme Page

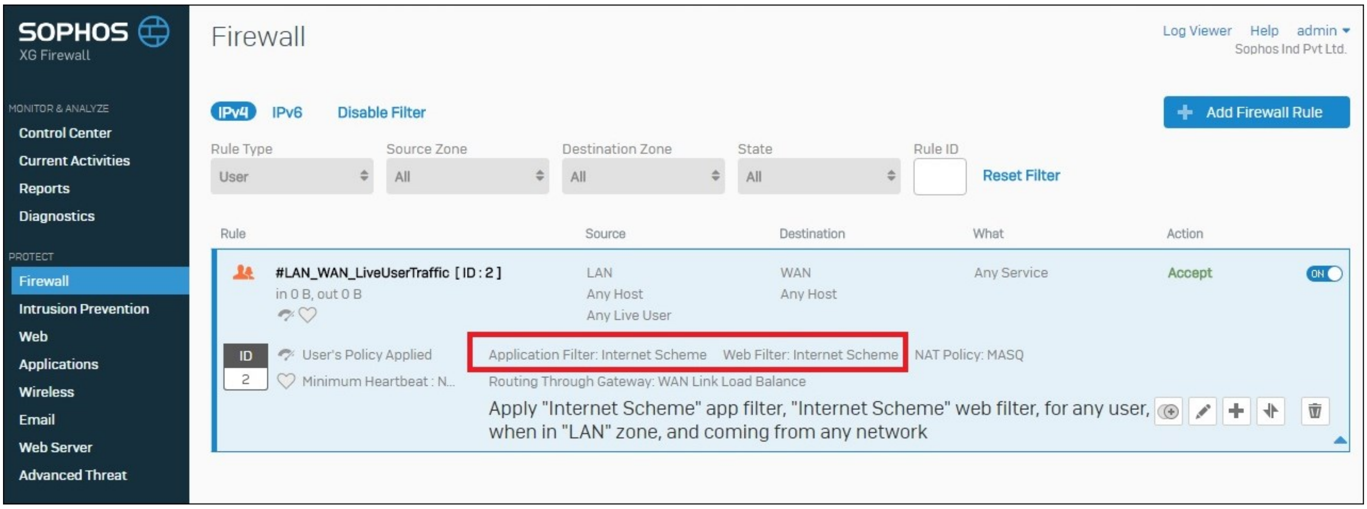
*The Internet Scheme page is displayed after migration from CR 10.6.3 MR4 to SF MR2. It displays the list of all users and groups affected by migrated firewall rules, listing out the corresponding web and app filter policies applied to them.

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.



	ID	Rule Name	Enable	Source	Destination	Service	Action	Identity	IM Scanning	Routing Through Gateway	Backup Gateway	WAF	Application Filter	Web Filter	Manage
⊟	LAN - WAN (Total 2)														
□	2	#LAN_WAN_LiveUserTraffic	ON	Any Host	Any Host	Any Service	Accept	Any Live User	●	Load Balance	None	●	User's Policy Applied	User's Policy Applied	
□	1	#LAN_WAN_AnyTraffic	ON	Any Host	Any Host	Any Service	Accept	-	●	Load Balance	None	●	Allow All	Allow All	

