CIS Benchmarks

CIS SOPHOS XG Firewall v18 Benchmark

v1.0.0 - 03-22-2021

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

This is the archive of the CIS SOPHOS XG Firewall v18 Benchmark v1.0.0. CIS encourages you to migrate to a more recent, supported version of this technology.

This document provides prescriptive guidance for establishing a secure configuration posture for SOPHOS XG Firewalls running SFOS version v18. This guide was tested against SFOS v18. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate SFOS v18 on a SOPHOS XG Firewall.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to: o be practical and prudent; o provide a clear security benefit; and o not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics: o are intended for environments or use cases where security is paramount o acts as a defense in depth measure o may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Wana Tun

Contributor
Darren Freidel
Wana Tun

Recommendations

1 Device Setup And Administration

The Device Setup section covers requirements for login banners, logging, management interfaces, password strength, device management authentication, SNMP polling, notifications and device services.

1.1 General Settings

The General settings section includes banner, device access profiles and logging settings.

1.1.1 Ensure admin session 'lock', 'logout' for inactivity and 'block' is configured for failed sign-in (Automated)

Profile Applicability:

- Level 1

Description:

Set to automatically lock the session after the configured time of inactivity (in minutes). This setting applies to the web admin and CLI console, the IPSec connection wizard, the network wizard, and the group import wizard. (Default: 3 minutes)

Set to automatically sign out the administrator from the web admin console after the configured time of inactivity. (Default: 10 minutes)

Set to block sign-in to the web admin console and CLI after the maximum numbers of failed sign-in attempts and the duration (in seconds) which attempts can be made from a single IP address.

Rationale:

An unattended computer with an open administrative session to the device could allow an unauthorized user access to the firewall's management interface. Thwart bruteforce attempts against login sessions to block multiple sign-in failures.

Audit:

```
Navigate to `System > Administration > Admin settings > Login security`.

Verify that `Lock admin session after _ Minutes of inactivity` is checked and
configured with no more than 3 minutes of default value.

Verify that `Logout admin session after _ Minutes of inactivity` is checked
and configured with no more than 10 minutes of default value.

Verify that `Block login` is checked.
```

Remediation:

```
Navigate to `System > Administration > Admin settings > Login security`.

Set `Lock admin session after _ Minutes of inactivity` is checked and
configured with no more than 3 minutes of default value.

Set `Logout admin session after _ Minutes of inactivity` is checked and
configured with no more than 10 minutes of default value.

Set `Block login` is checked.
```

Default Value:

Lock admin session after 3 minutes.

Log out admin session after 10 minutes.

References:

1. https://support.sophos.com/support/s/article/KB-000035727?language=en_US

CIS Controls:

Version 7

16.11 Lock Workstation Sessions After Inactivity
Automatically lock workstation sessions after a standard period of inactivity.

1.1.2 Ensure login disclaimer is set (Automated)

Profile Applicability:

- Level 1

Description:

Configure a login disclaimer, ideally approved by the organization's legal team. This banner should at minimum prohibit unauthorized access, provide notice of logging or monitoring, and avoid using the word "welcome" or similar words of invitation.

Rationale:

Through a properly stated login banner, the risk of unintentional access to the device by unauthorized users is reduced. Should legal action take place against a person accessing the device without authorization, the login banner greatly diminishes a defendant's claim of ignorance.

Audit:

```
Navigate to `System > Administration > Admin Settings > Login Disclaimer
Settings`.
Verify `Enable login disclaimer` is checked and disclaimer message is set
appropriately.
```

Remediation:

```
Navigate to `System > Administration > Admin Settings > Login Disclaimer
Settings`.
`Enable login disclaimer` is checked and set the disclaimer message
appropriately.
```

Default Value:

Not Configured

References:

1. https://community.sophos.com/kb/en-us/123142

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

1.1.3 Ensure NTP servers are configured appropriately (Automated)

Profile Applicability:

- Level 1

Description:

Synchronize the clock on XG firewall with NTP servers.

Rationale:

NTP enables the device to maintain an accurate time and date when receiving updates from a reliable NTP server. Accurate timestamps are critical when correlating events with other systems, troubleshooting, or performing investigative work. Logs and certain cryptographic functions, such as those utilizing certificates, rely on accurate time and date parameters. In addition, rules referencing a Schedule object will not function as intended if the device's time and date are incorrect.

Audit:

```
Navigate to `System > Administration > Time`.

Verify that `Time Zone` is set correctly.

Verify that `Use pre-defined NTP Server` Or `Use custom NTP Server` is
checked and synchronize the device's clock.
```

Remediation:

```
Navigate to `System > Administration > Time`.

Set `Time Zone` correctly.

Set `Use pre-defined NTP Server` Or `Use custom NTP Server` is checked and
synchronize the device's clock.
```

Default Value:

Not configured

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/tasks/AdministrationTimeSet.html

CIS Controls:

Version 7

6.1 Utilize Three Synchronized Time Sources

Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.

1.1.4 Ensure SSL server certificate for remote SSL VPN is configured correctly (Manual)

Profile Applicability:

- Level 2

Description:

The Certificate used to secure SSL VPN should satisfy the following criteria.

- It should be a valid certificate from a trusted source. In most cases this means a trusted Public Certificate Authority as remote sslvpn users may not have access to any Private Certificate Authorities for Certificate validation.
- The certificate should have a valid date. It should not have a "to" date in the past (it should not be expired), and should not have a "from" date in the future.
- The key length used to encrypt the certificate should be 2048 bits or more.
- The hash used to sign the certificate should be SHA-2 or better.

Rationale:

If presented with a certificate error, the end user in most cases will not be able to tell if their session is using a self-signed or expired certificate, or if their session is being eavesdropped on or injected into by a "Man in the Middle" attack.

Impact:

Not using a trusted Certificate, issued by a trusted Public Certificate Authority means that clients establishing VPN sessions will always see an error indicating an untrusted Certificate. This means that they will have no method of validating if their VPN session is being hijacked by a "Man in the Middle" (MitM) attack. It also "trains" them to bypass certificate warnings for other services, making MitM attacks easier for those other services as well.

Audit:

```
Verify that the certificate being used to secure the SSL VPN meets the
criteria listed.

Navigate to `System > Administration > Admin settings > Admin console and
end-user interaction > Certificate`

Ensure that a valid certificate is applied to the User portal.

Navigate to `Configure > VPN > Show VPN settings > SSL VPN settings > SSL
server certificate`.
```

```
Ensure that a valid certificate is used for the SSL VPN Gateway.
```

Remediation:

```
Create a CSR and install a certificate from a public CA.

Navigate to `System > Administration > Admin settings > Admin console and
end-user interaction > Certificate`.

Set a valid certificate to the User portal.

Navigate to `Configure > Show VPN settings > SSL VPN settings > SSL server
certificate`.

Set a valid certificate for the SSL VPN Gateway.
```

Default Value:

Not configured

References:

1. http://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/VPNSettings.html

CIS Controls:

Version 7

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

1.1.5 Ensure password complexity check is enabled (Automated)

Profile Applicability:

- Level 1

Description:

This checks all new passwords to ensure that they meet basic requirements for strong passwords.

Rationale:

Password complexity recommendations are derived from the USGCB (United States Government Configuration Baseline), Common Weakness Enumeration, and benchmarks published by the CIS (Center for Internet Security). Password complexity adds entropy to a password, in comparison to a simple password of the same length. A complex password is more difficult to attack, either directly against administrative interfaces or cryptographically, against captured password hashes. However, making a password of greater length will generally have a greater impact in this regard, in comparison to making a shorter password more complex.

Impact:

Simple passwords make an attacker's job very easy. There is a reasonably short list of commonly used admin passwords for network infrastructure, not enforcing password lengths and complexity can lend itself to making an attacker's brute force attack successful.

Audit:

```
Navigate to `System > Administration > Admin settings > Administrator
password complexity settings > Enable password complexity check`.

Verify that `Enable password complexity check` is enabled.

Ensure that the various password settings to values that are appropriate to
your organization. Should be checked for use at least one uppercase and one
lowercase letter, include at least 1 numeric character and include at least 1
special character like @,$,!,etc.
```

Remediation:

```
Navigate to `System > Administration > Admin settings > Administrator
password complexity settings > Enable password complexity check`.

Set Enable password complexity check.
Set that the various password settings to values that are appropriate to your
organization. It is suggested that there at least be some special characters
enforced, and that a minimum length be set. Ensure that Minimum Uppercase,
Lowercase and Special Characters.
Operationally, dictionary words should be avoided for all passwords -
passphrases are a much better alternative.
```

Default Value:

Not enabled

References:

1. https://support.sophos.com/support/s/article/KB-000035727?language=en_US

CIS Controls:

Version 7

4.2 Change Default Passwords
Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.

16 Account Monitoring and Control
Account Monitoring and Control

1.1.6 Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone (Automated)

Profile Applicability:

- Level 1

Description:

It is recommended to limit exposure of Firewall administration services from WAN/untrusted zone. When necessary, leverage on remote VPN or limiting only from selected IP addresses, or use of Sophos Central for firewall administration.

