

Protect your Sophos XG Firewall Best Practice



Table of Contents

Foreword.....	3
Document scope	3
Understanding Firewall Attack – the Cybersecurity Kill Chain	4
Understanding how a stereotypical external attack develops.....	4
1. Reconnaissance.....	4
2. Weaponization	4
3. Delivery	4
4. Exploitation.....	5
5. Installation	5
6. Command & Control	5
7. Actions & Objectives.....	5
Firewall Security 101 – The basics.....	6
Access Control, Passwords and Account Management.....	6
1. Restrict Local Service Access Control.....	7
2. Get your firewall and NAT rules in order	8
3. Tune your Intrusion Prevention.....	9
4. Enable and tune DoS and DDoS protection	12
5. Changing the Admin Password and Secure SSH CLI access with Public Key authentication.....	16
6. Changing Password Complexity rules and Login parameters	18
7. Configure Two- Factor authentication.....	19
8. Adopt and Apply Role-Based Administration.....	20
Security Maintenance & Housekeeping.....	23
Enable Firewall System Notifications.....	23
Develop a change and patch management policy.....	25
1. Hardware and Firmware Lifecycle policy	25
2. Allow automatic installation of Hotfixes	25
3. License Management.....	25
4. Create and implement a Sophos XG Firewall Backup policy	26
Outsource your firewall management.....	26

Foreword

Document scope

The focus of this document is to provide baseline guidance to secure the Sophos XG Firewall to a minimum level. The document will not provide guidance on each XG firewall feature that may, in turn, secure internal network devices and resources (a full, exhaustive Sophos XG Firewall best practice guide will be published in due course). This guide will not include advice and guidance on the following topics and are considered to be out of scope:

- Outsourcing management
- Legal Regulations
- Local/Regional of corporate requirements
- Business Continuity
- Disaster Recovery planning
- Network Security Architecture & Design
- Risk Management
- Information Security Governance

One size does not fit all, some security recommendations will apply to a customer where others will not. Sophos and our partners, provide award-winning Professional Services who are happy to provide best practice network security design, implementation, and training tailored to the needs of our customers.

While Sophos XG firewall is one of the most sophisticated, multilayered, leading-edge security appliances in use today, it is, as with most firewalls, not effective right out of the box. Administrators often concentrate efforts on configuring firewall features and functions to protect internal networks and resources, before securing the firewall itself.

Understanding Firewall Attack – the Cybersecurity Kill Chain

Understanding how a stereotypical external attack develops

While some administrators would appreciate a step by step guide and the associated checklist of actions to secure a firewall from the beginning, we must understand why we investing time in this process.

Hackers generally attack a firewall in seven distinct phases:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions and Objectives

Let's look at these stages in a little more detail and add some context.



1. Reconnaissance

During the reconnaissance phase, the attacker gathers information on the target before the actual attack is commenced. Information can be gathered via websites, social media, phishing calls, phishing emails to name but a few. Here, it is often the human rather than the technology that is the weakest link, where user education is paramount. Sophos provides staff training tools such as Sophos Phish Threat to assist an organization in the training of staff to identify phishing emails and raise general security awareness.

2. Weaponization

Weaponization refers to the attack creation rather than execution. For example, an attacker may choose to create a Phishing email containing a PDF document, or perhaps create a new strain of ransomware to be distributed by dropping memory sticks in a corporate car park.

3. Delivery

Now that the hacker has established his/her target, the delivery phase deals with the transmission of the attack. For example, this activity would include sending the Phishing email or physically delivering the memory sticks to a corporate car park.

While people aren't proficient at remembering lots of new information, they are very good at being adaptable. They generally follow that "this does just not seem right" instinct. As such, it is people and not technology that is the first

line of defense in detecting and stopping many of these attacks, to include new or custom attacks such as CEO Fraud or Spear Phishing. Also, people can identify and stop attacks that most technologies cannot even filter, such as attacks over the phone. A trained workforce greatly reduces this attack surface area.

4. Exploitation

This implies actual ‘detonation’ of the attack, such as the exploit running on the system. A trained, security-aware workforce will ensure the systems they are running are updated and current. They ensure they have endpoint protection running and enabled. They ensure that any sensitive data they are working with is on secured systems, making them far more secure against exploitation.

5. Installation

The attacker installs malware on the victim. Not all attacks require malware, such as a CFO fraud attack or harvesting login credentials. However, just like exploitation when malware is involved, a trained and secure workforce can help ensure they are using secure devices that are updated, current, and have endpoint protection enabled, which would stop many malware installation attempts. This is where we begin to go beyond just the “human firewall” and leverage the “human sensor”. A key step in detecting an infected system is to look for abnormal behavior. Who better to detect abnormal behavior than the people using the system every day? Once again Sophos help customers thwart this phase by providing AI or “Machine Learning” tools such as Intercept-X to assist the human in the identification of abnormal behavior.

6. Command & Control

This implies that once a system is compromised and/or infected, the system has to call home to a Command and Control (C&C) system for the cyber attacker to gain control. They’re looking for abnormal outbound activities like this. Sophos Firewall Advanced Threat Protection features are particularly adept at discovering C&C activity and block such traffic.

7. Actions & Objectives

Once the cyber attacker establishes access to the organization, they can then execute actions to achieve their objectives. Motivations vary greatly depending on the threat actor. It may include political, financial, or military gain, so it is very difficult to define what those actions will be.

Once again, this is where a trained workforce of human sensors embedded throughout your organization can vastly improve your ability to detect and respond to an incident, vastly improving your resilience capabilities.

Firewall Security 101 – The basics

Access Control, Passwords and Account Management

Define and adopt a firewall access control and password policy. The access control and password policy should include:

1. Local Service Access Control Definitions/requirements
2. Policy on Password change frequency
3. Policy on Password Complexity rules and Login security parameters
4. Policy for Two Factor authentication
5. Policy on Public Key authentication to secure SSH access (if remote SSH is necessary)
6. Policy on Role-based administration

Administrative access to the Sophos XG firewall should be restricted. Administrators should only allow Webadmin, User Portal, Captive Portal, and SSH access from trusted internal networks or better still trusted, and defined hosts. Where access is required and granted, role-based access should be considered to protect from internal malicious and (more likely) accidental misconfiguration of the firewall.

To remove services from public access (and attacker view) on specific firewall 'Zones', navigate to **System -> Administration** and select the **Device Access** tab:



Tip: Before making any change to your Sophos XG Firewall, it is good practice to back up the current configuration before any change in case of misconfiguration.

1. Restrict Local Service Access Control

The screenshot shows the 'Administration' page for a Sophos XG Firewall. The 'Device access' tab is selected. Under 'Local service ACL', a table lists services for various zones. The WAN zone row is highlighted with a red box, indicating that all services are disabled for this zone. The 'Apply' button is also highlighted with a red box.

