

Cysurance – Warrantied Events & Mitigating Requirements

Table of Contents

| | |
|--|-----------|
| <i>Introduction</i> | 2 |
| <i>Minimum Non-Configuration Requirements</i> | 2 |
| Operating System (OS) Versions and Updates | 2 |
| Take & Store a Configuration Snapshot | 3 |
| License and Enable Security Services | 4 |
| <i>Recommendations</i> | 6 |
| Audit & System Log Export and Archives | 6 |
| Enable Other Security Services | 6 |
| Consider Best Practices & Other Published Guidelines..... | 8 |
| <i>Warrantied Events & Configurations</i> | 8 |
| Unauthorized Remote Access | 8 |
| SSL/TLS VPN (Client or Clientless – If Applicable) | 8 |
| SSH (If Applicable) | 13 |
| IPSEC VPN (If Applicable) | 15 |
| ZTNA with CSE (If Applicable)..... | 16 |
| Software Vulnerability Exploitation | 17 |
| Enable the Intrusion Prevention Service (IPS) | 17 |
| Enable Relevant IPS Signatures | 18 |
| Enable Firewall Access Rules..... | 18 |
| Non-volumetric DDOS Attack | 19 |
| Intrusion Prevention Service (IPS)..... | 19 |
| Control Plane Flood Protection | 20 |
| Data Flood Protection..... | 21 |
| UDP Flood Protection..... | 21 |
| ICMP Flood Protection..... | 22 |
| TCP Flood Protection..... | 22 |
| GEO-IP Filter | 23 |
| GEO-IP Country Recommendations | 24 |
| Botnet Filter | 24 |
| <i>Additional Mitigating Requirements</i> | 25 |
| Access/Admin Port Changes | 25 |
| Cloud Backups | 28 |
| Periodic Diagnostic Reporting..... | 28 |

Introduction

This document introduces the events SonicWall will warrant against and provides configuration guidance for success mitigation. Configuration instructions and graphics reflect SonicOS 7.1.2-7019 as of November 7, 2024. This document, dated 19 June 2025, specifies the maximum timeframe of **30 days** for applying OS updates (unavoidable exceptions to this policy must be addressed with SonicWall and Cysurance on a case-by-case basis).

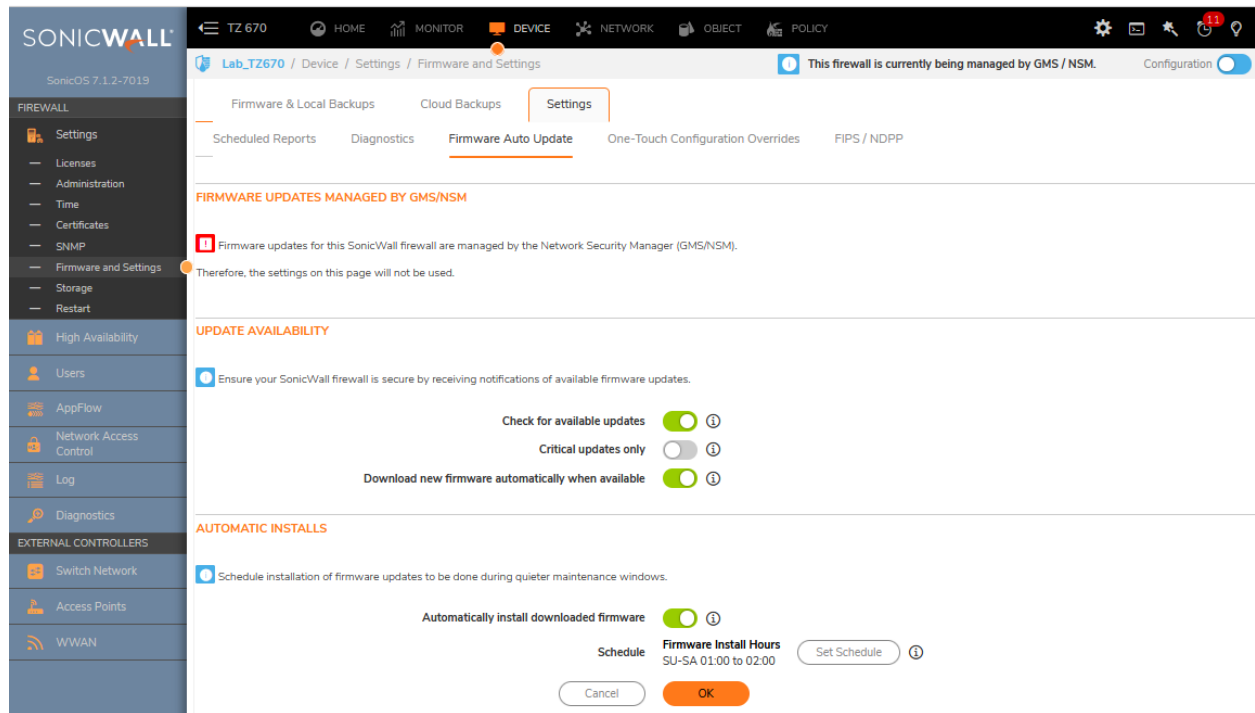
Minimum Non-Configuration Requirements

Qualifying firewalls must be configured according to this guide. Additional requirements include applying Operating System (OS) updates and patches as soon as possible (but within 30 days of release) and taking an initial 'snapshot' of the configured firewall by exporting and saving a Tech Support Report (TSR). This TSR will be required to file a claim, so safeguard it! Finally, a qualifying firewall must be licensed for security services and running, at a minimum, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Geo-IP Filter, and Botnet Filter.

Operating System (OS) Versions and Updates

To qualify for the embedded warranty, firewalls must run the most current OS, patches, and critical updates (installed as soon as possible but within 30 days of release).

Navigate to **Device | Settings | Firmware and Settings | Settings** tab. Enable *Check for available updates* and *Download new firmware automatically when available* in the **UPDATE AVAILABILITY** section, and *Automatically install downloaded firmware* in the **AUTOMATIC INSTALLS** section to have updates applied automatically. The updates can also be scheduled.



Take & Store a Configuration Snapshot

After initially configuring the firewall according to this configuration guide, configure and export a TSR.

1. Navigate to **Device | Diagnostics | Tech Support Report**.
2. Enable the following options at a minimum under the **CONFIGURE** section:
 - a. ARP Cache
 - b. DHCP Bindings
 - c. IKE Info
 - d. List of current users
 - e. DNS Proxy Cache
 - f. Inactive users
 - g. Detail of users
 - h. IP Stack Info
 - i. Geo-IP/Botnet Cache
 - j. User Name
 - k. Debug info in report
 - l. IP Report
 - m. Application Signatures
3. Download and save a TSR report by selecting *Download Tech Support Report* in the **ACTIONS** section.

SONICWALL TZ 670 HOME MONITOR **DEVICE** NETWORK OBJECT POLICY

Lab_TZ670 / Device / Diagnostics / Tech Support Report

This firewall is currently being managed by GMS / NSM. Configuration

TECH SUPPORT REPORT

Automatic secure crash analysis reporting ☒

Periodic secure diagnostic reporting for support purposes ☒

Time Interval (minutes) 1440

CSC Reporting Time Interval (minutes) 15

Include raw flow table data entries when sending diagnostic report ☐

CONFIGURE

| | | |
|---|---|--|
| Sensitive Keys <input type="checkbox"/> | Inactive users <input checked="" type="checkbox"/> | Extra Routing Info <input type="checkbox"/> |
| ARP Cache <input checked="" type="checkbox"/> | Detail of users <input checked="" type="checkbox"/> | Vendor Name Resolution <input type="checkbox"/> |
| DHCP Bindings <input checked="" type="checkbox"/> | IP Stack Info <input checked="" type="checkbox"/> | Debug info in report <input checked="" type="checkbox"/> |
| IKE Info <input checked="" type="checkbox"/> | IPv6 NDP <input type="checkbox"/> | IP Report <input checked="" type="checkbox"/> |
| List of current users <input checked="" type="checkbox"/> | IPv6 DHCP <input type="checkbox"/> | ABR Entries <input type="checkbox"/> |
| DNS Proxy Cache <input checked="" type="checkbox"/> | Geo-IP/Botnet Cache <input checked="" type="checkbox"/> | Application Signatures <input checked="" type="checkbox"/> |
| Wireless Diagnostics <input type="checkbox"/> | User Name <input checked="" type="checkbox"/> | |

Cancel Accept

ACTIONS

Download System Logs Download Tech Support Report Download SSO Auth Log Send Diagnostic Reports To Support

License and Enable Security Services

Qualifying firewalls must have a current security services subscription with Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Geo-IP Filter, and Botnet Filter services enabled, at minimum.