For additional security control - RBAC and administrative accounts can be enabled with 2-factor authentication using built-in RADIUS Server.

By disabling 'HTTPS', 'SSH' and 'Network services (PING/PING6, DNS, SMTP RELAY, SNMP)' on WAN zone to protect against reconnaissance attempts, network scanners and potential adversary.

Rationale:

When the device is exposed to the internet with service ports, it could be subjected to DOS, brute-force attempts, and underlying vulnerability on service ports can be discovered by the attacker.

Impact:

When left enabled - it could lead to brute force attempt on the Webadmin interface, denial of service attack from wide range of IP addresses and increase attack surface from potential adversary.

Audit:

```
Navigate to `System > Administration > Device Access > Local service ACL`.

Verify `HTTPS,SSH,PING/PING6,DNS,SMTP RELAY, SNMP` on `WAN Zone` is
unchecked.

Navigate to `Local service ACL exception rule`.

Verify that `Added exception rule` only allows limited IP addresses for
device management.
```

Remediation:

```
Navigate to `System > Administration > Device Access > Local service ACL`.

Uncheck `HTTPS,SSH,PING/PING6,DNS,SMTP RELAY, SNMP` on `WAN Zone`.
```

Default Value:

Not configured

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/AdministrationDeviceAccess.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

11.7 Manage Network Infrastructure Through a Dedicated Network
Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

1.1.7 Ensure valid certificate is set for web browser used to access Webadmin interface (Automated)

Profile Applicability:

- Level 2

Description:

Default HTTPS port 4444 is used to access XG Firewall's Webadmin interface. HTTPS certificate used to secure the administrative session should satisfy the following criteria:

1. A valid certificate from a trusted source should be used. While a certificate from a trusted Public Certificate Authority is certainly valid, one from a trusted Private Certificate Authority is absolutely acceptable for this purpose.
2. The certificate should have a valid date. It should not have a "to" date in the past (it should not be expired), and should not have a "from" date in the future.
3. The certificate should use an acceptable cipher and encryption level.

Rationale:

If a certificate that is self-signed, expired, or otherwise invalid is used for HTTPS interface, administrators in most cases will not be able to tell if their session is being eavesdropped or injected into by "Man in the Middle" attack.

Impact:

If the default self-signed certificate is used, an administrator will not be able to tell if their HTTPS session is being hijacked or not. Using a trusted certificate ensures that the session is both encrypted and trusted.

Audit:

```
Navigate to `System > Certificates > Certificates`.

Verify that the certificate used to secure HTTPS sessions meets the criteria
by reviewing the appropriate certificate.

Navigate to `System > Administration > Admin settings > Admin console and
end-user interaction > Certificate`.

Verify that correct Certificate is used for Webadmin, user portal, captive
portal and SPX reply portal.
```

Remediation:

```
If a new administrative Certificate is needed, acquire a Certificate that
meets the stated criteria and upload it to the XG Firewall. Optionally,
download the appliance Certificate Authority to the web browser used for
administration.

Navigate to `System > Certificates > Certificates > Add`

Import an appropriate Certificate for your administrative session, from a
trusted Certificate Authority.

Navigate to `System > Administration > Admin settings > Admin console and
end-user interaction > Certificate`

Choose the correct certificate to use for the web based administrative
session.
```

Default Value:

A self-signed certificate is used by default for the administrative interface.

References:

1. https://community.sophos.com/kb/en-us/132678

Additional Information:

Verify that the clock is both accurate and reliable on both the XG and on the administrative workstations before setting the SSL/TLS Service Profile. Inaccurate or mismatched clocks will result in certificate errors and can result in loss of HTTPS administrative access.

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

16.5 Encrypt Transmittal of Username and Authentication Credentials
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

1.2 SNMP & Device Notification Settings

Device Notification Settings section contains setting up SNMP server and email settings on how the device sends notification for critical events that need administrator's attention.

1.2.1 Ensure SNMPv3 is selected for queries and traps (Manual)

Profile Applicability:

- Level 1

Description:

SNMP (Simple Network Management Protocol) gives access to XG Firewall information such as status of the firewall, service availability, CPU, memory and disk usage. Although XG Firewall supports SNMPv1 and SNMPv2c protocols, you should always use SNMPv3 for user and the authorized hosts to send traps. Specify encryption and authentication settings to ensure confidentiality, message integrity, and user validity.

Rationale:

SNMPv3 utilizes AES-128 encryption, message integrity, user authorization, and device authentication security features. SNMPv2c does not provide these security features. If an SNMPv2c community string is intercepted or otherwise obtained, an attacker could gain read access to the firewall. Note that SNMP write access is not possible.

Audit:

```
Navigate to `System > Administration > SNMP`.

Verify that SNMPv1 and v2 are not configured.

Verify that `SNMPv3 users and traps > Encryption algorithm` is configured
with either AES or DES. Set appropriate password strength for both
authentication and encryption.
```

Remediation:

```
Navigate to `System > Administration > SNMP`.

Remove insecure SNMPv1 and v2 configurations.

Set `SNMPv3 users and traps > Encryption algorithm` is configured with either
AES or DES. Set appropriate password strength for both authentication and
encryption.
```

Default Value:

Not configured

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/tasks/AdministrationSNMPUserAdd.html

CIS Controls:

Version 7

4.5 Use Multifactor Authentication For All Administrative Access
Use multi-factor authentication and encrypted channels for all administrative account access.

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

14.4 Encrypt All Sensitive Information in Transit
Encrypt all sensitive information in transit.

1.2.2 Ensure notification is configured to send system and security events (Manual)

Profile Applicability:

- Level 1

Description:

This recommendation ensures that administrator receives notification on system events, reports and security incidents either via email or SNMP Traps.

Rationale:

Verify the notification settings to ensure that correct email address of sender "From Email Address” and recipient “Send notification to email address” is configured. Both settings should be reflected according to the rightful sender and recipient together with notification list for admin, system, security events.

Impact:

This recommendation ensures that administrator receives the notifications for critical system, security events and reports.

Audit:

```
Navigate to `System > Administration > Notification settings > Mail server
settings`.

Verify that `Send notification via > Built-in email server` or `External
email server` is checked and configure email settings appropriately.

Navigate to `Configure > System services > Notification list`.

Verify that appropriate admin, system and security events are checked to send
email notification and/or SNMP traps.
```

Remediation:

```
Navigate to `System > Administration > Notification settings`.

When `built-in email server` is used.

Set the `from email address` of the sender.

Set the `Send notifications to email address` of the administrators’ email
address.
```

```
Set `Management interface IP address` to send notification from.

When `External mail server` is used.

Set the `Mail server IPv4 address/FQDN - Port` is set to the outgoing mail
server.

Set `username` and `password` to authenticate to the outgoing mail server.
Set `connection security` to `STARTTLS` or `SSL/TLS`.

Navigate to `Configure > System services > Notification list`.

Set the appropriate admin, system and security events to send email
notification and/or SNMP traps.
```

Default Value:

Not configured

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/tasks/AdministrationNotificationList.html

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

2 User Identification & Authentication

All the users accessing the network resources should be authenticated by Firewall. Once authentication is successful XG Firewall communicates with directory servers to get additional authorization data for access control.

While the users are on the network, XG Firewall can identify and map according to the username instead of IP addresses and establish Identification, Authentication, Authorization and Accountability(IAAA).

2.1 Ensure Firewall rules are configured to identify users before authorizing access (Manual)

Profile Applicability:

- Level 2

Description:

Configure appropriate settings to map IP addresses to usernames. Mapping users to IP addresses is what permits the firewall to create rules based on users and groups rather than IP addresses and subnets, as well as log events by usernames rather than IP addresses or DNS names. The specifics of how to achieve IP-to-username mapping is highly dependent on the environment. It can be enabled by integrating the firewall with a domain controller, captive portal, Terminal Server, Kerberos, NTLM, and synchronized security heartbeat from a variety of devices.

Rationale:

Understanding which user is involved in a security incident allows appropriate personnel to move quickly between the detection and reaction phases of incident response. In environments with either short DHCP lease times, or where users may move frequently between systems, the ability to analyze or report, or alert on events based on user accounts or user groups is a tremendous advantage. For forensics tasks when DHCP lease information may not be available, the Source User information may be the only way to tie together related data.