Zone	Admin services		Authentication services				Network services			Other services						
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Client Authentication	Chromebook SSO	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
VPN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
WiFi	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Turning off access to captive portal stops user notifications from appearing. Example: Web filter and Sandstorm notification pages

Local service ACL exception rule

Rule name IP version Manage

No records found

Where possible, remove ALL services from the WAN and other custom ‘External’ zones.

Tip: Some firewalls are located in secure areas and external datacentres. Should the firewall not be reachable from a trusted source, administrators should avoid opening up direct device access (Webadmin, SSH, etc) on untrusted, external interfaces. To do so would not only identify the device to the attacker but invite a myriad of attacks including brute force passwords and DoS attacks. In such environments, it is far better to manage the firewall via Sophos Central. However, if managing the Sophos XG firewall from Sophos Central, ensure you enable two-factor authentication within Sophos Central.


Note: Where Sophos Central is not utilized, and external firewall management is required, consider managing the firewall via an alternative secure connection e.g. IPSec or SSL remote access VPN.

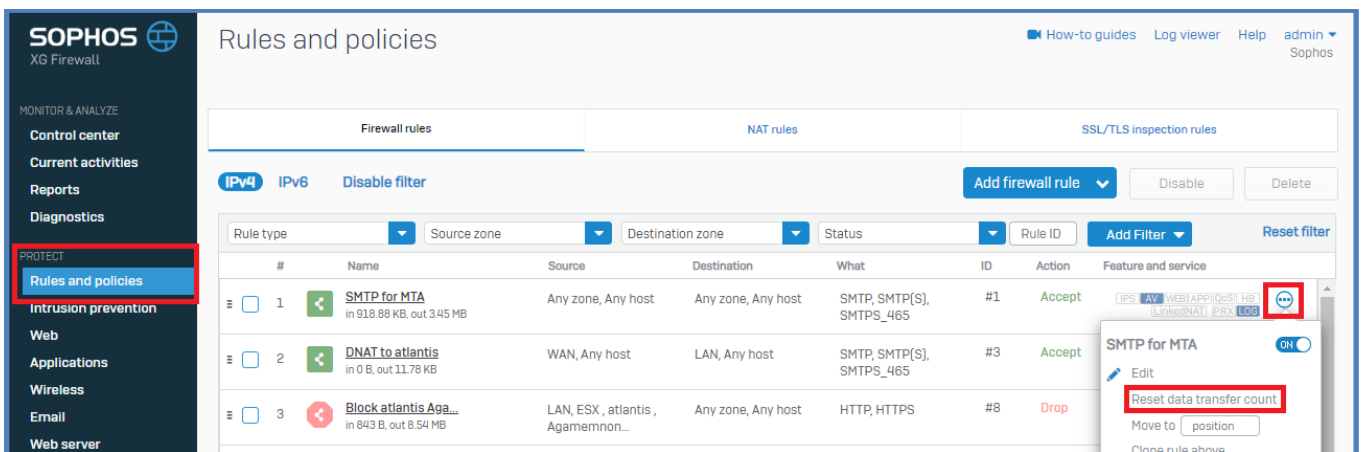
2. Get your firewall and NAT rules in order

Once again, the purpose of this guide is to provide practical best practice guidance to secure your XG firewall, before attempting to use the firewall to protect internal network nodes/resources. Firewall rules can be utilized to aid the security of the firewall itself and thwart additional attack vectors.

Sophos recommends that administrators check the following firewall rule best practice criteria and modify it as appropriate to your firewall environment.


- Ensure that your firewall rules are ordered correctly. Firewall rules are matched from the top down, and as a rule of thumb, more specific rules will precede general rules.
- Audit your firewall rules regularly:
 - Ensure unused rules are deleted and remove redundant host definitions.

 **Tip:** Reset your data transfer count periodically, any unused rule will then be easily identifiable. Rules that should be required, yet do not show use, may indicate a higher firewall rule match.




#	Name	Source	Destination	What	ID	Action	Feature and service
1	SMTP for MTA in 918.88 KB, out 3.45 MB	Any zone, Any host	Any zone, Any host	SMTP, SMTP(S), SMTPS_465	#1	Accept	IPS, AV, WEB, APP, QoS, S, H, U, W, NAT, PRX, LOG
2	DNAT to atlantis in 0 B, out 11.78 KB	WAN, Any host	LAN, Any host	SMTP, SMTP(S), SMTPS_465	#3	Accept	
3	Block atlantis Aga... in 843 B, out 8.54 MB	LAN, ESX, atlantis, Agamemnon...	Any zone, Any host	HTTP, HTTPS	#8	Drop	

- Where possible, ensure firewall rule traffic is logged

 **TIP:** In addition to local log storage, Logs should be saved to an external destination such as a Syslog Server or Sophos Central for the preservation of data for Incident Response (IR), audit, and in case of hardware failure.

- Customize your IPS (Refer to section 3) and apply the IPS policy to your firewall rules.
- Reduce the threat landscape - Create a firewall rule to block countries of origin.

 **Note:** Although useful within localized organizations, customers that communicate/trade across the globe will not be able to utilize GeoIP filtering effectively. Customers should also note that hackers may utilize local country 'Pivot points' to launch attacks, therefore GeoIP filtering should be considered as an aid to security and not relied upon.

- If appropriate, ensure a firewall rule is created to restrict DNS, allowing DNS queries to sanctioned servers and sanctioned hosts only to prevent phishing/DNS poisoning attacks and ensure correct DNS resolution.
- Create your firewall rules with as much granularity as possible. E.g. refrain from creating rules that allow traffic from an entire zone or network where a specific host could be defined.

- Group firewall rules from WAN to LAN and LAN to WAN. Organizing rules in this way simplifies administration and minimizes human error.
- Pay attention to WAN to LAN rules:
 - Make sure the rule is necessary – what specific business function does it serve? Can this function be achieved through another mechanism?
 - Reverse Proxy traffic from WAN to DMZ instead of NAT'ing traffic to specific internal hosts



Tip: NAT'ing traffic to specific hosts may allow administrators to analyze traffic via IPS rules as well as Anti-Virus scanning, but traffic analysis will not be as comprehensive as running traffic via a reverse proxy's MOD Security rules. In addition to normal checks, Reverse Proxies may guard against Cross-Site Scripting (XSS), SQL Injection as well as a myriad of other vulnerabilities.

3. Tune your Intrusion Prevention

IPS can consume a lot of the CPU if not properly configured. You will need to find a balance between an acceptable performance level and the security posture of your organization. In this area, you are the expert in what that balance is. In general, the more secure the traffic inspection (the more IPS rules enabled and threats mitigated) the lower the performance. You will need to prioritize the protections that most directly improve your security posture based on the type of traffic and data in your environment.

IPS settings

The IPS settings are:

- **stream**
- **lowmem**
- **maxsesbytes**
- **maxpkts**

To view the status of the IPS settings:

Log in to the Command Line Interface (CLI) using Telnet or SSH. You can also access the CLI from admin > Console in the upper right corner of the Admin Console.