1. Gateway Anti-Virus: Navigate to **Policy | Security Services | Gateway Anti-Virus**, enabling the service and setting configuration toggles according to the diagram below.
2. Anti-Spyware: Navigate to **Policy | Security Services | Anti-Spyware**, enabling the service and setting configuration toggles according to the diagram below.
3. Intrusion Prevention: Navigate to **Policy | Security Services | Intrusion Prevention**, enabling the service and configuring it according to this guide's *Non-Volumetric DDOS Attack* section.
4. Geo-IP Filter: Navigate to **Policy | Security Services | Geo-IP Filter**, enabling the service and configuring it according to this guide's *Non-Volumetric DDOS Attack* section.
5. Botnet Filter: Navigate to **Policy | Security Services | Botnet Filter**, enabling the service and configuring it according to this guide's *Non-Volumetric DDOS Attack* section.

SonicOS 7.1.2-7019

Rules and Policies

Access Rules

NAT Rules

Routing Rules

DNS Rules

Content Filter Rules

App Rules

Endpoint Rules

DPI-SSL

DPI-SSH

Security Services

Summary

Gateway Anti-Virus

Anti-Spyware

Intrusion Prevention

Geo-IP Filter

Botnet Filter

App Control

Content Filter

Anti-Spam

Capture ATP

DNS Security

Endpoint Security

TZ 670

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

Lab_TZ670 / Policy / Security Services / Gateway Anti-Virus

This firewall is currently being managed by GMS / NSM.

Configuration

Status / Settings

Signatures

Enable the Gateway Anti-Virus per zone from the [Object > Match Objects > Zones](#) page.

Gateway Anti-Virus

Cloud Anti-Virus

STATUS

Signature Database

Downloaded

Last Checked

12/24/2024 15:27:320

Signature Database Timestamp

UTC 12/24/2024 09:41:58.000

Gateway Anti-Virus Expiration Date

08/23/2026

GLOBAL SETTINGS

Enable Gateway Anti-Virus

Configure

| # | PROTOCOLS | ENABLE INBOUND INSPECTION | ENABLE OUTBOUND INSPECTION |
|---|--------------|---------------------------|----------------------------|
| 1 | HTTP | | |
| 2 | FTP | | |
| 3 | IMAP | | |
| 4 | SMTP | | |
| 5 | POP3 | | |
| 6 | CIFS NETBIOS | | |
| 7 | TCP STREAM | | |

Total: 7 item(s)

Cancel

Accept

SonicOS 7.1.2-7019

Rules and Policies

Access Rules

NAT Rules

Routing Rules

DNS Rules

Content Filter Rules

App Rules

Endpoint Rules

DPI-SSL

DPI-SSH

Security Services

Summary

Gateway Anti-Virus

Anti-Spyware

Intrusion Prevention

Geo-IP Filter

Botnet Filter

App Control

Content Filter

Anti-Spam

Capture ATP

DNS Security

Endpoint Security

TZ 670

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

Lab_TZ670 / Policy / Security Services / Anti-Spyware

This firewall is currently being managed by GMS / NSM.

Configuration

Status/Settings

Signatures

Enable the Anti-Spyware per zone from the [Object > Match Objects > Zones](#) page.

ANTI-SPYWARE STATUS

Signature Database

Downloaded

Signature Database Timestamp

UTC 12/19/2024 17:12:20.000

Last Checked

12/24/2024 15:27:320

Anti-Spyware Expiration Date

08/23/2026

ANTI-SPYWARE GLOBAL SETTINGS

Enable Anti-Spyware

Configure

Reset

| SIGNATURE GROUPS | PREVENT ALL | DETECT ALL | LOG REDUNDANCY FILTER (SECONDS) |
|-------------------------|-------------|------------|---------------------------------|
| High Priority Spyware | | | 0 |
| Medium Priority Spyware | | | 0 |
| Low Priority Spyware | | | 0 |

| PROTOCOLS | HTTP | FTP | IMAP | SMTP | POP3 |
|---------------------------|------|-----|------|------|------|
| Enable Inbound Inspection | | | | | |

Enable Inspection of Outbound Spyware Communication

Cancel

Accept

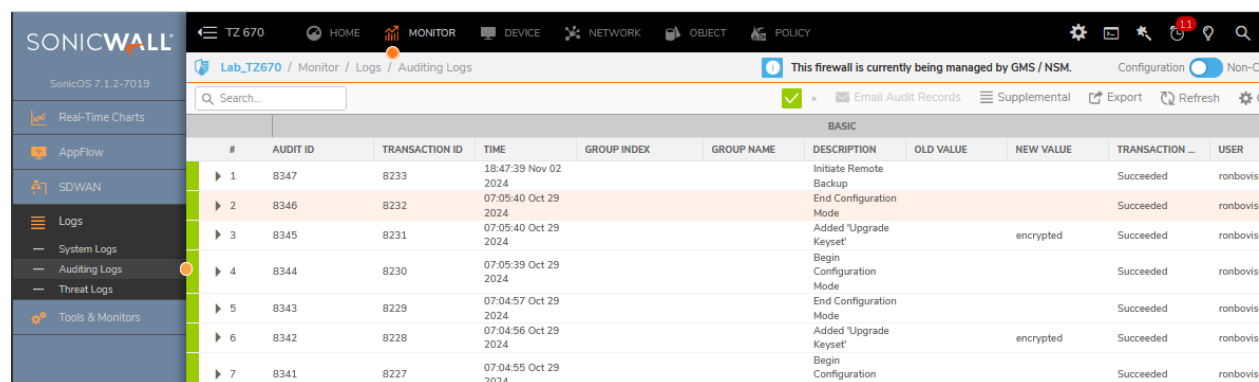
Recommendations

Besides implementing minimum requirements and configurations, consider other strongly advised recommendations. If followed, they should provide additional security for a qualifying firewall and aid in filing a claim if necessary. These recommendations include exporting and archiving Audit and System log files, enabling additional security services, incorporating additional security services, and implementing best practices from SonicWall sources such as Knowledge-Based (KB) articles. **Note:** Consider, test, and apply configuration changes carefully, as SonicWall isn't responsible for the outcome.

Audit & System Log Export and Archives

Current Audit and System logs will be required when filing a claim. Providing additional Audit and System logs that extend the reporting period may improve the chances of filing a successful claim. Doing this requires exporting and archiving Audit and System logs, ideally at a regular cadence (e.g., once a week). **Note:** Archiving logs may require additional storage capacity or a central repository.