Audit:

```
Validate allowed fire rules with source zone (LAN/DMZ) are configured with
user identification. Source network where users are located must authenticate
to XG Firewall first before accessing network resources.

Verify that `Protect > Rules and policies > Firewall rules` and within the
firewall rule ensure `Match known users` is checked and add authorized `User
or groups`. Captive portal redirects to unknown users by ensuring `Use web
authentication for unknown users` is checked.
```

Remediation:

```
To enable user based firewall rule:

Navigate to `Protect > Rules and policies > Firewall rules` edit existing
policies or when creating a new firewall policy `match known users` is
checked.
`Log firewall traffic` is checked to log for allowed traffic.
```

```
Configure authentication server to use for firewall connections.

Navigate to `Configure > Authentication > Services > Firewall authentication
methods` move the primary authentication server at the top.

Configure Clientless users for devices such as printers and IoT devices that
unable to authenticate with standard authentication options.

To add the devices to clientless users, navigate to `Configure >
Authentication > Clientless users > Add or Add range`

In Active directory environment AD SSO can be configured to allow
unauthenticated web access.

Navigate to `Configure > Authentication > Web Authentication > Authorize
unauthenticated users for web access > Kerberos & NTLM` and `show captive
portal link` is checked.

In Window only environment clientless SSO can be configured to authenticate
with XG based on security logon events at the Domain Controllers.

Navigate to `Configure > Authentication > STAS > Enable Sophos Transparent
Authentication Suite > Add new collector` and `Restrict client traffic during
identity probe > Yes`.

Refer to the reference section for more information with the configuration.
```

Default Value:

Not configured.

References:

1. 1. “How to integrate Sophos firewall with active directory” - https://community.sophos.com/kb/en-us/123155
2. 2. “Clientless SSO in a single AD Domain Controller Environment?” - https://community.sophos.com/kb/en-us/123156
3. 3. “How to deploy STAS v2.5” – https://community.sophos.com/kb/en-us/133531
4. 4. “How to configure clientless users” – http://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/concepts/ClientlessUserManage.html

CIS Controls:

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

16 Account Monitoring and Control

Account Monitoring and Control

16.13 Alert on Account Login Behavior Deviation

Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.

2.2 Ensure Encrypted connection is used in connecting external Active Directory and LDAP (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft has made secure connections mandatory for recent server versions. The security of the communication can be significantly improved for LDAP simple binds that are performed over SSL/TLS connections.

Rationale:

Unsigned network traffic is susceptible to replay attacks in which an intruder intercepts the authentication attempt and the issuance of a ticket. The intruder can reuse the ticket to impersonate the legitimate user. Additionally, unsigned network traffic is susceptible to man-in-the-middle (MiTM) attacks in which an intruder captures packets between the client and the server, changes the packets, and then forward them to the server.

Audit:

```
Navigate to `Configure > Authentication > Servers > Edit` and verify that
`Connection security` is selected with either `SSL/TLS` or `STARTTLS` is used
and `Validate server certificate` is checked.
```

Remediation:

```
Navigate to `Configure > Authentication > Servers > Edit or Add` and set
`Connection security` with either `SSL/TLS` or `STARTTLS` and `Validate
server certificate` is checked.
```

Default Value:

Not configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/AuthenticationActiveDirectoryServer.html

CIS Controls:

Version 7

11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions
Manage all network devices using multi-factor authentication and encrypted sessions.

3 System Services, Firmware and Updates

This section covers High Availability (HA) and XG firewall update of ATP, AV, IPS, Application signatures, WAF, firmware and security related hotfixes.

3.1 Ensure "Fully Synchronized" High Availability peer is configured (Manual)

Profile Applicability:

- Level 2

Description:

High Availability (HA) is a clustering technology that is used to maintain uninterrupted service in the event of power, hardware, or software failure. Sophos Firewall devices can be configured in Active-Active or Active-Passive HA modes. The Devices (The Primary and Auxiliary Device) are physically connected over a dedicated HA link port.

Rationale:

To ensure availability of both the firewall and the resources it protects, a High Availability peer is required. In the event a single firewall fails, or when maintenance such as a firmware update is required, the HA peer can be used to automatically fail over session states and maintain overall availability of the network.

Impact:

Not configuring High Availability (HA) correctly directly impacts the availability of the system. With HA in place, standard maintenance such as OS updates, network and power cabling changes can be accomplished with no outage or a minimum impact.

Audit:

```
Navigate to `System Services > High Availability > High Availability Status`.
Verify that `HA status` is either `Established[Active-Passive]` or
`Established[Active-Active]` and confirm `Local` and `Peer` devices are not
showing `Standalone` or `Faulty`.


Navigate to `High Availability Configuration > Select ports to be monitored`.
Verify that correct interfaces are monitored.

`Keepalive request interval` and `Keepalive attempts` should be set to
optimal setting or remain default value of `250` milliseconds and `16`
attempts respectively.
```

Remediation:

```
Navigate to `System Services > High Availability > High Availability Status`.
When `Local` and `Peer` devices are shown as `Standalone` or `Faulty`,
connection to the auxiliary device could be lost or becomes a faulty node,
re-configure HA and sync auxiliary device to a working state.


Navigate to `High Availability Configuration > Select ports to be monitored`.
Set the correct interfaces to be monitored.

Configure default value of `Keepalive request interval` to `250` milliseconds
and `Keepalive attempts` to `16` attempts or set to optimal setting
respectively.
```

Default Value:

Not configured

References:

1. https://www.sophos.com/en-us/medialibrary/PDFs/documentation/SophosFirewall/Pocket-Guides/Active-Active-HA-Configuration.pdf
2. https://support.sophos.com/support/s/article/KB-000035744?language=en_US

CIS Controls:

Version 7

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

3.2 Ensure 'Pattern updates' is set to download and install updates every 15 minutes (Manual)

Profile Applicability:

- Level 1

Description:

Set Pattern download/installation to 'auto update' and interval of 'every 15 minutes'

Rationale:

New protection patterns may be released at any time. With frequent update schedule, the firewall can ensure threats with new definitions are quickly mitigated. A daily update schedule could leave an organization vulnerable to a known virus for nearly 24 hours, in a worst-case scenario. Setting an appropriate threshold value reduces the risk of a bad definition file negatively affecting traffic.

Impact:

Advanced Threat Protection (ATP) patterns, AV signatures, GeoIP database, IPS and application signatures to block immediate, active threats to the environment. With a 15 minutes update schedule, the firewall can ensure threats with new definitions are quickly mitigated.

Audit:

```
Navigate to `System > Backup & Firmware > Pattern Updates`.

Verify that `Pattern download/installation > Auto update` is set to `ON`.

Verify that `Interval` is set to `Every 15 minutes`.

Verify that `Pattern` `Last successful update` is showing `Success`
```

Remediation:

```
Navigate to `System > Backup & Firmware > Pattern Updates`.

Set `Pattern download/installation > Auto update` to `ON`.

Set the download `Interval` to `Every 15 minutes`.

When the `Pattern` `Last successful update` is not showing `Success`, click
`Update pattern now` to download the updates manually.
```

Default Value:

Not configured

References:

1. http://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/PatternManage.html

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy Automated Software Patch Management Tools
Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

12 Boundary Defense
Boundary Defense

3.3 Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes' (Manual)

Profile Applicability:

- Level 1

Description:

Set hotfixes to be applied automatically whenever there is an out-of-band security update is available for the device.

Rationale:

Security updates of the XG device can be released at any time. To ensure XG and the rest of the network remain protected from known vulnerability hotfixes should be allowed and device can be applied automatically.

Audit:

```
Navigate to `System > Backup & Firmware > Firmware > Hotfix`.

Verify that `Hotfix > Allow automatic installation of hotfixes` is checked.
```

Remediation:

```
Navigate to `System > Backup & Firmware > Firmware > Hotfix`.

Tick the checkbox `Allow automatic installation of hotfixes`.
```

Default Value:

This setting is enabled by default.

References:

1. http://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/AvailableFirmware.html

CIS Controls:

Version 7

3.4 Deploy Automated Operating System Patch Management Tools
Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.

3.5 Deploy Automated Software Patch Management Tools
Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

12 Boundary Defense
Boundary Defense

3.4 Ensure XG takes encrypted backup of the configuration and send to designated email address with scheduled frequency (Manual)

Profile Applicability:

- Level 1

Description:

Set XG to send encrypted backup of the configuration to administrators' email address or store at the backup FTP server.

Rationale:

Hardware or software failure can happen any time. In the event network needs to be restored immediately, ensure the backup snapshot of the configuration is taken at regular interval and store in secure encrypted format at the redundant location to restore at the new device.

Audit:

```
Navigate to `System > Backup & Firmware > Backup & Restore > Backup`.
Backup mode is set to either `FTP` or `Email`.

When `Backup mode` is set to `FTP`, verify that `FTP server IP`, `Username`
or `FTP password` is set.

When `Backup mode` is set to `Email` verify that `Email Address` is set to
the administrators' email address.

Verify that `Frequency` is set to `Daily, Weekly or Monthly`.

Verify that `Encryption password` is set and ensure that encrypted backup can
be sent successfully.
```

Remediation:

```
Navigate to `System > Backup & Firmware > Backup & Restore > Backup`.
Backup mode is set to either `FTP` or `Email`.

When `Backup mode` is set to `FTP`, configure `FTP server IP`, `Username` or
`FTP password`.

When `Backup mode` is set to `Email`, configure `Email Address` to the
administrators' email address.

`Frequency` is set to `Daily, Weekly or Monthly`.

Set strong `Encryption password` and ensure that encrypted backup can be sent
```

```
successfully. Store the `Encryption password` in secure location for future
recovery.
```

Default Value:

Not enabled.