Select option 4. Device Console.

Enter the following command:

```
show ips-settings
```

```
console> show ips-settings
-----IPS Settings-----
    stream on
    lowmem off
    maxsesbytes 0
    maxpkts 8
    mmap off
    enable_appsignatures off
    http_response_scan_limit 65535

-----IPS Instances-----
IPS CPU
 1    0
 2    1
```

Stream (Reccomended = on)

If **stream** is set to **on**, the IPS engine builds an internal table during a session and deletes them at the end of each session. It also reassembles all incoming packets and checks the data for any known signatures. The IPS engine can also:

- Buffer the entire stream of packets inside a TCP session.
- Reassemble the TCP segments into a correct stream based on the sequence numbers.
- Check for overlapping packets along with duplicate segments and their checksums.
- Scan every packet with the IPS engine to identify the malicious or duplicate payload.

To turn on **stream**, enter the command:

```
set ips packet-streaming on
```

If **stream** is set to **off**, then protocols such as Telnet, POP3, SMTP, and HTTP are vulnerable as reassembly of packets or segments can no longer occur. Data is sometimes broken up into chunks of packets and must be reassembled to check for signatures, these protocols are now vulnerable to malicious files that are hidden by splitting. There are no specific parameters for IPS calibration and the settings for **maxpkts** and **stream** will be different from case to case based on the:

- Deployment type and size.
- The number of signatures being used.
- Network traffic being generated.
- Bandwidth provided by the ISP.

To turn off **stream**, enter the command:

```
set ips packet-streaming off
```

lowmem (Recommended = ??)

If **lowmem** is set to **on**, the appliance stores signatures in a compressed format. When matching signatures, the appliance has to decompress that data and consumes more processing power.

To turn on **lowmem**, enter the command:
set ips lowmem-settings on

If **lowmem** is set to **off**, the signatures will take up more storage space, but signature matching will consume less processing power.

To turn off **lowmem**, enter the command:
set ips lowmem-settings off

Maxsesbytes (Recommended = ??)

maxsesbytes is the number of bytes checked per session of data packets. The default setting (**0**) means the device will check all the data in the session, which consumes more processing power.

The recommended setting is **0**. Changing maxsesbytes it to a limited value can lower the amount of processing power used but will reduce the detection capabilities of the IPS.

To set the number of bytes checked, enter the command:
set ips maxsesbytes-settings update <any *number* or *0* to check all the data>

maxpkts (Recommended = ??)

maxpkts is the number of packets checked for signatures inbound and outbound. The default setting of **8** means it will check a total of 16 packets, 8 on each side, which consumes a low amount of processing power.

The recommended setting is between **100** and **300**, depending on the amount of processing power you have available. This setting covers 98% of all applications except for file transfer programs. If IPS checks all incoming packets, all unclassified packets are submitted to IPS, which can consume a lot of processing power.

To set the number of packets checked on both sides, enter the command:

Set ips maxpkts <any *number* or *all*>

4. Enable and tune DoS and DDoS protection

A Denial of Service (DoS) attack is an attempt to make a machine or network resource unavailable to the intended users. This type of attack involves saturating the target machine with external communications requests so that it cannot respond to legitimate traffic or the machine responds so slowly that it is essentially useless.

Common DoS Attacks are:

- **ICMP Flood:** In this method, the perpetrators send large numbers of IP packets with the source addresses appearing as the address of the victim. The network's bandwidth is quickly used up and prevents legitimate packets from getting through to their destination.
- **SYN/TCP Flood:** A SYN flood is when a host sends a flood of TCP/SYN packets, often with a forged sender address. Every packet is handled like a connection request; this causes the server to spawn a half-open connection because it sends back a TCP/SYN-ACK packet (Acknowledge) and waits for a packet in response from the sender address (the response to the ACK Packet). However, as the sender address is forged, the response never comes (the host that legitimately has the forged address ignores the packet because it didn't send the request. These half-open connections occupy the number of available connections the firewall can make and keep it from responding to legitimate requests until after the attack ends.
- **UDP Flood:** A UDP flood attack can be initiated by sending many UDP packets to random ports on a remote host. For many UDP packets, the victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients.

Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is the attack where multiple (legitimate or compromised) systems perform a DoS Attack on a single target or system. This distributed attack can compromise the targeted machine or force it to shutdown, which shuts down service to the legitimate users.

Protecting your network from a DoS attack

You can protect your network against DoS attacks for both IPv4 and IPv6 traffic by configuring the appropriate DoS Settings on the Sophos XG Firewall. You can configure DoS Settings by following the steps below:

1. Navigate to **Intrusion Prevention > DoS & Spoof Protection**.
2. Set the Packet and Burst rates under **DoS Settings** section according to your network traffic and check the **Apply Flag** next to the parameter to enable scanning for the respective type of traffic.
- As an example, we have set **Packet rate per Source (Packet/min)** as **1200** for **ICMP/ICMPv6 Flood** and checked the **Apply Flag** next to it to enable scanning for ICMP and ICMPv6 traffic.

The screenshot displays the 'Intrusion Prevention' configuration page, specifically the 'DoS & Spoof Protection' section. The 'DoS Settings' table is as follows:

Attack Type	Source				Destination			
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)	Apply Flag	Source Traffic Dropped	Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)	Apply Flag	Destination Traffic Dropped
SYN Flood	12000	100	<input type="checkbox"/>	0	12000	100	<input type="checkbox"/>	0
UDP Flood	12000	100	<input type="checkbox"/>	0	18000	100	<input type="checkbox"/>	0
TCP Flood	12000	100	<input type="checkbox"/>	0	12000	100	<input type="checkbox"/>	0
ICMP/ICMPv6 Flood	1200	100	<input checked="" type="checkbox"/>	0	300	100	<input type="checkbox"/>	0
Dropped Source Routed Packets	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
Disable ICMP/ICMPv6 Redirect Packet	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
ARP Hardening	-	-	-	-	-	-	<input type="checkbox"/>	-

An 'Apply' button is located at the bottom left of the table area. A link 'Click Here for DoS Attacks status' is located at the bottom right.

3. Click **Apply** to apply the configured DoS Settings.

Once DoS settings are applied, SF checks the network traffic to ensure that it does not exceed the configured limit.