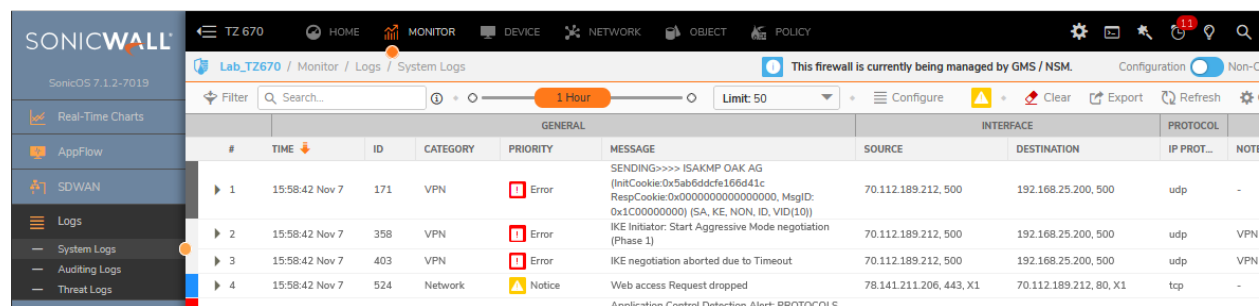
To export Audit logs: Navigate to **Monitor | Logs | Auditing Logs** and select *Export*.



The screenshot shows the SonicWall management interface. The top navigation bar includes 'TZ 670', 'HOME', 'MONITOR' (selected), 'DEVICE', 'NETWORK', 'OBJECT', and 'POLICY'. Below the navigation bar, the breadcrumb trail is 'Lab_TZ670 / Monitor / Logs / Auditing Logs'. A status message indicates 'This firewall is currently being managed by GMS / NSM.' and 'Configuration Non-C'. The left sidebar shows 'Real-Time Charts', 'AppFlow', 'SDWAN', 'Logs' (selected), 'System Logs', 'Auditing Logs', 'Threat Logs', and 'Tools & Monitors'. The main content area displays a table of auditing logs with columns: #, AUDIT ID, TRANSACTION ID, TIME, GROUP INDEX, GROUP NAME, DESCRIPTION, OLD VALUE, NEW VALUE, TRANSACTION, and USER. The table contains 7 entries, all with a status of 'Succeeded' and user 'ronbovis'.

| # | AUDIT ID | TRANSACTION ID | TIME | GROUP INDEX | GROUP NAME | DESCRIPTION | OLD VALUE | NEW VALUE | TRANSACTION | USER |
|---|----------|----------------|----------------------|-------------|------------|--------------------------|-----------|-----------|-------------|----------|
| 1 | 8347 | 8233 | 18:47:39 Nov 02 2024 | | | Initiate Remote Backup | | | Succeeded | ronbovis |
| 2 | 8346 | 8232 | 07:05:40 Oct 29 2024 | | | End Configuration Mode | | | Succeeded | ronbovis |
| 3 | 8345 | 8231 | 07:05:40 Oct 29 2024 | | | Added 'Upgrade Keyset' | | encrypted | Succeeded | ronbovis |
| 4 | 8344 | 8230 | 07:05:39 Oct 29 2024 | | | Begin Configuration Mode | | | Succeeded | ronbovis |
| 5 | 8343 | 8229 | 07:04:57 Oct 29 2024 | | | End Configuration Mode | | | Succeeded | ronbovis |
| 6 | 8342 | 8228 | 07:04:56 Oct 29 2024 | | | Added 'Upgrade Keyset' | | encrypted | Succeeded | ronbovis |
| 7 | 8341 | 8227 | 07:04:55 Oct 29 2024 | | | Begin Configuration | | | Succeeded | ronbovis |

To export System logs: Navigate to **Monitor | Logs | System Logs** and select *Export*. **Note:** Selecting *Configure* on the menu bar will allow you to configure what system events are logged, and



The screenshot shows the SonicWall management interface. The top navigation bar is the same as the previous screenshot. The breadcrumb trail is 'Lab_TZ670 / Monitor / Logs / System Logs'. A status message indicates 'This firewall is currently being managed by GMS / NSM.' and 'Configuration Non-C'. The left sidebar is the same as the previous screenshot. The main content area displays a table of system logs with columns: #, TIME, ID, CATEGORY, PRIORITY, MESSAGE, SOURCE, DESTINATION, IP PROT..., and NOTI. The table contains 4 entries, all with a status of 'Error' or 'Notice' and user 'ronbovis'.

| # | TIME | ID | CATEGORY | PRIORITY | MESSAGE | SOURCE | DESTINATION | IP PROT... | NOTI |
|---|----------------|-----|----------|----------|---|-------------------------|------------------------|------------|------|
| 1 | 15:58:42 Nov 7 | 171 | VPN | Error | SENDING>>>> ISAKMP OAK AG (InitCookie:0x5ab6ddcfe166d41c RespCookie:0x0000000000000000, MagID: 0x1C00000000) [SA, KE, NON, ID, VID(10)] | 70.112.189.212, 500 | 192.168.25.200, 500 | udp | - |
| 2 | 15:58:42 Nov 7 | 358 | VPN | Error | IKE Initiator: Start Aggressive Mode negotiation (Phase 1) | 70.112.189.212, 500 | 192.168.25.200, 500 | udp | VPN |
| 3 | 15:58:42 Nov 7 | 403 | VPN | Error | IKE negotiation aborted due to Timeout | 70.112.189.212, 500 | 192.168.25.200, 500 | udp | VPN |
| 4 | 15:58:42 Nov 7 | 524 | Network | Notice | Web access Request dropped | 78.141.211.206, 443, X1 | 70.112.189.212, 80, X1 | tcp | - |

Enable Other Security Services

Consider enabling additional security services, such as App Control and Content Filter, to further enhance the firewall's ability to secure network environments and resources.

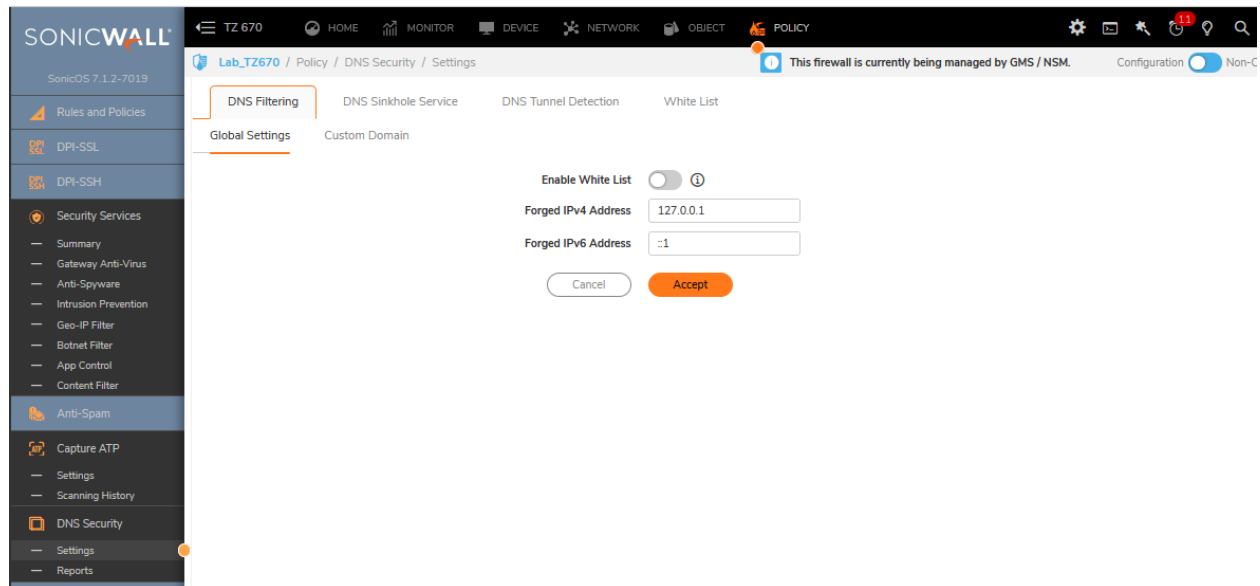
1. App Control: Navigate to **Policy | Security Services | App Control**, enabling the service configuring the service according to the Firewall Administration Guide.