References:

1. http://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/concepts/BackupRestore.html

CIS Controls:

Version 7

10.1 Ensure Regular Automated Back Ups
Ensure that all system data is automatically backed up on regular basis.

10.2 Perform Complete System Backups
Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

10.4 Ensure Protection of Backups
Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

10.5 Ensure Backups Have At least One Non-Continuously Addressable Destination
Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.

3.5 Ensure No Expired Subscription Licenses (Manual)

Profile Applicability:

- Level 1

Description:

Licensing is used to enable various features on XG Firewall regardless whether the license is for hardware or software/virtual firewall.

Rationale:

Active subscription will ensure the device is getting up-to-date signatures for both known and unknown threats and remain functional for services requires cloud lookup.

Impact:

Expired subscription will lapse security updates which will impact the security effectiveness of the feature/functionality.

Audit:

```
Navigate to `System > Administration > Licensing`.

Verify under `Module subscription details` under `Status` to ensure there is
no expired licenses for all the subscriptions.
```

Remediation:

```
Navigate to `System > Administration > Licensing`.


Under `Module subscription details` and click `Synchronize` to connect to the
licensing server to get latest subscription details. Or contact Sophos
immediately to renew the expired licenses.
```

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/Licensing.html
2. https://support.sophos.com/support/s/article/KB-000038005?language=en_US

CIS Controls:

Version 6

11.5 Maintain Network Device Patch Levels
Install the latest stable version of any security-related updates on all network devices.

Version 7

8.2 Ensure Anti-Malware Software and Signatures are Updated
Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.

3.6 Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode" (Manual)

Profile Applicability:

- Level 2

Description:

IKEv1 Aggressive Mode does not provide Peer Identity Protection. They are vulnerable to offline dictionary or brute force attack.

Rationale:

As stated in CVE-2002-1623, the design of the Internet Key Exchange (IKE) protocol, when using Aggressive Mode for shared secret authentication, does not encrypt initiator or responder identities during negotiation, which may allow remote attackers to determine valid usernames by monitoring responses before the password is supplied or sniffing.

Impact:

The use of IKEv1 with Aggressive Mode has considerable confidentiality impact.

Audit:

```
Navigate to `Configure > VPN > IPsec policies`.
Verify that active `IPsec Policy` in used is not configured with `Key
exchange` `IKEv1` and `Authentication mode` `Aggressive mode`.
```

Remediation:

```
Navigate to `Configure > VPN > IPsec policies`.
Remove any active `IPsec Policy` configured with `Key exchange` `IKEv1` and
`Authentication mode` `Aggressive mode` and replace with `IKEv2` or `Main
mode`.
```

Default Value:

Not configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/tasks/IPsecPolicyAdd.html

CIS Controls:

Version 6

16.13 User/Account Authentication Must Be Performed Over Encrypted Channels
Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.

3.7 Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server (Manual)

Profile Applicability:

- Level 2

Description:

XG Firewall provides extensive logging capabilities for traffic, system, and network protection functions. You can use logs to analyze network activity to help identify security issues and reduce network abuse.

You can store logs locally, send them to Sophos Central, or send them to third-party syslog servers.

You can select logs to store or send by module or feature, or you can select all logs.

Rationale:

Firewall

Firewall logs provide information about traffic associated with the firewall configuration, such as firewall rules, MAC filtering, and DoS attacks.

IPS

IPS logs provide records of detected and dropped attacks based on unknown or suspicious patterns (anomalies) and signatures.

Antivirus

Antivirus logs provide details of viruses detected in HTTP, SMTP, FTP, POP3, IMAP4, HTTPS, SMTPS, IMAPS, and POPS traffic.

Anti-spam

Anti-spam logs provide details about SMTP, POP3, IMAP4, SMTPS, POPS, IMAPS spam, and probable spam mails.

Content filtering

Content filtering logs provide details about web and application filtering events, such as those associated with web policies.

Events

Event logs provide information about configuration activities, authentication activities, and system activities.

Web server protection

Web server protection logs provide details of web server protection activities, for example, protection policies.

Advanced threat protection

Advanced threat protection logs provide information about ATP events such as drops or alerts.

Wireless

Wireless logs provide details about access point activity and SSIDs.

Heartbeat

Heartbeat logs provide information about the health status of the endpoints.

System health

System health logs provide details of CPU usage, memory usage, number of live users, interfaces, and disk partitions.

Sandstorm

Sandstorm logs provide records of all Sandstorm events.

Audit:

```
Navigate to `Protect > Rules and policies`.
Verify the configured the Firewall rules and ensure `Log firewall traffic` is
checked.


Navigate to `Configure > System services > Log settings`.
Verify that external syslog server is configured and sending system, security
events to external syslog server.
```

Remediation:

```
Navigate to `Protect > Rules and policies`.
Set `Log firewall traffic` is checked for configured firewall rules.
```

```
Navigate to `Configure > System services > Log settings`.
Configure external syslog server and set to send system, security events to
external syslog server.
```

Default Value:

Not configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/ServicesLogSettings.html

CIS Controls:

Version 6

6.4 Regularly Monitor Logs For Anomalies
Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.

Version 7

6.2 Activate audit logging
Ensure that local logging has been enabled on all systems and networking devices.

6.3 Enable Detailed Logging
Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.

4 Advanced Threat & Synchronised Security

Advanced threat protection allows you to monitor and analyze all traffic on your network for threats and take appropriate action. For example - when the threat is detected, logging the affected machines' name/IP, current logged in users, threat type and source/destination of the traffic and drop the connection. You can also view Sandstorm activity and the results of file analysis. Use these results to determine the level of risk posed to your network.

4.1 Ensure 'Enable advanced threat protection' is set to 'ON' and Policy is set to 'Log and drop' (Manual)

Profile Applicability:

- Level 2

Description:

Advanced threat protection analyzes incoming and outgoing network traffic (for example, DNS requests, HTTP requests, and IP packets) for threats.

Rationale:

Using ATP, you can quickly detect compromised clients in your network and raise an alert or drop the traffic from those clients.

Audit:

```
Navigate to `Advanced threat > Advanced threat protection > Enable advanced
threat protection`.


Verify that `Enable advanced threat protection` is set to `ON`.


Verify that Policy is set to `Log and drop`.


Verify that wide range of network/host IP addresses are not added to
`Network/Host Exceptions`.

Verify that wide range of destination URL/IP addresses are not added to
`Threat Exceptions` that may expose network to the security risks.
```

Remediation:

```
Navigate to `Advanced threat > Advanced threat protection > Enable advanced
threat protection`.


Verify that `Enable advanced threat protection` is set to `ON`.


Set the policy to `Log and drop`.


Remove unnecessary exemption from network and threat exceptions.
```

Default Value:

Not enabled.

References:

1. Sandstorm is a cloud-based malware detonation, analysis and blocking service for SOPHOS XG firewalls. It is based on exploit prevention technologies from Endpoint InterceptX combined with deep learning neural network to detect unknown malware delivered through the network. Post-analysis threat intelligence report generated from Sandstorm highlight attack vector and breakdown of threat intelligence obtained through file analysis. Advanced threat protection detects and blocks outbound command and control activity by observing traffic in real-time. This Advanced Threat section covers requirements related to Sandstorm settings and Advanced threat protection configuration.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

4.2 Ensure Sandstorm is enabled at the firewall rule for web protection and does not exclude any file type from Sandstorm analysis (Manual)

Profile Applicability:

- Level 2

Description:

By enabling 'Detect zero-day threats with Sandstorm' at the firewall rule increases the possibility of identifying unknown viruses. And ensure administrator does not exclude file types from Sandstorm analysis.

Rationale:

When a user downloads a file from the internet via HTTP/S, FTP protocol and the file contains active content or unknown reputation that cannot be easily detected by signature-based AV engine, it will be uploaded to SOPHOS cloud sandboxing service for additional analysis. Accidental exclusion of file type at Sandbox configuration will reduce the security effectiveness.

Impact:

With Detect zero-day threats with Sandstorm is unchecked, users may unknowingly download files that have not been seen by AV engines or weaponized office documents. Exclude file types in the Sandstorm settings could also bypass broad range of true filetype from uploading to the cloud for additional analysis.

Audit:

```
For firewall rules that allowed outbound traffic to the internet should be
enabled with 'detect zero-day threats with Sandstorm'.

Navigate to `Protect > Rules and policies > Firewall rules` existing firewall
rule with allowed outbound traffic and verify `Security features > Web
filtering > Malware and content scanning > Scan HTTP and decrypted HTTPS`,
`Detect zero-day threats with Sandstorm` and `Scan FTP for malware` is
checked.


Navigate to `Protect > Advanced threat > Sandstorm settings` and verify
`Exclude file types` to ensure there are no file type is exempted from
Sandbox analysis.
```

Remediation:

```
Navigate to `Protect > Rules and policies > Firewall rules` existing firewall
rule with allowed outbound traffic and configure `Security features > Web
filtering > Malware and content scanning > Scan HTTP and decrypted HTTPS`,
`Detect zero-day threats with Sandstorm` and `Scan FTP for malware` is
checked.


Navigate to `Protect > Advanced threat > Sandstorm settings` and remove file
type exceptions from `Exclude file types`.
```

References:

1. https://support.sophos.com/support/s/article/KB-000036574?language=en_US
2. https://support.sophos.com/support/s/article/KB-000036080?language=en_US
3. https://support.sophos.com/support/s/article/KB-000036564?language=en_US

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

4.3 Ensure Sandstorm is enabled for Email Protection and set to MTA mode (Manual)

Profile Applicability:

- Level 2

Description:

By enabling ‘Detect zero-day threats with Sandstorm’ at the SMTP policy increases the possibility of identifying unknown viruses delivered through email gateway.