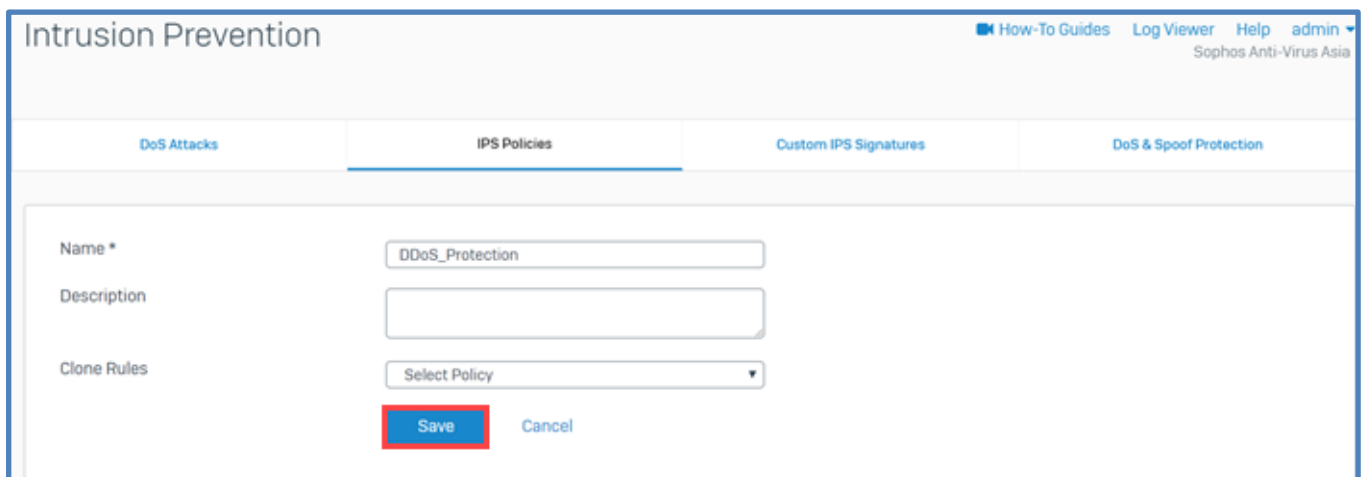
- For example, once the settings above are applied, SF scans the network traffic for ICMP and ICMPv6 packets. If the number of ICMP/ICMPv6 packets from a particular source exceeds 1200 per minute, it drops the excessive packets and continues dropping until the attack is over.

Protecting your network from a DDoS Attack

This type of attack is harder to protect against because there isn't a single host that can be blocked – usually, the firewall will get far few packets from each host but have far more hosts sending packets. This means that no specific host will trigger the threshold defined in the previous section but the total real number of incoming packets if the same or more.

You can protect your network against DDoS attacks by using **Intrusion Prevention** policies in SF. Please note that the DDoS signatures are only available on the XG550, XG650, and XG750 models. To configure an IPS policy, follow the steps below.


1. Navigate to **Intrusion Prevention > IPS Policies**.
2. Click **Add** to create a new Intrusion Prevention policy named **DDoS_Protection**.



The screenshot shows the 'Intrusion Prevention' configuration page in the Sophos Firewall management console. The 'IPS Policies' tab is active. The form contains the following fields:

- Name ***: A text input field containing 'DDoS_Protection'.
- Description**: An empty text input field.
- Clone Rules**: A dropdown menu with 'Select Policy' selected.

At the bottom of the form, there are two buttons: 'Save' (highlighted with a red box) and 'Cancel'.

3. Click **Save**.
4. Click on the  icon for the **DDoS_Protection** policy.
5. Click on **Add** to create a new rule named **DDoS_Signatures**.
6. In the **Smart Filter** field, type "DDoS" (without the quotes) and then press enter.
7. Set the **Action** to **Drop Packet**.

Intrusion Prevention How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

DoS Attacks **IPS Policies** Custom IPS Signatures DoS & Spoof Protection

Add IPS Policy Rules

Rule Name *

Category Severity Platform Target Clear Filter

Smart Filter: ddos ✕

Select All Select Individual Signature

<input type="checkbox"/>	Name	SID	Category	Severity	Platform	Target	Recommended Action
<input checked="" type="checkbox"/>	DNS isc.org DDoS	1604117	DNS	2 - Major	Windows	Server	Drop Packet
<input checked="" type="checkbox"/>	Incoming LOIC DDOS Tool	1100012	Misc	2 - Major	Windows	Server	Drop Packet
<input checked="" type="checkbox"/>	Malware Hidden Cobra Botnet DDoS Handshake Success	3310108	Malware Communication	1 - Critical	Windows	Client	Drop Packet
<input checked="" type="checkbox"/>	Outgoing LOIC Tool Participating in DDOS	1100011	Misc	2 - Major	Windows	Server	Drop Packet
<input checked="" type="checkbox"/>	Outgoing LOIC Tool Participating in DDOS	1100013	Misc	2 - Major	Windows	Server	Drop Packet

List of Matching Signatures [1 - 5 of 5]

Action

Save Cancel

8. Click on **Save** and then click on **Save** again to save the policy.
9. Navigate to **Firewall** and apply the Intrusion Prevention policy to the **User/Network Rule**.

Edit User/Network Rule How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Advanced

User Applications

Intrusion Prevention

Traffic Shaping Policy

Web Policy

Apply Web Category based Traffic Shaping Policy

Application Control

Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

GREEN YELLOW No Restriction

Block clients with no heartbeat

Minimum Destination HB Permitted:

GREEN YELLOW No Restriction

Block request to destination with no heartbeat

NAT & Routing

Rewrite source address [Masquerading]

Primary Gateway

Backup Gateway

DSCP Marking

5. Changing the Admin Password and Secure SSH CLI access with Public Key authentication


ALWAYS CHANGE THE DEFAULT ADMINISTRATOR PASSWORD BEFORE DEPLOYING A FIREWALL TO PRODUCTION!


There are several ways to change the Sophos Admin password:

Via the Webadmin Console

1. Navigate to **Administration > Device Access > Default admin password settings**
2. Change the password
3. Click **Apply**

The screenshot shows the Sophos XG Firewall Administration console. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Administration' menu item is highlighted. The main content area shows the 'Administration' page with the 'Device access' tab selected. Below the tabs, there is an 'Apply' button. The 'Local service ACL exception rule' section is empty. The 'Default admin password settings' section shows the 'User name' as 'admin' and three password input fields: 'Current password *', 'New password *', and 'Confirm Password'. An 'Apply' button is highlighted. The 'Public key authentication for admin' section shows the 'Enable authentication' toggle set to 'OFF', which is highlighted. Below it is an 'Authorized keys' section with a search/add input field. An 'Apply' button is highlighted at the bottom of this section.

 **Tip:** Turn on **Public key authentication for admin** to allow access to the command-line interface (CLI) using the SSH key.