The screenshot shows the SonicWall management interface for the 'App Control' service. The left sidebar lists various security services, with 'App Control' highlighted. The main panel displays the 'Status / Settings' tab. At the top, a notification states 'This firewall is currently being managed by GMS / NSM.' Below this, a message indicates to 'Enable App Control per zone from the Objects > Zones page.' The 'STATUS' section shows the 'App Signature Database' as 'Downloaded', with a timestamp of 'UTC 11/06/2024 14:35:16.000', a 'Last Checked' time of '11/07/2024 10:03:00.736', and an 'App Signature DB Expiration Date' of '08/23/2026'. The 'GLOBAL SETTINGS' section includes three toggle switches: 'Enable App Control' (checked), 'Enable Logging for All Apps' (checked), and 'Enable Filename Logging' (unchecked). A 'Global Log Redundancy filter Interval' is set to '60 seconds'. At the bottom are buttons for 'Configure Settings', 'Reset', 'Cancel', and 'Accept'.

2. Content Filter: Navigate to **Policy | Security Services | Content Filter**, enabling the service and configuring the service according to the Firewall Administration Guide.

The screenshot shows the SonicWall management interface for the 'Content Filter' service. The left sidebar lists various security services, with 'Content Filter' highlighted. The main panel displays the 'SonicWall CFS' configuration page. At the top, a notification states 'This firewall is currently being managed by GMS / NSM.' Below this, the 'Content Filter Type' is set to 'SonicWall CFS'. The 'CFS STATUS' section shows the 'License Status' as 'Licensed', 'Expiration Date' as 'UTC 08/23/2026 00:00:00.000', and 'Server Status' as 'Server is ready'. The 'GLOBAL SETTINGS' section includes a 'Max URL Caches (entries)' field set to '7680', an 'Enable Content Filtering Service' toggle (checked), a 'Block if CFS Server Is Unavailable' toggle (unchecked), and a 'Server Timeout' field set to '5 second(s)'. The 'CFS EXCLUSION' section includes an 'Exclude Administrator' toggle (unchecked) and an 'Excluded Address' dropdown set to 'None'. At the bottom are buttons for 'Cancel' and 'Accept'.

3. DNS Security: Navigate to **Policy | DNS Security | Settings**, enabling the service and configuring the service according to the firewall Administration Guide.



Consider Best Practices & Other Published Guidelines

Explore SonicWall's exhaustive library of guides, best practices, and KB articles to discover other ways to increase security in your environment further: <https://www.sonicwall.com/support>

Warrantied Events & Configurations

Unauthorized Remote Access

Unauthorized remote access happens when a threat actor gains access to a computer, network, or system without proper authorization despite correct configuration of SonicWall firewall protocols and requirements.

The firewall will prevent unauthorized remote access to it and protected network resources as long as access is contained within a virtual private network and properly configured according to this guide. To qualify for this warranty, TLS, SSH, or CSE must secure all access to the firewall.

Protected remote firewall and resource access are possible through an SSL/TLS VPN connection (either by a client such as NetExtender or directly to the firewall's IP address). An IPSEC VPN (usually site-to-site) is another means. Finally, Cloud Secure Edge (CSE) can provide remote access connectivity through a client or the firewall's built-in connector. Regardless of the method, these features and capabilities must be intentionally and carefully configured to mitigate the risk of unauthorized remote access. The following sections provide essential configuration guidance.

SSL/TLS VPN (Client or Clientless – If Applicable)

A SonicWall firewall can be managed directly through a TLS web connection by configuring a browser with the IP address of the firewall appended by the administrative service port. Additionally, users (regardless of any administrative role) can access the firewall and its resources via a firewall-provided portal. This access can be gained through a TLS web connection by configuring a browser with the IP address of the firewall or

through a client such as NetExtender. Methods, policies, privileges, and profiles must be carefully considered and configured, regardless of the user account, to reduce the risk of unauthorized remote access.

1. Ensure the local user password policy is strong (at least 12 characters, a combination of letters, numbers, special characters, unrepeatd passwords, etc.).
 - a. Navigate to **Device | Settings | Administration | Login / Multiple Administrators** tab.
 - b. Under LOGIN SECURITY, set password parameters and apply them to the appropriate administrator role (**Note:** These password constraints also apply to local user accounts). Set other account parameters as necessary to ensure strict control and minimal risk of compromise. Enable or populate these options (see the diagram below for minimum requirements for each):
 - i. Password must be changed every (days)
 - ii. Change password after (hours)
 - iii. Bar repeated passwords for this many changes
 - iv. New password must contain 8 characters different from the old password
 - v. Enforce a minimum password length of
 - vi. Enforce password complexity
 - vii. Upper Case Characters
 - viii. Lower Case Characters
 - ix. Number Characters
 - x. Symbolic Characters
 - xi. Admin/user lockout
 - xii. Local admin/user account lockout

The screenshot displays the SonicWall configuration interface for a device named 'Lab_TZ670'. The left sidebar shows the navigation menu with categories like FIREWALL, High Availability, Users, AppFlow, Network Access Control, Log, and Diagnostics. The main content area is titled 'Lab_TZ670 / Device / Settings / Administration' and shows the 'Login / Multiple Administrators' tab selected. The 'LOGIN SECURITY' section includes various password and lockout settings, many of which are enabled with green toggle switches. The 'MULTIPLE ADMINISTRATORS' section at the bottom shows options for handling preemption by another admin and inter-admin messaging. The interface also includes a top navigation bar with tabs like HOME, MONITOR, DEVICE, NETWORK, OBJECT, and POLICY, and a status bar at the bottom with 'Cancel' and 'Accept' buttons.

SONICWALL TZ 670 HOME MONITOR DEVICE NETWORK OBJECT POLICY

SonicOS 7.1.2-7019

Lab_TZ670 / Device / Settings / Administration

This firewall is currently being managed by GMS / NSM. Configuration Non-C

Firewall Administrator Login / Multiple Administrators SonicOS API Management Login by Certificate

LOGIN SECURITY

Apply these password constraints for

Admin
Other full admin
Limited admin
Guest admin
Other local users
System admin
Crypto admin
Audit admin

Log out the Admin after inactivity of (mins)

Admin/user lockout
Local admin/user account lockout
Log event only without lockout
Failed login attempts before lockout
Lockout Period (mins)