Rationale:

Targeted attacks with Email attachments that contain zero-day viruses and weaponized office documents could be thwarted at the Email gateway by scanning at the SMTP proxy before routed to the internal email server. Accidental exclusion of file type at Sandbox configuration will reduce the security effectiveness.

Impact:

Zero-day viruses and Advanced Persistent Threats (APT) can be delivered via weaponized office documents as a form of attachment to the business email. By setting appropriate malware protection setting to scan for viruses and detect zero-day threats with Sandstorm before delivering the emails to the MTA.

Audit:

```
This configuration option is only applicable when the device is configured
with `MTA mode` and set `Sophos` as primary malware scanning engine.



Navigate to `Protect > Email`. Verify the existing SMTP policy `Malware
protection > Selected antivirus action` to `Drop`. Email attachment
successfully verified by antivirus engine as malicious should be set to
`Drop`.

`Quarantine unscannable content` is checked to prevent files with multiple
layers of compression and password protected archives files that cannot be
scanned by antivirus engine should be `quarantined`.


Verify that `Detect zero-day threats with Sandstorm` should be checked and
set the scanned file size to 10 MB.
```

Remediation:

```
This configuration option is only applicable when the device is configured
with `MTA mode` and set `Sophos` as primary malware scanning engine.



Navigate to `Protect > Email`. Verify the existing SMTP policy and set
`Malware protection > Selected antivirus action` to `Drop`. Email attachment
successfully verified by antivirus engine as malicious should be set to
`Drop`.

`Quarantine unscannable content` is checked to prevent files with multiple
layers of compression and password protected archives files that cannot be
scanned by antivirus engine should be `quarantined`.


Set `Detect zero-day threats with Sandstorm` is checked and set the scanned
file size to 10 MB.
```

Default Value:

Not configured.

References:

1. https://support.sophos.com/support/s/article/KB-000036574?language=en_US
2. https://support.sophos.com/support/s/article/KB-000036080?language=en_US
3. https://support.sophos.com/support/s/article/KB-000036564?language=en_US

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

4.4 Ensure Synchronised Security Heartbeat is enforced on Firewall Rules (Manual)

Profile Applicability:

- Level 2

Description:

Security Heartbeat enables XG Firewall and endpoints managed by Sophos Endpoint Protection to communicate through Sophos Central and exchange information on the endpoints' security status, the so-called health status. XG Firewall administrators as well as Sophos Central administrators are able to define policies for network access based on the endpoints' health status. Endpoints with security incidents can be immediately isolated thus preventing threats to spread across the network.

Rationale:

Sophos Endpoint Protection ensures that the endpoint belongs to the organization and has permission to access the network. These endpoints send at regular intervals updates about their health status to XG Firewall which in turn applies the defined policies based on that information.

Impact:

Missing heartbeat or endpoint with compromised state should not be allowed to connect to servers, internet and other devices within the network. Synchronized security heartbeat can identify the source of infection and isolate the device from the rest of the network.

Audit:

```
Navigate to `Protect > Central Synchronization`.
Verify that `Security Heartbeat` is turned `ON`.

Check that XG firewall is registered to Sophos Central, configured to receive
Heartbeat from the Sophos Endpoints.


Navigate to `Protect > Rules and Policies > Firewall rules`.
Filter `Rule type >` `Network` and `User`, filter `source zone > LAN` and
`DMZ`.
Verify on the configured firewall rule `Configure Synchronized Security
Heartbeat` and check that `Minimum source HB permitted` is set to `Green` or
`Yellow`.

If the rule is configured to allow Egress traffic with clients are connecting
resources on `WAN` zone, `Minimum source HB permitted` should be configured
```

```
with either `Green` or `Yellow` for tighter security control.

If the rule is configured to allow traffic between `LAN` to `DMZ` zones with
communication between Sophos protected Endpoints and Server, please consider
additional control with setting both `Minimum source HB permitted` and
`Minimum destination HB permitted` to either `Green` or `Yellow`.
```

Remediation:

```
Navigate to `Protect > Central Synchronization`.

Register Sophos XG Firewall to Sophos Central, set `Security Heartbeat` to
`ON`.

Navigate to `Protect > Rules and Policies`.
Filter `Rule type > Network` and `User`, filter `source zone > LAN` and
`DMZ`.
Navigate to configured firewall rule with `Configure Synchronized Security
Heartbeat`.


Set `Minimum source HB permitted` to `Green` or `Yellow`.


If the rule is configured to allow Egress traffic with Sophos Endpoints are
connecting resources on `WAN` zone, set `Minimum source HB permitted` to
either `Green` or `Yellow` for tighter security control.


If the rule is configured to allow traffic between `LAN` to `DMZ` zones with
communication between Sophos protected Endpoints and Server, configure
additional control with setting both `Minimum source HB permitted` and
`Minimum destination HB permitted` to either `Green` or `Yellow`.
```

Default Value:

Not configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/CentralSynchronization.html

CIS Controls:

Version 7

19 Incident Response and Management
Incident Response and Management

5 Protection Rules And Profiles

This section covers all aspect of protection configuration both Ingress and Egress traffic including SSL/TLS Inspection rules, URL filtering, AV, IPS and Application control, Web server security profiles, Wireless and VPN profiles.

5.1 Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly. (Manual)

Profile Applicability:

- Level 2

Description:

Configure Web Policy to control users' web browsing activities, block inappropriate web categories and enforce malware scanning for FTP and HTTP(S) traffic.

Rationale:

Web protection keeps an organization safe from attacks that result from web browsing and helps you increase productivity. By blocking objectionable URL categories and potentially unwanted applications (PUAs), enforcing malware scanning for FTP, HTTP(S), the threat of malware propagation through the firewall is greatly reduced. It is recommended to mitigate malware found in FTP, HTTP(S) through outgoing traffic, you can configure to prevent users downloading certain File Types, Block web category or Warn with appropriate deterrent messages display to the users.

Impact:

Any misconfigured policies or unintended exceptions will allow users to access inappropriate web categories, URLs that linked to drive-by-downloads and malware.

Audit:

```
Navigate to `Protect > Web`.

Verify that configured web policies have categories with `objectionable
classification` is set to block. Ensure that Status is set to `ON` with the
block rule is on top.


Within the web policy `Advanced settings > Enable logging and reporting` is
checked.


Navigate to `Protect > Web > General settings > Protection > Malware and
content scanning`.


Verify that `Action on malware scan failure` is set to `Block(best
protection)`.
```

```
Verify that `Block potentially unwanted applications` is checked.


Navigate to `Protect > Web > Exceptions`.


Verify that configured exceptions do not have dangerous `URL patterns, web
site categories and wide range of destination IP address(website address)`
that will have security impact to the `source IP addresses (end-users'
address)` with skipped `HTTPS decryption, HTTPS certificate validation,
malware and content scanning, sandstorm and policy check`.
```

Remediation:

```
Navigate to `Protect > Web`

Set the web policy to block categories with `objectionable classification`
and change the status to `ON`.

Within the web policy set the `Enable logging and reporting`.

Navigate to `Protect > Web > General settings > Protection > Malware and
content scanning`

Action on `malware scan failure` is set to `Block(best protection)`.

Enable `Block potentially unwanted applications`.

Navigate to `Protect > Web > Exceptions`

Remove/edit `exceptions` with `URL patterns, website categories and
destination IP address (website address)` that could reduce security
effectiveness to the `source IP address (end-users' address)`.
```

Default Value:

Not configured

References:

1. https://support.sophos.com/support/s/article/KB-000036683?language=en_US
2. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/concepts/WebProtection.html

CIS Controls:

Version 7

7.4 Maintain and Enforce Network-Based URL Filters

Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.

7.5 Subscribe to URL-Categorization service

Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.

7.6 Log all URL requests

Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

8 Malware Defenses

Malware Defenses

5.2 Ensure SSL/TLS inspection rules is enabled to all relevant firewall policies (Manual)

Profile Applicability:

- Level 2

Description:

With SSL/TLS inspection rules, you can intercept and decrypt SSL and TLS connections over TCP, enabling XG firewall to enforce secure connections between clients and web servers. SSL/TLS inspection enables the prevention of malware transmitted through encrypted connections.