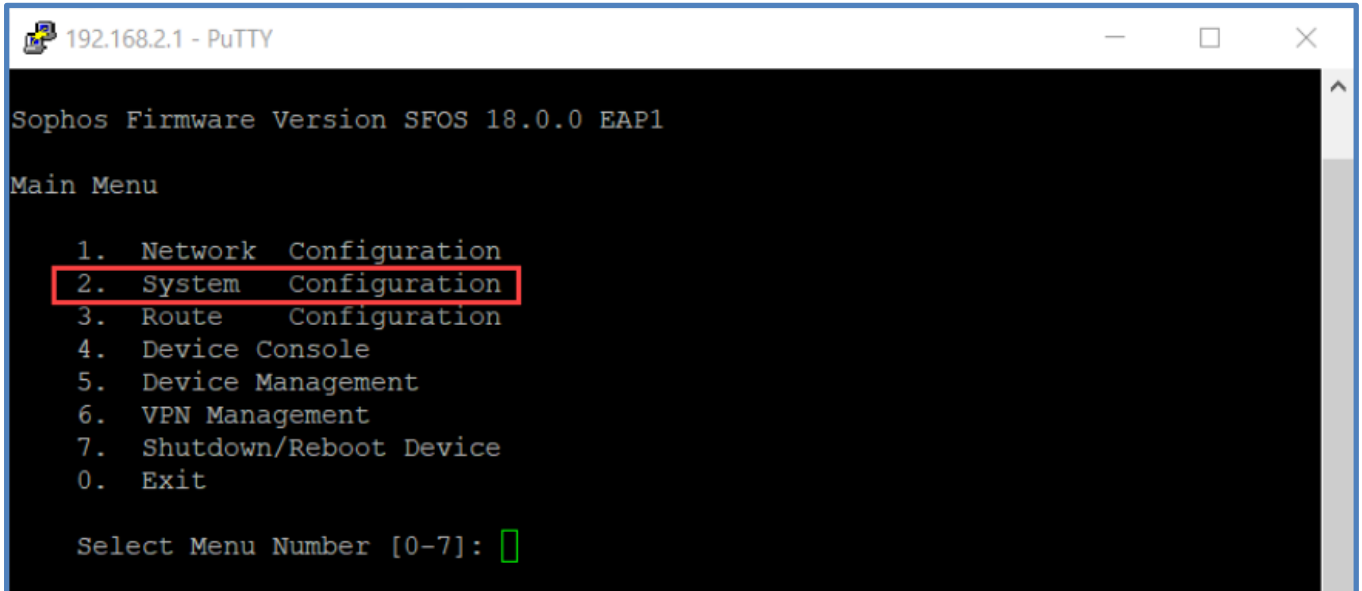
 **Note:** Only admin and support users can add an SSH sign-in key without authentication. All other users are required to provide a password for authentication before adding an SSH key.

Systems should not be accessed via shared accounts. Ideally, an individual's usernames should match the username of their corporate identity e.g. first name.surname.

Add the list of **Authorized keys for admin**. SSH keys may be generated using SSH client tools (example: PuTTY).

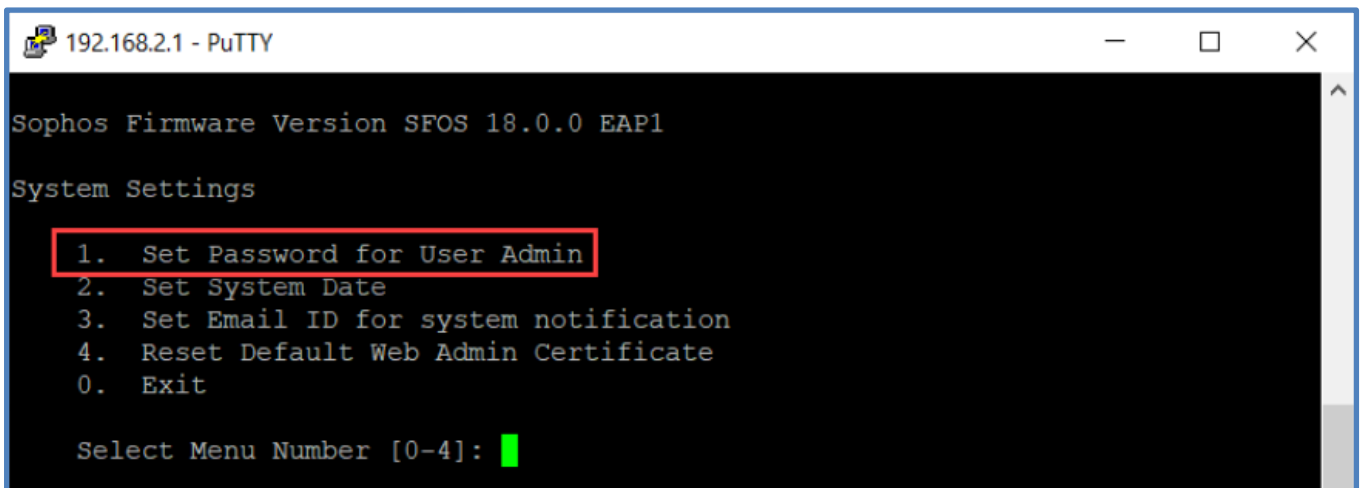
Via Console

1. Sign in to the command-line interface (CLI) and choose option **2. System Configuration**



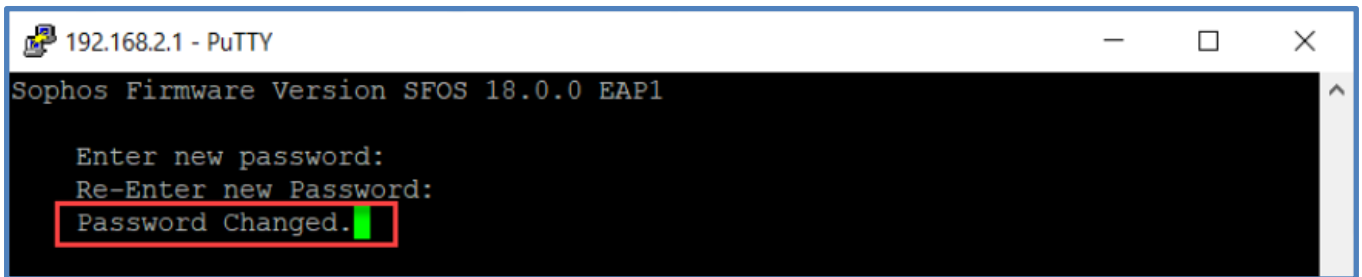
```
192.168.2.1 - PuTTY
Sophos Firmware Version SFOS 18.0.0 EAP1
Main Menu
1. Network Configuration
2. System Configuration
3. Route Configuration
4. Device Console
5. Device Management
6. VPN Management
7. Shutdown/Reboot Device
0. Exit
Select Menu Number [0-7]:
```