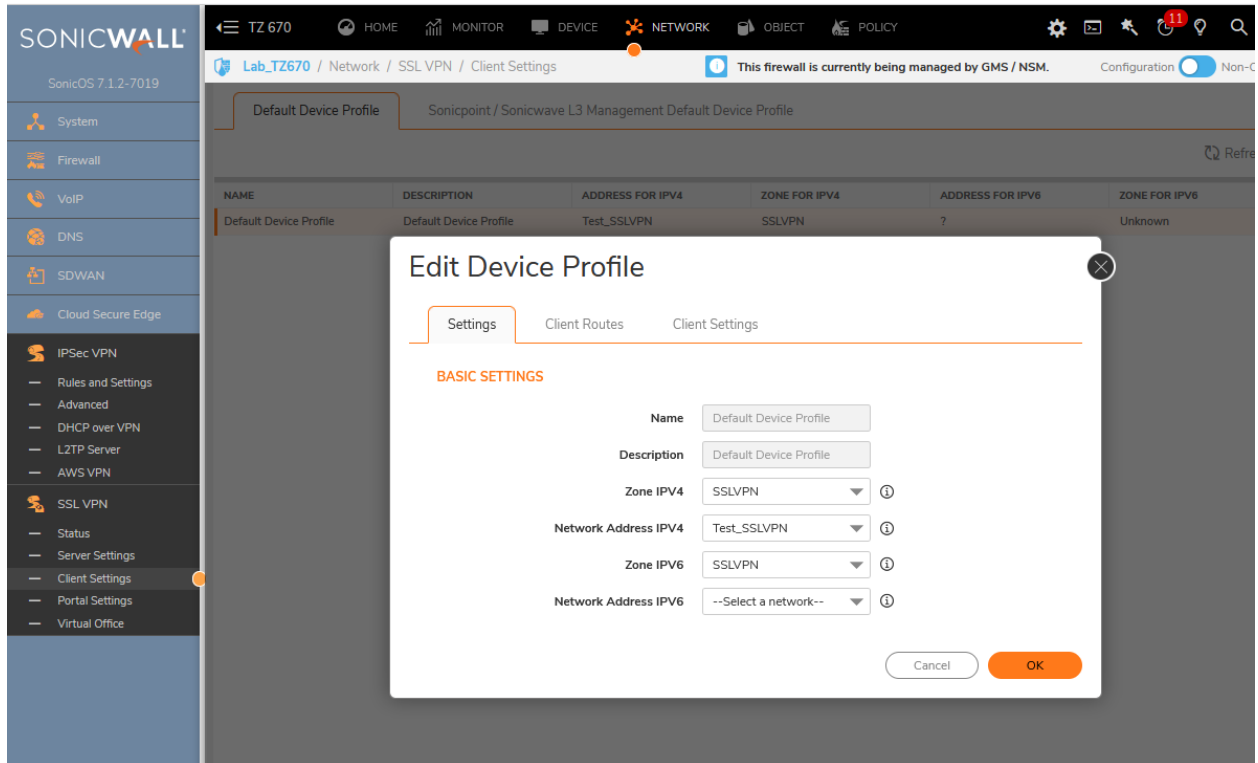
MULTIPLE ADMINISTRATORS

On preemption by another admin
Drop to non-config mode
Log out
Allow preemption by a lower priority admin after inactivity of (mins)

Inter-admin messaging
Messaging polling interval (secs)
Multiple Admin Roles

Cancel Accept

2. Configure SSL VPN user profiles to ensure least-privileged network access.
 - a. Navigate to **Network | SSL VPN | Client Settings | Default Device Profile** tab.
 - b. Edit the Default Device Profile (unless another profile has been created for applicable users).
 - c. Configure appropriate and least-privileged settings, authorized client routes, and client settings in each tab.

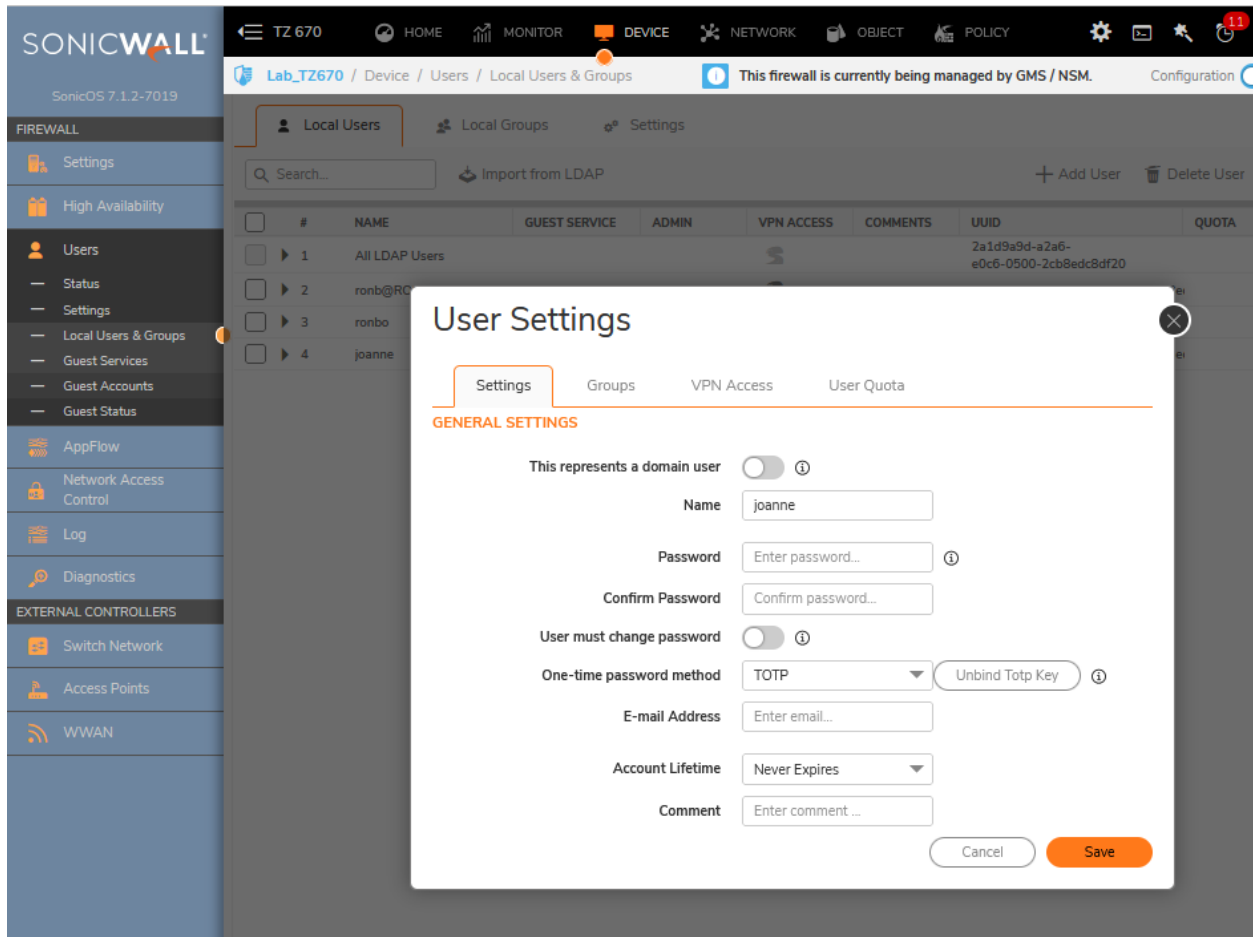


3. Enable Multi-Factor Authentication (MFA): One-Time Password (OTP).
 - a. Configure OTP settings under **Device | Users | Settings | Authentication** tab.
 - b. Enable OTP and set its parameters under USER AUTHENTICATION SETTINGS.

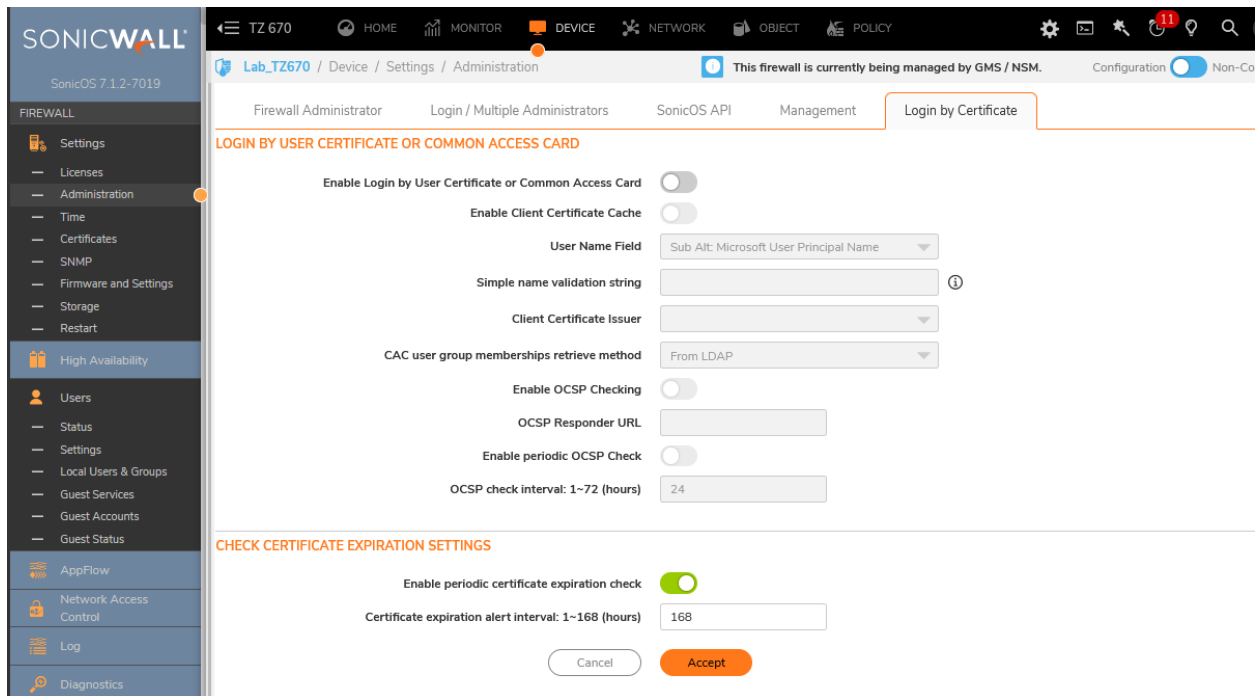
The screenshot displays the SonicWall management interface for a device labeled 'TZ 670'. The left sidebar shows the navigation menu with 'Users' selected. The main content area is titled 'USER AUTHENTICATION SETTINGS' and includes the following sections:

- User authentication method:** Set to 'LDAP + Local Users'. Below this are links to 'Configure RADIUS', 'Configure LDAP', and 'Configure TACACS+'.
- SINGLE-SIGN-ON METHOD(S):** Includes a 'Configure SSO' link, 'SSO Agent' (checked), and 'Terminal Services Agent' (unchecked).
- ONE-TIME PASSWORD:** Includes 'Enforce password complexity for One-Time Password' (checked), 'One-time password E-mail format' (radio buttons for 'Plain Text' and 'HTML', with 'Plain Text' selected), 'One Time Password Format' (dropdown menu set to 'Characters'), and 'One Time Password Length' (input fields set to 10). A 'Password Strength: Good' indicator is shown.

- c. Enable OTP for user accounts under **Device | Users | Local Users & Groups | Settings** tab for each user.



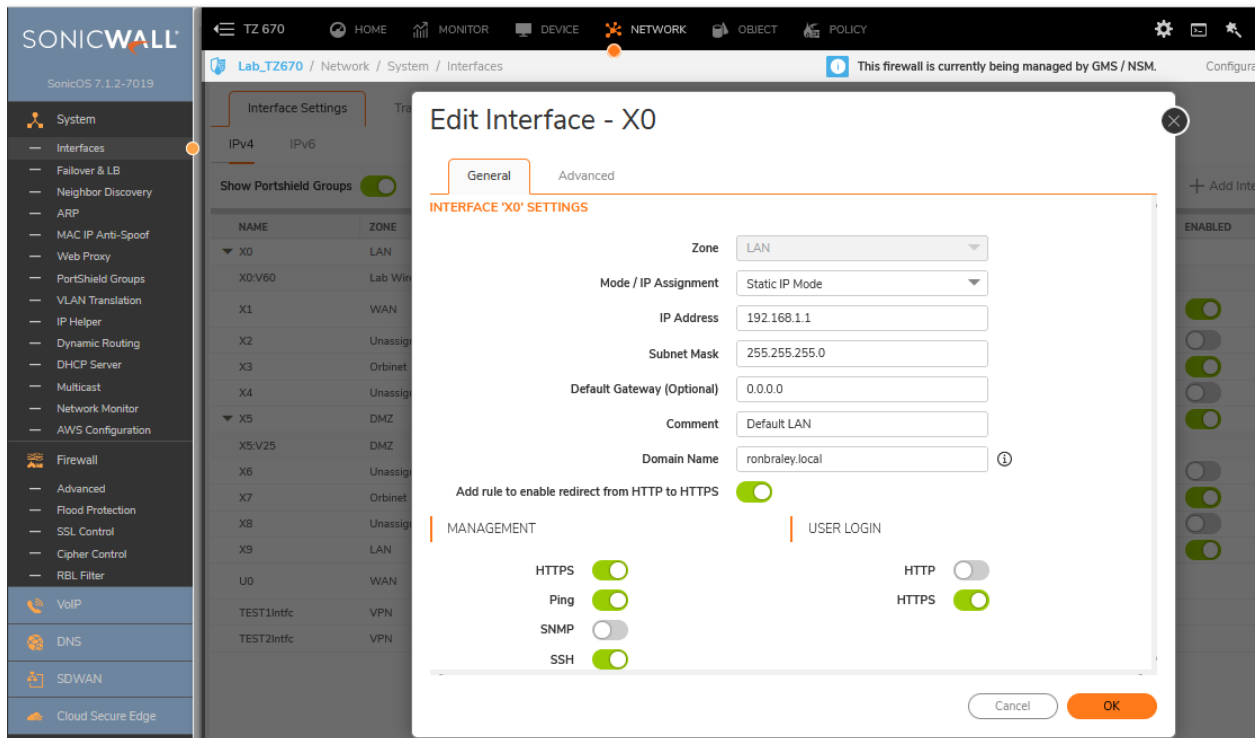
4. Enable MFA: Smart Cards.
 - a. Configure Smart Card settings under **Device | Settings | Administration | Login by Certificate** tab.



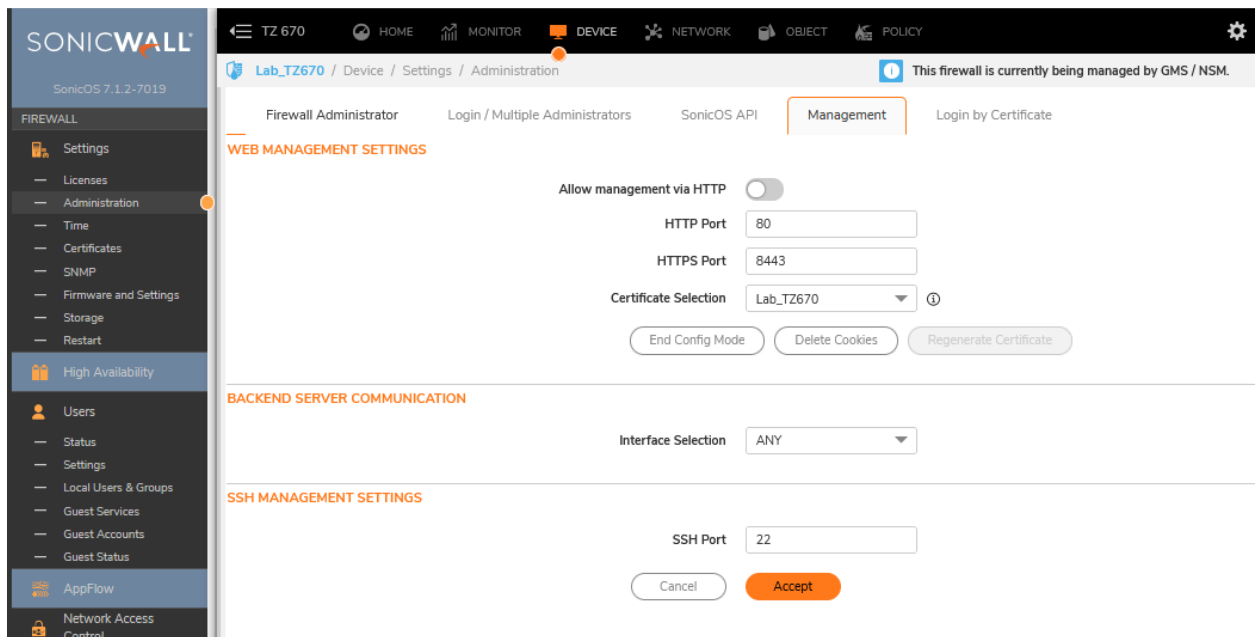
SSH (If Applicable)

A SonicWall firewall can be managed directly through a Secure Shell (SSH) connection. Steps for minimizing remote access risks for these connections are as follows:

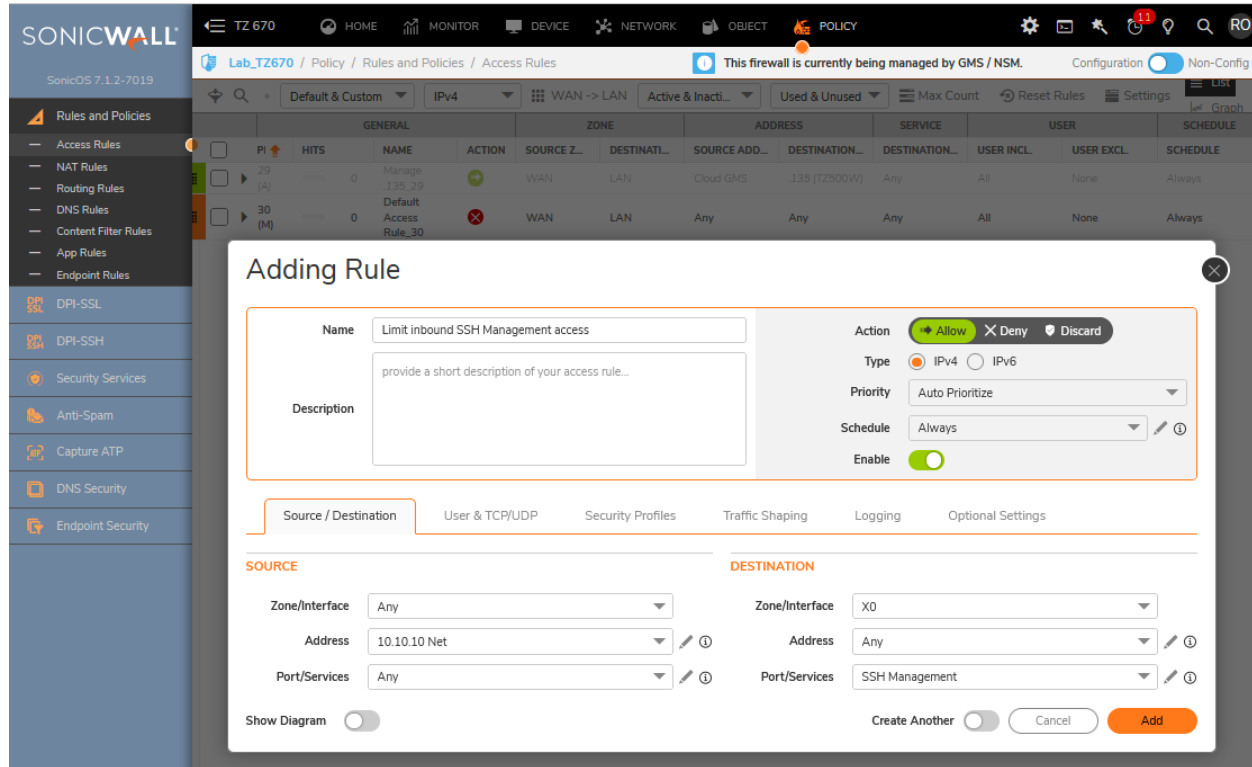
1. Enable SSH management (per interface).
 - a. Navigate to **Network | System | Interfaces | General** tab for the interface that should allow SSH communications.
 - b. Enable **SSH** under the MANAGEMENT section.



2. Set the service port if it should differ from the default.
 - a. Navigate to **Device | Settings | Administration | Management** tab.
 - b. Set the SSH Port under the SSH MANAGEMENT SETTINGS section.



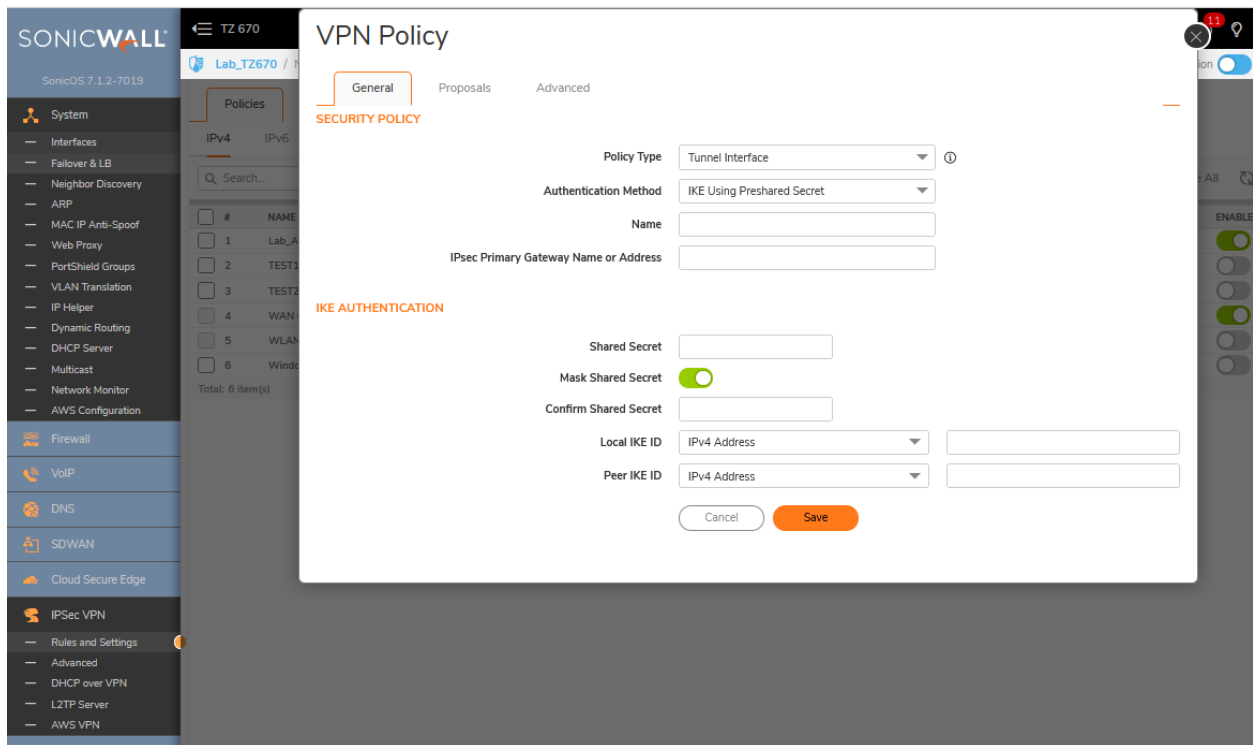
3. Restrict inbound SSH access to particular hosts or networks through a firewall access rule.
 - a. Navigate to **Policy | Rules and Policies | Access Rules**.
 - b. Select +Add at the bottom of the screen.
 - c. Create a rule that limits SSH access (the graphic below is only an example).



IPSEC VPN (If Applicable)

This feature is typically used for encrypted site-to-site connectivity and resource sharing, not individual remote access. Nevertheless, it's crucial to restrict access to just essential networks, ports, protocols, and services to minimize the risk of unauthorized remote access. The best way to do this is through:

1. Configure strong IPSEC VPN security policies based on specific routes and strong ciphers.
 - a. Navigate to **Network | IPsec VPN | Rules and Settings**.
 - b. Select +Add near the top of the screen.
 - c. Configure the policy under General, Network, Proposals, and Advanced tabs. **NOTE:** Tunnel Interfaces offer more ease and flexibility in policy configuration and firewall access rule integration.