Rationale:

By applying SSL/TLS inspection rule to the applicable traffic, the threat of malware propagation through the encrypted communication is greatly reduced. SSL/TLS inspection profile also can limit any communication with insecure encryption protocol within the organization.

Impact:

Not enforcing security policy on encrypted traffic may allow malware to transit the security boundary without blocks or alerts. With proper security policy to scan and decrypt the TLS/SSL traffic, XG firewall has visibility of the communication and not only block the malware at the gateway but also preventing insecure communication to take place.

Audit:

```
Navigate to `Rules and policies > SSL/TLS inspection rules > SSL/TLS
inspection settings`.


Verify that `Non-decryptable traffic > SSL 2.0 and SSL 3.0` is set to
`Reject` or `Drop`.


Verify that `SSL compression` is set to `Reject` or `Drop`.


Verify that `When SSL/TLS connections exceed limit` is set to `Drop` or
`Reject`.


Verify that `TLS 1.3 decryption` is set to `Decrypt as 1.3`.
Verify that `Advanced settings > SSL/TLS engine` is set to `Enabled`.


Verify the configured `SSL/TLS inspection rule` and check the `Action` to
`Decrypt` and `Log connections` is checked. The rule position should be above
rules configured with `Action` set to `Don't decrypt`.


Verify the configured Firewall rules and `Scan HTTP and decrypted HTTPS` and
`Detect zero-day threats with Sandstorm` is checked.
```

Remediation:

```
Navigate to `Rules and policies > SSL/TLS inspection rules > SSL/TLS
inspection settings`.


Set `Non-decryptable traffic > SSL 2.0 and SSL 3.0` to `Reject` or `Drop`.


Set `SSL compression` to `Reject` or `Drop`.


Set `When SSL/TLS connections exceed limit` to `Drop` or `Reject`.


Set `TLS 1.3 decryption` to `Decrypt as 1.3`.


Set `Advanced settings > SSL/TLS engine` to `Enabled`.


Navigate to configured `SSL/TLS inspection rule` and set the `Action` to
`Decrypt` and `Log connections` is checked. Set the rule position to above
rules configured with `Action` set to `Don't decrypt`.


Navigate to the configured Firewall rules. Set `Scan HTTP and decrypted
HTTPS` and `Detect zero-day threats with Sandstorm` is checked.
```

Default Value:

No TLS/SSL inspection is enabled on any default or new firewall rule.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/FirewallSSLTLSRules.html
2. https://docs.sophos.com/nsg/sophos-firewall/18.0/releasenotes/en-us/nsg/sfos/releasenotes/rn_SSLTLSInspectionEdit.html

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

5.3 Ensure Application filter is set to block high risk (Risk Level 4 and 5) applications (Manual)

Profile Applicability:

- Level 2

Description:

When there is a firewall rule to allow outgoing traffic, configure it to identify and control Layer-7 applications and drop traffic that are classified under high risk applications (Risk Level 4 and 5) with application filter.

Rationale:

Most organizations may require visibility of the Layer-7 applications, and control access to applications for users behind the firewall. Application filter can reduce the attack surface of risk prone applications, peer-to-peer networking (P2P), these applications can be used to distribute bots, spyware, adware, trojans, rootkits, worms, and other types of malware. It is recommended to block traffic classified as high risk applications. Create custom policies according to the requirements of an organization.

Audit:

```
Navigate to `Rules and policies > Firewall rules`.

Verify that configured outgoing firewall rules with `Identify and control
applications (App control)` is set to `Block high risk (Risk Level 4 and 5)
apps`.
```

Remediation:

```
Navigate to `Rules and policies > Firewall rules`.

Set the configured outgoing firewall rules with `Identify and control
applications (App control)` to `Block high risk (Risk Level 4 and 5) apps`.
```

Default Value:

Not enabled.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/ApplicationFilter.html
2. https://support.sophos.com/support/s/article/KB-000035669?language=en_US

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

5.4 Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules (Manual)

Profile Applicability:

- Level 2

Description:

Network attacks can be prevented using IPS rules. The firewall matches signatures with traffic patterns and takes the action specified in the rule. IPS signatures identify threats and specify a recommended action to take when the firewall encounters matching traffic. Signatures are specific to applications, services, or platforms. The firewall includes predefined signatures and you can also create custom signatures.

Rationale:

XG firewall intercepts and blocks network based attacks targeted at both servers and clients protected behind the firewall. The set of default policies prevents network attacks for several common types of traffic. Depending on the traffic requirement, custom IPS rules can be created to take specific actions based on severity, target, platform and category.

Audit:

```
Navigate to `Rules and policies > Firewall rules`.


Navigate to configured firewall rules. Verify that `Detect and prevent
exploits (IPS)` is configured with appropriate IPS rule based on the
direction of the traffic. Either one of these rule should be present
gerenalpolicy, lantowan_strict, lantowan_general, dmzpolicy, LAN TO WAN, LAN
TO DMZ, WAN TO DMZ, WAN TO LAN, DMZ TO WAN, DMZ TO LAN or “custom IPS rule”.

It's recommended to have IPS rule with client-side exploitation protection
policy for user network with allowed outgoing. And similar policy with server
side protection for any incoming firewall rules from WAN zone.
```

Remediation:

```
Navigate to `Rules and policies > Firewall rules`.


Navigate to configured firewall rules. Set `Detect and prevent exploits
(IPS)` with appropriate IPS rule based on the direction of the traffic.
Configure IPS policy with gerenalpolicy, lantowan_strict, lantowan_general,
dmzpolicy, LAN TO WAN, LAN TO DMZ, WAN TO DMZ, WAN TO LAN, DMZ TO WAN, DMZ TO
LAN or “custom IPS rule”.
```

```
Set IPS rule with client-side exploitation protection policy for user network
with outgoing allowed. And similar policy with server side protection for any
incoming firewall rules from WAN zone.
```

Default Value:

Not configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/concepts/IPSPolicies.html

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

12.7 Deploy Network-Based Intrusion Prevention Systems
Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.

5.5 Ensure Web Application Firewall (WAF) is configured with appropriate protection policies in all the WAF rules in use (Manual)

Profile Applicability:

- Level 2

Description:

XG firewall protects web servers against Layer 7 (application) vulnerability exploits. These attacks include cookie, URL, and form manipulation. It can also mitigate common threats such as application and cross-site scripting (XSS) attacks. XG firewall provides default policies for some common web services.

Rationale:

XG firewall's Web Application Firewall (WAF) feature protects web servers deployed in a network and related applications from any underlying vulnerability exploits. It protects applications accessed via HTTP and HTTPS at the layer-7 Application Layer. Besides Layer 7 based attacks, the web server is safeguarded against cookie tampering, forceful browsing, and hidden field tampering. The WAF also mitigates user-induced vulnerabilities in applications that leave web applications open to attacks, such as cross-site scripting, directory traversal, and forced URL browsing.

Audit:

```
Navigate to `Protect > Web server > General settings > SlowHTTP protection
settings`.

Verify that `Time-out for request headers` is `ON`.


Verify the minimum amount of time to receive a request `Soft limit` is set to
optimal configuration. Default setting is `10`.


Verify the maximum amount of time to receive the request header `Hard limit`
is set to optimal configuration. Default setting is `30`.


Verify the amount of data, in bytes, to extend the time-out set by the soft
limit. Every time the rate is exceeded, the soft limit is increased by one
second. The default extension rate is `5000`.


Verify that `TLS version settings > TLS version` is set to TLS 1.2. Select
the minimum TLS version that is allowed to connect to the WAF. Note that if
TLS version 1.2 is selected, clients like Microsoft Internet Explorer 8 or
```

earlier and those running on Window XP won’t be able to connect to the WAF.

Navigate to the configure WAF rules `Rules and policies > Firewall rules`, filter `Rule type > WAF`. Verify under `Advanced > Protection > edit protection policy` to check `Mode` is set to `Reject`.

Verify that `Cookie signing` is set to `ON`.

Verify that `Static URL hardening` is set to `ON` with specify the URLs you want to serve. Note that this feature isn’t effective for dynamic URLs created by the client, for example, using JavaScript.

Verify that `Form hardening` is set to `ON`.

Verify that `Antivirus` is set to `ON` with `Mode` set to either `Sophos` or `Dual scan`. And Direction of the scanning is set to `Uploads and Downloads`.

Verify that `Block unscannable content` is set to `ON`.

Verify that `Block clients with bad reputation` is set to `ON`.

Verify that `Common threat filter` is set to `ON`. And confirm that these rule IDs (901100,901110,949100,949190,949110,959100,980100,980110,980120,980130,980140) are not added to the Skip filter rules.

Verify that `Application attacks` is checked.

Verify that `SQL injection attacks` is checked.

Verify that `XSS attacks` is checked.

Verify that `Protocol enforcement` is checked.

Verify that `Scanner detection` is checked.

Verify that `Data leakage` is checked.

Within the configured firewall rule with WAF verify that Intrusion prevention is set to either `WAN TO LAN` or `WAN TO DMZ` or custom IPS rule with target server platform.