2. Then choose option **1. Set Password for User Admin**.



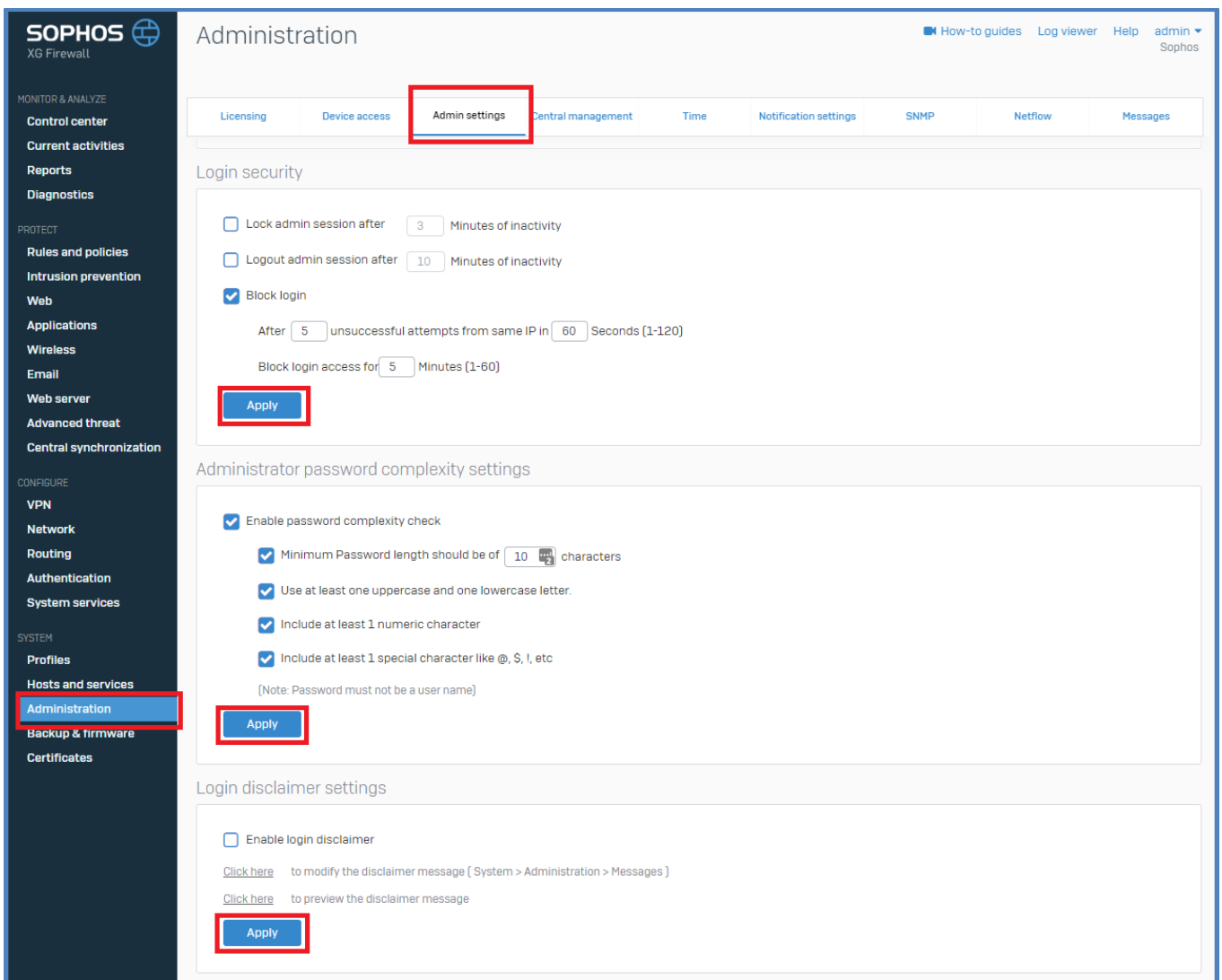
```
192.168.2.1 - PuTTY
Sophos Firmware Version SFOS 18.0.0 EAP1
System Settings
1. Set Password for User Admin
2. Set System Date
3. Set Email ID for system notification
4. Reset Default Web Admin Certificate
0. Exit
Select Menu Number [0-4]:
```


3. Set the new password, re-enter the new password, and hit Enter.



6. Changing Password Complexity rules and Login parameters

To change password complexity rules and login parameters, navigate to **Administration**, and select the **Admin Settings** tab:



 **Tip:** While this is not a security-related feature, while we are here, why not enable your Login Disclaimer. In some countries, it is not illegal to carry out a Brute Force password attack – without a disclaimer!

7. Configure Two- Factor authentication

Now that we have restricted access to trusted devices and firewall zones, administrators should consider implementing two-factor authentication. Two-factor authentication (2FA) is an effective – and increasingly important – weapon in the IT manager’s armory.

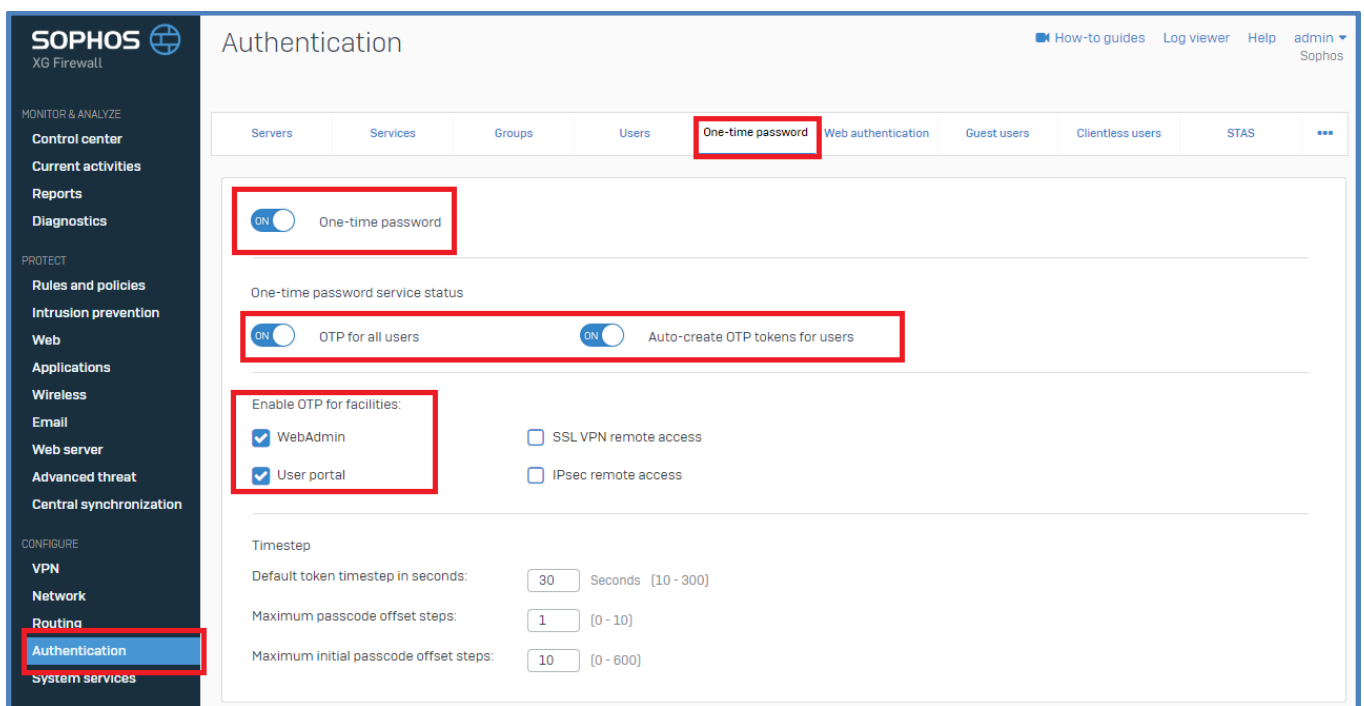
2FA delivers an extra layer of protection for user accounts that, while not fool-proof, significantly decreases the risk of unauthorized access and system breaches.