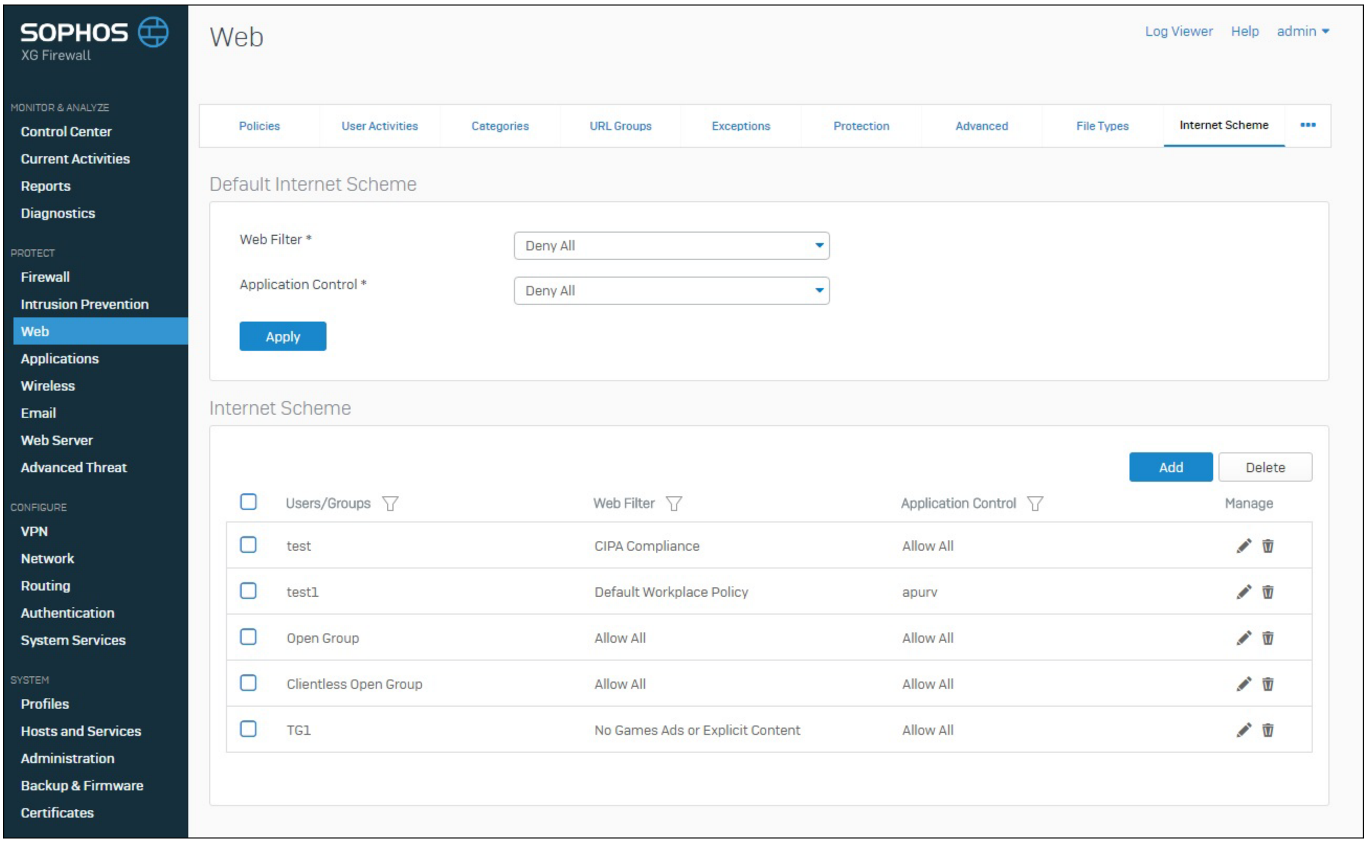


Rule Type: User
Source Zone: All
Destination Zone: All
State: All
Rule ID:

Rule	Source	Destination	What	Action
#LAN_WAN_LiveUserTraffic [ID : 2] in 0 B, out 0 B	LAN Any Host Any Live User	WAN Any Host	Any Service	Accept

ID 2
User's Policy Applied
Minimum Heartbeat : N...
Application Filter: Internet Scheme Web Filter: Internet Scheme NAT Policy: MASQ
Routing Through Gateway: WAN Link Load Balance
Apply "Internet Scheme" app filter, "Internet Scheme" web filter, for any user, when in "LAN" zone, and coming from any network

In the Internet Scheme* page in SF (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.



Web

Default Internet Scheme

Web Filter * Deny All

Application Control * Deny All

Internet Scheme

□	Users/Groups	Web Filter	Application Control	Manage
□	test	CIPA Compliance	Allow All	✎ 🗑
□	test1	Default Workplace Policy	apurv	✎ 🗑
□	Open Group	Allow All	Allow All	✎ 🗑
□	Clientless Open Group	Allow All	Allow All	✎ 🗑
□	TG1	No Games Ads or Explicit Content	Allow All	✎ 🗑

Behavior Difference

Once migrated, difference of behavior between Cyberoam Firewall Rules and SF 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, SF 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, SF will allow you to create custom IPS signatures, policies, etc. but will not scan or log traffic.

Similarly, if any license expires, SF 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 SF 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 WiFi 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 SF.

Web Application Firewall (WAF)

The WAF configuration of the Cyberoam Appliance will not be migrated to the SF Firmware. You will have to re-configure WAF-related policies in the SF 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 SF 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 SF.
- After migration, each agent will be bound to the SF Device through the appliance certificate and communication will take place over a secure channel. Hence, an agent authenticating to one SF Device cannot be bound to another SF Device.
- In SF, 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 SF 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 SF.
- 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 SF 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 SF 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, SF 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)
- File Type Exception configuration for Web Categories

Identity

For integration with an Active Directory (AD) Server, Integration Type ‘Loose Integration’ has been discontinued. By default, SF Device 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 SF. 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 SF. Existing Cyberoam HA setups will be migrated to SF with a unique random passphrase. You can check and update the HA configuration from **Configure > System Services > High Availability** in SF firmware.

Certificates

Cyberoam Certificates will be carried over to SF firmware with the following changes:

- All Self-signed Certificates and Certificate Authorities will be regenerated on migration. You will have to re-import the certificate for all services that use them.
- Cyberoam Self signed CA will be renamed to SecurityApplianceSelfSIgnedCA.
- 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.
- Behaviour 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 SF 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 SF 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 SF 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

SF 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 SF, 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 SF Migration

1. The SF Admin Console cannot be accessed via HTTP.
    a. In SF, HTTP setting has been removed from the Device Access page.
    b. If HTTP access was enabled before migration, 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 migration, the HTTP admin port settings will be removed.
2. SF cannot be accessed over TELNET.
    a. If Telnet access was enabled before migration, 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. Will not support AV Scanning on Virtual Host without active Webserver Protection (WAF) subscription.
6. SF 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 migration. 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 SF, admin needs an active Web Server Protection subscription for AV scanning of Web Servers.

Renamed CR Features

19. 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.
20. QoS is renamed to Traffic Shaping.
21. Network > Gateway is renamed to WAN Link Manager.
22. Parent Proxy is renamed to Upstream Proxy.
23. Appliance Access is renamed to Device Access.
24. 4-eye Authentication is renamed to Data Anonymization.
25. Data Transfer Policies is renamed to Network Traffic Quota.
26. Country Host Group is renamed to Country Group.
27. Wireless WAN is renamed to Cellular WAN.
28. In Web > Protection, Deny Unknown Protocols is renamed to Block unrecognized SSL protocols.
29. In Web > Protection, Allow Invalid Certificates is renamed to Block invalid certificates (behaviour is changed as the name suggests)