Remediation:

Navigate to `Protect > Web server > General settings > SlowHTTP protection settings`.

Set `Time-out for request headers` to `ON`.

Set the minimum amount of time to receive a request `Soft limit` to optimal configuration. Default setting is `10`.

Set the maximum amount of time to receive the request header `Hard limit` to optimal configuration. Default setting is `30`.

Set the amount of data, in bytes, to extend the time-out set by the soft limit. Every time the rate is exceeded, the soft limit is increased by one second. The default extension rate is `5000`.

Set `TLS version settings > TLS version` to TLS 1.2. Select the minimum TLS version that is allowed to connect to the WAF. Note that if TLS version 1.2 is selected, clients like Microsoft Internet Explorer 8 or earlier and those running on Window XP won’t be able to connect to the WAF.

Navigate to the configure WAF rules `Rules and policies > Firewall rules`, filter `Rule type > WAF`. Under `Advanced > Protection > edit protection policy` set `Mode` to `Reject`.

Set `Cookie signing` to `ON`.

Set `Static URL hardening` to `ON` with specify the URLs you want to serve. Note that this feature isn’t effective for dynamic URLs created by the client, for example, using JavaScript.

Set `Form hardening` to `ON`.

Set `Antivirus` to `ON` with scanning `Mode` to either `Sophos` or `Dual scan`. And Direction of the scanning is set to `Uploads and Downloads`.

Set `Block unscannable content` to `ON`.

Set `Block clients with bad reputation` to `ON`.

Set `Common threat filter` to `ON`. Remove these rule IDs (901100,901110,949100,949190,949110,959100,980100,980110,980120,980130,980140) added to the Skip filter rules.

Set `Application attacks` to enable.

Set `SQL injection attacks` to enable.

Set `XSS attacks` to enable.

Set `Protocol enforcement` to enable.

Set `Scanner detection` to enable.

Set `Data leakage` to enable.

Within the configured firewall rule with WAF verify that Intrusion prevention is set to either `WAN TO LAN` or `WAN TO DMZ` or custom IPS rule with target server platform.

Default Value:

Not configured.

References:

1. https://support.sophos.com/support/s/article/KB-000036712?language=en_US
2. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/tasks/WAFProtectionPolicyAdd.html
3. https://support.sophos.com/support/s/article/KB-000036242?language=en_US
4. https://support.sophos.com/support/s/article/KB-000035562?language=en_US
5. https://support.sophos.com/support/s/article/KB-000035559?language=en_US
6. https://support.sophos.com/support/s/article/KB-000036412?language=en_US
7. https://support.sophos.com/support/s/article/KB-000035560?language=en_US

CIS Controls:

Version 6

9.6 Deploy And Configure Application Firewalls
Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.

Version 7

8 Malware Defenses
Malware Defenses

5.6 Ensure Email protection is configured with appropriate protection policies (Manual)

Profile Applicability:

- Level 2

Description:

Create one or more Email protection policy to handle email routing and protect domains and mail servers. You can configure SMTP/S, POP/S, and IMAP/S policies with SPAM and malware checks, data protection, and Email encryption.

Rationale:

By scanning both inbound and outbound Email traffic, the threat of malware delivered through Emails and data exfiltration can be prevented at the gateway firewall. Per domain policy allows unrestricted configuration based on security needs. Appropriate Email protection policy enforces TLS, SMTP DoS and other security settings for incoming and outgoing emails.

Audit:

```
Navigate to `Protect > Email > General settings`. Verify that appropriate
`SMTP deployment mode` is used. Note that `legacy mode` is not compatible
with Sandstorm for Email.


Navigate to `SMTP settings`.


Verify that `Reject based on IP reputation`. XG Firewall checks the sender's
IP reputation before the spam checks specified in the SMTP policy.


Verify that `SMTP DoS settings` is Enable. XG Firewall protects the network
from SMTP denial-of-service attacks.


Navigate to `SMTP TLS configuration`. Verify that `Disable legacy TLS
protocols` is Enable. To overcome TLS vulnerabilities, it is recommended to
turn off legacy TLS protocols.


Navigate to `POP and IMAP TLS configuration`. Verify that `Disable legacy TLS
protocols` is Enable.


Navigate to `Malware protection`. Verify that `Primary antivirus engine` is
```

set to `Sophos`. If `Avira` is selected XG Firewall will turn off Sandstorm in SMTP policies with single antivirus scan.

Navigate to `DKIM verification`. Verify that DKIM verification is `ON` and `DKIM verification failed`, `Invalide DKIM signature`, `No DKIM signature found` should be set to `Quarantine` or `Reject`. With DKIM XG validates the source domain name and message integrity through cryptographic authentication, preventing email spoofing. DKIM verification is applied to inbound emails. Note that XG Firewall quarantines DKIM-signed emails that use RSA SHA-1 or have key length less than 1024 or more than 2048 bits.

Navigate to `Protect > Email > Relay settings > Host based relay`. Verify that `ANY` is not added to the `allow relay from hosts/networks`. Adding `ANY` will result in an open relay, allowing anyone on the internet to send emails through XG Firewall.

Navigate to `Protect > Email > Policy & exceptions`. Verify the configured SMTP policy `Malware protection > Selected antivirus action` is set to `Drop` and `Quarantine unscannable content` is checked and `Detect zero-day threats with Sandstorm Scanned file size` is set to 10 MB.

Remediation:

Navigate to `Protect > Email > General settings`. Set the appropriate `SMTP deployment mode` to `MTA mode` when possible. `legacy mode` is not compatible with Sandstorm for Email and reduce the security effectiveness.

Navigate to `SMTP settings`.

Set `Reject based on IP reputation` to Enable. XG Firewall checks the sender's IP reputation before the spam checks specified in the SMTP policy.

Set `SMTP DoS settings` to Enable. XG Firewall protects the network from SMTP denial-of-service attacks.

Navigate to `SMTP TLS configuration`. Set `Disable legacy TLS protocols` to Enable. To overcome TLS vulnerabilities, it is recommended to turn off legacy TLS protocols.

Navigate to `POP and IMAP TLS configuration`. Set `Disable legacy TLS protocols` to Enable.

Navigate to `Malware protection`. Set `Primary antivirus engine` to `Sophos`. If `Avira` is selected XG Firewall will turn off Sandstorm in SMTP policies with single antivirus scan.

Navigate to `DKIM verification`. Set `DKIM verification` to `ON` and `DKIM

```
verification failed`, `Invalide DKIM signature`, `No DKIM signature found`
are set to `Quarantine` or `Reject`. With DKIM XG validates the source domain
name and message integrity through cryptographic authentication, preventing
email spoofing. DKIM verification is applied to inbound emails. Note that XG
Firewall quarantines DKIM-signed emails that use RSA SHA-1 or have key length
less than 1024 or more than 2048 bits.


Navigate to `Protect > Email > Relay settings > Host based relay`. Remove
`ANY` from the `allow relay from hosts/networks`. Adding `ANY` will result in
an open relay, allowing anyone on the internet to send emails through XG
Firewall. Set only the specified host or enable authenticated relay.

Navigate to `Protect > Email > Policy & exceptions`. Set the configured SMTP
policy `Malware protection > Selected antivirus action` to `Drop` and
`Quarantine unscannable content` is checked and `Detect zero-day threats with
Sandstorm Scanned file size` is set to 10 MB.
```

Default Value:

Not configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/learningContents/Email_ProtectEmailsMTA.html

CIS Controls:

Version 7

8 Malware Defenses
Malware Defenses

5.7 Ensure DoS & Spoof Protection is enabled with the appropriate settings (Manual)

Profile Applicability:

- Level 1

Description:

Enable SYN/TCP/UDP Flood protection for source and destination networks with appropriate threshold for Flood protection which depend highly on the environment and device used. Default packet/minutes or packet/seconds value may not be appropriate for all the environment and understanding of traffic patterns on the specific environment may be required to set accurate threshold.

Enable Spoof protection to drop the packet if the source IP address of a packet does not match any entry on the firewall's routing table or if the packet is not from a direct subnet.

Rationale:

DoS/DDoS attacks where the CPU and memory buffers of the victim device becomes overwhelmed by incomplete sessions. Many attacks can be successfully mitigated against resources protected by firewall or firewall itself.

Impact:

Organization may expose to both internal and external DoS and reconnaissance attacks. Malicious traffic flooding and malware communication can cause network congestion and consuming valuable network resources.