You can implement two-factor authentication using one-time passwords, also known as passcodes. Passcodes are generated by Sophos Authenticator on a mobile device or tablet without the need for an internet connection. When users log on, they must provide a password and a passcode. Alternatively, administrators may choose to deploy hardware ‘RSA’ style tokens to the user base.

You can configure two-factor authentication using the one-time password (OTP) service. First, turn on the OTP service. You should then specify the features for which two-factor authentication is required.

The following steps are executed on the firewall.

Navigate to **Authentication** and select the **One-time password** tab. Now select the **Settings** button and specify the settings:



Do not forget to click the apply button at the foot of the screen.

8. Adopt and Apply Role-Based Administration

As approximately 70% of all network attacks are instigated within the organization, granular Role-based administration is an often overlooked tool in the I.T. Security realm. Role-based access control:

- Aides forensic investigation
 - (a company auditor with read-only rights investigating an employee cannot be accused of tampering with firewall database data or logs).
- Reduces risk of accidental configuration mistakes
- Reduces the risk of malicious activity
- Promotes granular auditing, accountability, and transparency
- Allows administrators to remove access to an individual without impacting other trusted users

Sophos Firewall gives administrators the ability to configure sub-admin accounts that cannot access certain areas and have read or read/write access in others.

To establish role-based administration, understand the XG firewall user rights assignments against your user access requirements. Then choose an appropriate predefined role for each user, or perhaps create a custom role if required. Sophos recommends that you follow the policy of Least Privilege where a user is only given exactly the access rights they need to do their functions and no more. Define what each user needs to do and then assign the role that meets all job requirements. If there is no pre-defined role that matches – you will have to create a custom one.

Protect your Sophos XG Firewall – Best Practice

To Create a custom administration role, Navigate to **Profiles > Device Access**, before clicking **Add**. Give a name to the new Role-based on the function. There are several accounts predefined roles such as Audit Admin or Crypto Admin.

Select either **None**, **Read-Only**, or **Read-Write**. You can set this for all categories or individually. Click **Save** to create the role.

Profiles

Log Viewer Help admin Sophos

Schedule Access Time Surfing Quota Network Traffic Quota Network Address Translation **Device Access**

Add Profile

Profile Name *

Configuration	<input type="radio"/> None	<input type="radio"/> Read-Only	<input type="radio"/> Read-Write
Control Center	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Initial Setup	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
+ System	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Objects	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Network	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
+ Wireless Protection	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
+ Identity	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Security Policy	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
+ VPN	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
IPS	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Web & Content Filter	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Application Filter	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Sandstorm Activity	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
+ WAF	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Traffic Shaping	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Email Protection	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Traffic Discovery	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
+ Logs & Reports	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

To add a user to the new role, navigate to **Authentication > Users** before clicking **Add**. Fill out the settings for the user as normal. Change **User Type** to **Administrator**, before selecting the user profile we have just created. Remember to **save** the settings.

The screenshot shows the 'Add User' configuration page in the Sophos XG Firewall management interface. The page is titled 'Authentication' and has a navigation bar with tabs for Servers, Services, Groups, Users, One-Time Password, Captive Portal, Guest Users, Clientless Users, and STAS. The 'Users' tab is selected. The 'Add User' form contains the following fields:

- Username *: TestUser
- Name *: Test User
- Description: Description
- Password *: Two password fields, both masked with dots.
- User Type *: Radio buttons for 'User' and 'Administrator'. The 'Administrator' option is selected.
- Profile *: WebFilterAdmin
- Email *: testuser@test Sophos.sophos.net

Below the form, there is a 'Policies' section with the following settings:

- Group *: Open Group
- Surfing Quota *: Unlimited Internet Access
- Access Time *: Allowed all the time
- Network Traffic: None
- Traffic Shaping: None

A red rectangular box highlights the 'User Type' and 'Profile' fields.

Security Maintenance & Housekeeping

Enable Firewall System Notifications

Sophos XG firewall can be configured to alert administrators of system-generated events. Administrators should review the list of events and ensure that key events are monitored to ensure that issues and events can be acted upon promptly. Sophos recommends that you adopt a regular triage and investigation routine to make sure that no events are missed or left to linger too long.

Notifications are sent via either an email and/or to SNMP traps. To configure Notifications, navigate to **Configure -> System services** and select the **Notifications list** tab.

The screenshot shows the Sophos XG Firewall web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'CONFIGURE' menu is expanded to show 'System services', which is selected. The main content area displays the 'Notification list' configuration page. At the top, there are tabs for 'High availability', 'Traffic shaping settings', 'RED', 'Malware protection', 'Log settings', 'Notification list', 'Data anonymization', 'Traffic shaping', and 'Services'. The 'Notification list' tab is active. Below the tabs, there is a 'General' section with two toggle switches: 'Email notifications' (ON) and 'SNMP traps' (OFF). Below this is a 'Notifications' section with an 'Expand all' link and a list of notification categories, each with a chevron icon and a count of notifications:

Category	Count
Admin	0 of 2
HA	0 of 2
IPS	0 of 5
ATP	0 of 2
Disk/Memory	0 of 3
Firmware	1 of 3
System	1 of 6
RED	0 of 2
AP	0 of 2
VPN	0 of 4
Virus	0 of 5

At the bottom of the page, there are 'Save' and 'Cancel' buttons.

Protect your Sophos XG Firewall – Best Practice

Where administrators utilize email as the notifications transmission media, notifications can be sent from either an in-built SMTP server or an external SMTP server. Notification SMTP server options are configured under **System -> Administration** selecting the **Notification settings** tab.

The screenshot displays the Sophos XG Firewall Administration interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Administration' menu item is highlighted. The main content area is titled 'Administration' and features a top navigation bar with tabs: Licensing, Device access, Admin settings, Central management, Time, Notification settings (selected), SMTP, Netflow, and Messages. Below the tabs, the 'Mail server settings' section includes a warning icon and a radio button selection for 'Send notifications via', with 'Built-in email server' selected. The 'Email settings' section contains three input fields: 'From email address *', 'Send notifications to email address *', and 'Management interface IP address' (set to 'None'). A 'Sent in email notifications' checkbox is also present. At the bottom, there are 'Apply' and 'Test mail' buttons.