Audit:

```
Navigate to `Protect > Intrusion Prevention > DoS & Spoof Protection`
Verify that `Enable spoof prevention` is checked on LAN and DMZ zones.

Verify that `Apply Flag` is checked on `SYN flood`, `UDP flood`, `TCP flood`,
`ICMP/ICMPv6` flood on both Source and Destination.

Verify that `Apply Flag` is checked on `Dropped source routed packets`,
`Disable ICMP/ICMPv6 redirect packet`, `ARP hardening` on Destination.

Verify that `DoS bypass rule` is not added with wide range of source or
destination networks that will reduce integrity of overall DoS protection.
```

Remediation:

```
Navigate to `Protect > Intrusion Prevention > DoS & Spoof Protection`
Set `Enable spoof prevention` is checked on LAN and DMZ zones.

Set `Apply Flag` is checked on `SYN flood`, `UDP flood`, `TCP flood`,
`ICMP/ICMPv6` flood on both Source and Destination.

Set `Apply Flag` is checked on `Dropped source routed packets`, `Disable
ICMP/ICMPv6 redirect packet`, `ARP hardening` on Destination.

Validate `DoS bypass rule` is not added with wide range of source or
destination networks that will reduce integrity of overall DoS protection.
```

Default Value:

Not Configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/IPSDoSAndSpoofProtection.html
2. https://support.sophos.com/support/s/article/KB-000035754?language=en_US

CIS Controls:

Version 7

12 Boundary Defense
Boundary Defense

5.8 Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone (Manual)

Profile Applicability:

- Level 1

Description:

Window service ports directly accessible from WAN zone could lead to bruteforce attempts, wormable attacks and other unpatched vulnerabilities.

Unencrypted protocols that could potentially impact confidentiality, integrity and availability shouldn't be directly accessible from the WAN Zone.

Rationale:

Any allowed rules with port-forwarding (DNAT) enabled to access internal Window services such as (TCP/UDP 445,137-139,3389) and other unencrypted protocols (TCP/UDP 21,23,113,135,513,389,1433,5800,5900) could lead to potential compromise or data leakage.

Impact:

Directly accessible ports to the internal servers open bigger attack surface for the adversary. For example, allowing Port 3389 RDP from internet could lead to unpatched vulnerability such as Bluekeep CVE-2019-0708, vulnerability known to associate with WannaCry ransomware.

Audit:

```
Navigate to `Rules and policies > Firewall rules`.
Verify the `Firewall rules` with `Source zone` `WAN` with service ports
`TCP/UDP 445,137-139,3389,21,79,23,113,135,513,389,1433,5800,5900` exists in
the allowed rules.
```

Remediation:

```
Navigate to `Rules and policies > Firewall rules`.
Disable or only allow with specific source IP address in `Firewall rules`
with `Source zone` `WAN` with service ports `TCP/UDP 445,137-
139,3389,21,79,23,113,135,513,389,1433,5800,5900`. When absolute necessary to
allow access from Internet, consider the use of VPN.
```

Default Value:

Not Configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/learningContent/RulesPoliciesCreateDNATAndFirewallRulesForInternalServers.html?hl=dnat

CIS Controls:

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

12 Boundary Defense
Boundary Defense

5.9 Ensure Wireless Protection is configured with secure configuration (Manual)

Profile Applicability:

- Level 1

Description:

When XG firewall is used as Wireless controller to manage Sophos Access Points, it is important to tighten configuration to prevent unauthorized access to the Wireless network.

Rationale:

By providing wireless connectivity to the clients, it creates potential attack surface to the wireless users as well as the local network. Important configurations such as security mode, method of handling traffic should be considered before providing the Wireless access.

Impact:

Authentication with weaker encryption algorithm could lead to compromising encryption keys and unauthorized access to both Wireless and local network. Due to availability and lack of physical access control to Wireless network, it is important to tighten security settings.

Audit:

```
Navigate to `Wireless > Wireless networks`
Verify the existing `Wireless` settings with `Security mode`, either `WPA2
Personal` or `WPA2 Enterprise` should be used.

Under `Advanced settings`
Verify that `Encryption` is set to `AES[secure]`
Verify that `Time-based access` is `Enable` with `Select active time` and
appropriate schedule to limit the availability.

Verify that `Client isolation` is `Enabled`.
```

Remediation:

```
Navigate to `Wireless > Wireless networks`
Set the existing `Wireless` settings with `Security mode`, either `WPA2
Personal` or `WPA2 Enterprise`.

Under `Advanced settings`
Set `Encryption` to `AES[secure]`
Set `Time-based access` to `Enable` with `Select active time` and configure
appropriate schedule to limit the availability.

Set `Client isolation` to `Enabled`.
```

Default Value:

Not Configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/concepts/WirelessNetworks.html?hl=wireless

CIS Controls:

Version 7

15 Wireless Access Control
Wireless Access Control

5.10 Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from `WAN` Zone (Manual)

Profile Applicability:

- Level 1

Description:

Allowed firewall rules with no specific source or ANY service definitions from WAN/untrusted zone could lead to unintended exposure to the outside threats.

Rationale:

Limit the unintended exposure to systems and services. Allowed rules from WAN zone should be created with very specific source network or GEO IP and targeted service definition to the internal host.

On top of the allowed policy, there should be IPS rule enabled with WAN to LAN or WAN to DMZ profile.

Impact:

Having a allowed firewall rule 'ANY' to 'ANY' with no layer-7 threats protections could lead to threat exposure of unpatched systems, bruteforce attempts and denial of service etc.

Audit:

```
Navigate to `Protect > Rules and policies > Firewall rules`.
Filter `Destination zone` to `LAN` or `DMZ`.

Verify that no allowed firewall rules from `WAN` zone with service definition
`ANY` to `LAN` or `DMZ` zone with destination network set to `ANY`.
```

Remediation:

```
Navigate to `Protect > Rules and policies > Firewall rules`.
Filter `Destination zone` to `LAN` or `DMZ`.

Remove allowed firewall rules from `WAN` zone with service definition `ANY`
to `LAN` or `DMZ` zone with destination network set to `ANY`. Or change the
rule to specific source/destination with target service definition.
```

Default Value:

Not Configured.

References:

1. https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/sfos/concepts/FirewallRules.html?hl=firewall%2Crules

CIS Controls:

Version 6

9.1 Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Version 7

9.2 Ensure Only Approved Ports, Protocols and Services Are Running
Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Device Setup And Administration**		
1.1	**General Settings**		
1.1.1	Ensure admin session 'lock', 'logout' for inactivity and 'block' is configured for failed sign-in (Automated)	□	□
1.1.2	Ensure login disclaimer is set (Automated)	□	□
1.1.3	Ensure NTP servers are configured appropriately (Automated)	□	□
1.1.4	Ensure SSL server certificate for remote SSL VPN is configured correctly (Manual)	□	□
1.1.5	Ensure password complexity check is enabled (Automated)	□	□
1.1.6	Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone (Automated)	□	□
1.1.7	Ensure valid certificate is set for web browser used to access Webadmin interface (Automated)	□	□
1.2	**SNMP & Device Notification Settings**		
1.2.1	Ensure SNMPv3 is selected for queries and traps (Manual)	□	□
1.2.2	Ensure notification is configured to send system and security events (Manual)	□	□
2	**User Identification & Authentication**		
2.1	Ensure Firewall rules are configured to identify users before authorizing access (Manual)	□	□
2.2	Ensure Encrypted connection is used in connecting external Active Directory and LDAP (Manual)	□	□
3	**System Services, Firmware and Updates**		
3.1	Ensure "Fully Synchronized" High Availability peer is configured (Manual)	□	□
3.2	Ensure 'Pattern updates' is set to download and install updates every 15 minutes (Manual)	□	□
3.3	Ensure ‘Hotfix’ is set to ‘Allow Automatic Installation of hotfixes’ (Manual)	□	□
3.4	Ensure XG takes encrypted backup of the configuration and send to designated email address with scheduled frequency (Manual)	□	□
3.5	Ensure No Expired Subscription Licenses (Manual)	□	□
3.6	Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode" (Manual)	□	□

3.7	Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server (Manual)	□	□
4	**Advanced Threat & Synchronised Security**		
4.1	Ensure 'Enable advanced threat protection' is set to ‘ON’ and Policy is set to ‘Log and drop’ (Manual)	□	□
4.2	Ensure Sandstorm is enabled at the firewall rule for web protection and does not exclude any file type from Sandstorm analysis (Manual)	□	□
4.3	Ensure Sandstorm is enabled for Email Protection and set to MTA mode (Manual)	□	□
4.4	Ensure Synchronised Security Heartbeat is enforced on Firewall Rules (Manual)	□	□
5	**Protection Rules And Profiles**		
5.1	Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly. (Manual)	□	□
5.2	Ensure SSL/TLS inspection rules is enabled to all relevant firewall policies (Manual)	□	□
5.3	Ensure Application filter is set to block high risk (Risk Level 4 and 5) applications (Manual)	□	□
5.4	Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules (Manual)	□	□
5.5	Ensure Web Application Firewall (WAF) is configured with appropriate protection policies in all the WAF rules in use (Manual)	□	□
5.6	Ensure Email protection is configured with appropriate protection policies (Manual)	□	□
5.7	Ensure DoS & Spoof Protection is enabled with the appropriate settings (Manual)	□	□
5.8	Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone (Manual)	□	□
5.9	Ensure Wireless Protection is configured with secure configuration (Manual)	□	□
5.10	Ensure No Firewall Rules with source \`ANY\`, service \`ANY\` and destination \`ANY\` from \`WAN\` Zone (Manual)	□	□

Appendix: Change History

Date	Version	Changes for this version