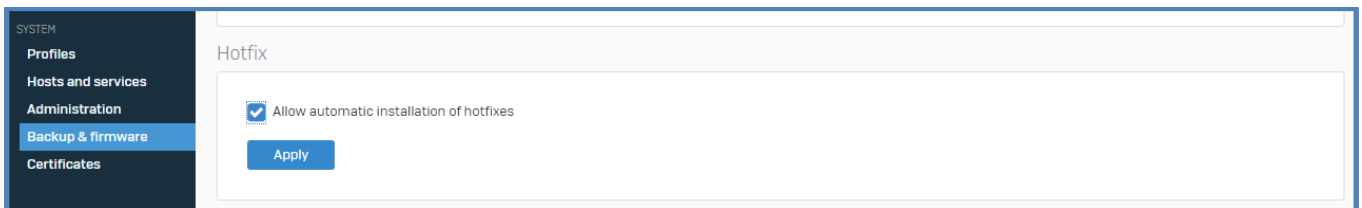
Develop a change and patch management policy

1. Hardware and Firmware Lifecycle policy

The administrator must be aware of Sophos Hardware and Software end of life policy. Administrators should ensure that systems are running on supported and maintained firmware revisions. Unsupported firmware revisions are unlikely to receive vital security patches and updates which, in turn, vastly diminishes the firewall's capabilities and effectiveness. The Sophos UTM and XG Firewall lifecycle policy can be found here: <https://www.sophos.com/en-us/support/technical-support/lifecycle-policy.aspx#XGFirewallSoftware>

2. Allow automatic installation of Hotfixes

Administrators should allow automatic installation of Hotfixes. This will allow Sophos to react quickly and remediate any zero-day threat with minimum delay. Administrators should note that although there is a slight risk in automatic hotfix installation, (Sophos cannot provide any guarantees against false positives or other issues), however, in our opinion, the risk of not updating firewalls promptly with urgent patches represents a far greater security risk. To enable automatic hotfix installation, navigate to **System -> Backup & firmware** before selecting the **Allow automatic installation of hotfixes** checkbox and clicking **Apply**.



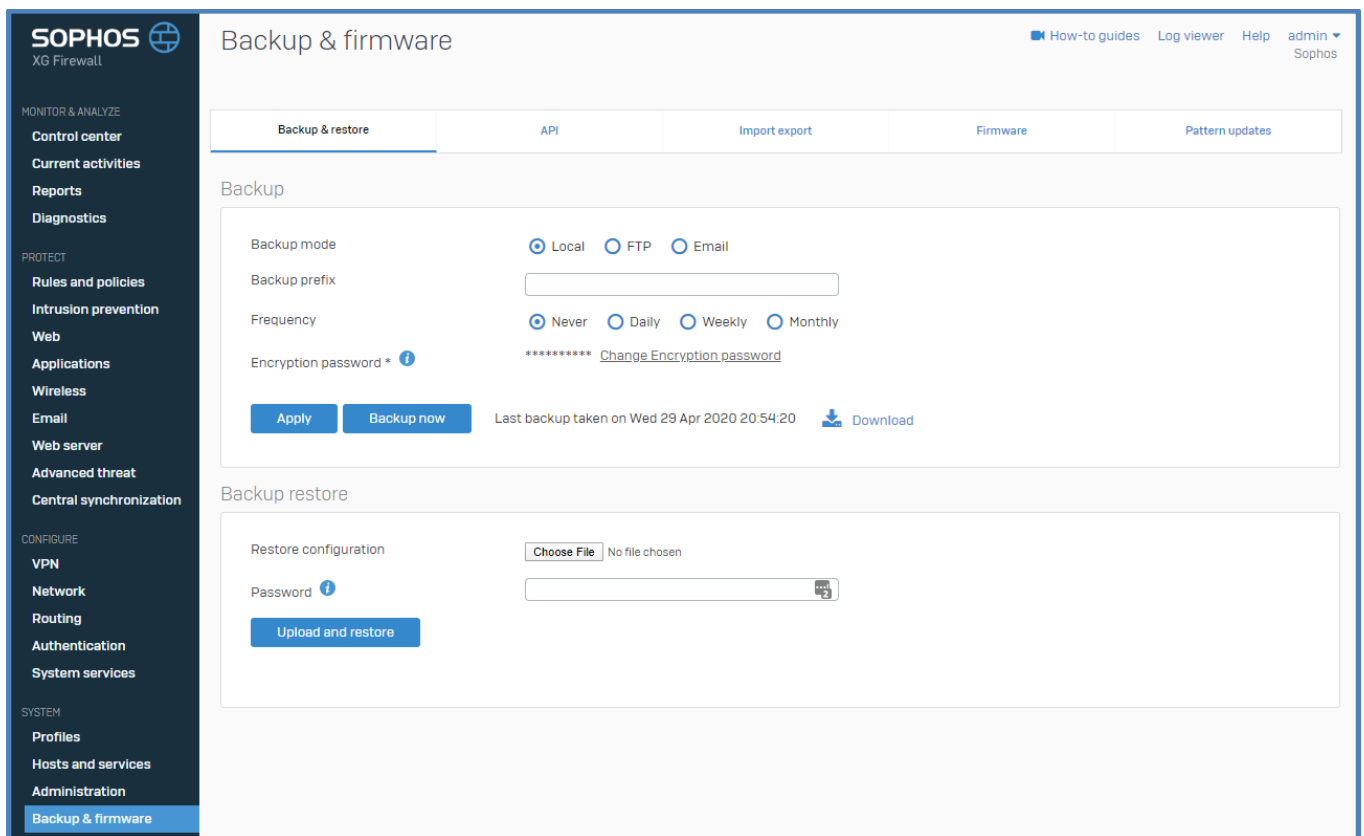
3. License Management

Administrators should ensure the firewall module licenses have not expired or about to expire. Unlicensed modules lead to critical components not functioning correctly and will not scan traffic for malicious activity. Stateful firewalling provides limited value.

4. Create and implement a Sophos XG Firewall Backup policy

By default, the Sophos XG firewall will create a backup through manual administrator intervention, stored locally. Sophos advises that backups are taken daily as well as before and after major configuration changes. All backups should be encrypted with a Preshared key as backup files contain operational keys which could compromise the security of the firewall should they fall into the wrong hands. In addition to locally saved backups, backups should be stored off-box to aid disaster recovery in case of complete system failure.

To configure scheduled backup frequency, backup file location, backup encryption key, and define backup transmission media, navigate to **System -> Backup & firmware** before selecting the **Backup & Restore** tab.



If you have configured Central management of your XG in Sophos Central, you can also enable and schedule backups here. More information on this can be found here <https://docs.sophos.com/central/Customer/help/en-us/central/Customer/concepts/FirewallBackup.html?hl=backup>

Outsource your firewall management

If your organization does not employ network security-centric personnel, consider outsourcing management of your firewall to a Sophos accredited Managed Service Provider (MSP).