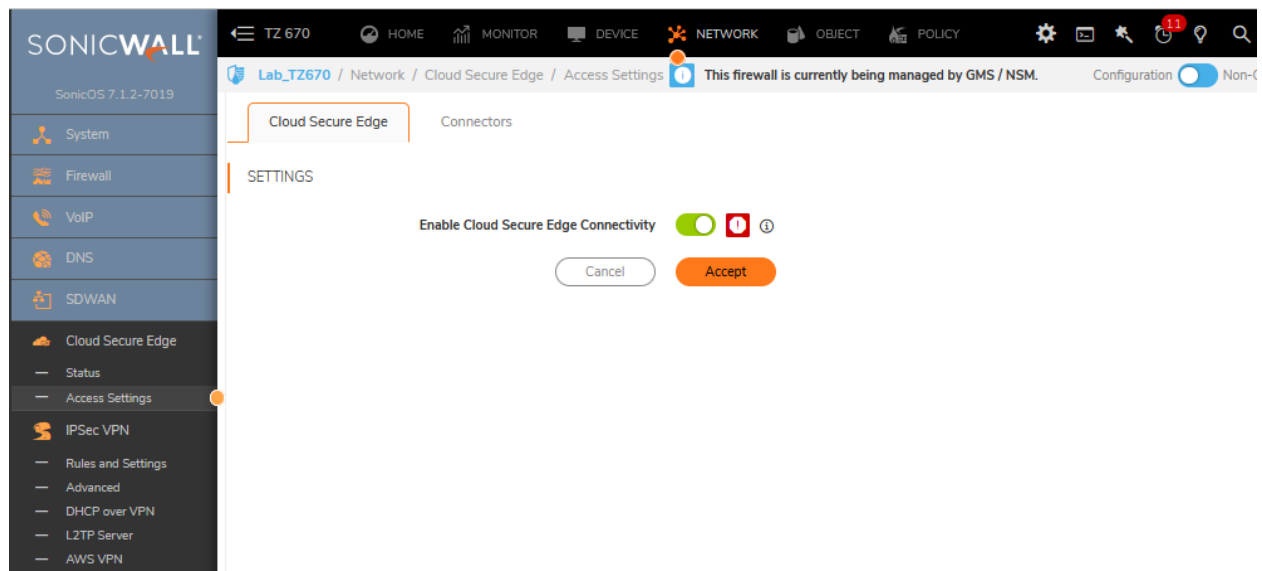


2. Secure the tunnel interfaces with firewall access rules to limit hosts, networks, ports, and protocols.
 - a. Navigate to **Policy | Rules and Policies | Access Rules**.
 - b. Create access rules based on VPN zones or interfaces limiting traffic to/from specific hosts, networks, ports, and protocols.

ZTNA with CSE (If Applicable)

SonicWall's CSE reduces the risk of unauthorized remote access through ZTNA (Zero Trust Network Access), which can be facilitated by a user's client application or the firewall's built-in connector. Unlike traditional VPNs, CSE provides least-privilege access based on real-time trust scoring, eliminating the need for device configuration and reducing the risk of over-provisioning. But, as with the other warranted events, CSE itself must be implemented and configured thoughtfully to mitigate the risk of unauthorized remote access effectively. The following offers best practices.

1. Enable the firewall CSE connector.
 - a. Navigate to **Network | Cloud Secure Edge | Access Settings | Cloud Secure Edge** tab.
 - b. Toggle Enable Cloud Secure Edge Connectivity.



2. Conversely, purchase client licensing and install and configure the CSE client as needed. The client itself can be downloaded at <https://getcseapp.sonicwall.com/download/>
3. Specific CSE configurations and use cases can be found here: <https://docs.banyansecurity.io/docs/solutions/>

Software Vulnerability Exploitation

Many, if not most, security breaches happen because of unapplied security vulnerability patches. An alternative to discreetly patching every system, called ‘virtual patching,’ can mitigate the risk of vulnerability exploitation.

Virtual Patching uses behavioral and signature-based Intrusion Prevention Service (IPS) capabilities to stop exploits before they reach vulnerable systems. Restricting accessible ports, protocols, hosts, and services via firewall access rules also aids in protecting unpatched systems. Enable and configure the IPS and relevant signatures and utilize firewall access rules to protect against unpatched vulnerabilities.

Enable the Intrusion Prevention Service (IPS)

Configuration

1. Navigate to **Policy | Security Services | Intrusion Prevention**.
2. Under IPS GLOBAL SETTINGS, Enable the option **Enable IPS**.
3. Enable **Prevent** and **Detect** all for **High** and **Medium Priority** Attacks.
4. Enable **Detect** all for **Low Priority** attacks.
5. Click **Accept**

SONICWALL Lab_TZ670 / Policy / Security Services / Intrusion Prevention

This firewall is currently being managed by GMS / NSM. Configuration Non-Config

Status / Settings Signatures

Enable the Intrusion Prevention Service per zone from the [Object > Match Objects > Zones](#) page.

IPS STATUS

Signature Database Downloaded
 Signature Database Timestamp UTC 10/04/2024 15:14:30.000 Update
 Last Checked 10/07/2024 18:51:23.816
 IPS Service Expiration Date 08/23/2026

IPS GLOBAL SETTINGS

Enable IPS ☒

Configure Res

| # | SIGNATURE GROUPS | PREVENT ALL | DETECT ALL | LOG REDUNDANCY FILTER (SECONDS) |
|---|-------------------------|-------------------------------------|-------------------------------------|---------------------------------|
| 1 | High Priority Attacks | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 2 | Medium Priority Attacks | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 3 | Low Priority Attacks | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 60 |

Cancel Accept

Enable Relevant IPS Signatures

Configuration

1. Navigate to **Policy | Security Services | Intrusion Prevention**.
2. Enable signatures relevant to the vulnerabilities being mitigated (WEB-ATTACKS category, in this example).

SONICWALL Lab_TZ670 / Policy / Security Services / Intrusion Prevention

This firewall is currently being managed by GMS / NSM. Configuration Non-Config

Status / Settings Signatures

Search... Priority: All Category: WEB-... View By: Signature Refresh Columns

| # | CATEGORY | NAME | ID | GID | PREVENT | DETECT | PRIORITY |
|----|-------------|---|------|--------|-------------------------------------|-------------------------------------|--------------|
| 1 | WEB-ATTACKS | HTTP Request with Malformed Host Header 1 | 61 | 684451 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 2 | WEB-ATTACKS | HTTP Request with Malformed Host Header 2 | 62 | 684452 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 3 | WEB-ATTACKS | Web Application Cross-Site Scripting (XSS) 71 | 173 | 721223 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 4 | WEB-ATTACKS | Web Application Remote Code Execution 1 | 273 | 44966 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 5 | WEB-ATTACKS | Web Application Remote Code Execution 2 | 274 | 44967 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 6 | WEB-ATTACKS | Web Application Cross-Site Scripting (XSS) 39 -c3 | 596 | 721222 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 7 | WEB-ATTACKS | GitLab ipynb Stored XSS 1 | 705 | 710123 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 8 | WEB-ATTACKS | Web Application Remote Code Execution 3 | 833 | 44984 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 9 | WEB-ATTACKS | Web Application Remote Code Execution 33 | 849 | 754117 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 10 | WEB-ATTACKS | Web Application Remote Code Execution 28 | 855 | 754112 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 11 | WEB-ATTACKS | Atchshadow Access 1 | 871 | 23442 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 12 | WEB-ATTACKS | Web Application Cross-Site Scripting (XSS) 22 | 1002 | 733404 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 13 | WEB-ATTACKS | Web Application SQL Injection (UNION SELECT) 12 | 1004 | 734486 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 14 | WEB-ATTACKS | Kentico CMS Insecure Deserialization | 1009 | 717987 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 15 | WEB-ATTACKS | WordPress plugin wp-google-maps SQL Injection | 1010 | 731779 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 16 | WEB-ATTACKS | Microsoft SharePoint Server Elevation of Privilege (CVE-2023-29357) 3 | 1011 | 742763 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |
| 17 | WEB-ATTACKS | Web Application Cross-Site Scripting (XSS) 78 -c6 | 1014 | 733601 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 / 3 Medium |

Enable Firewall Access Rules

Configuration

1. Navigate to **Policy | Rules and Policies | Access Rules**.
2. To further mitigate software exploits, create access rules between security zones or interfaces limiting traffic to/from specific hosts, networks, ports, and protocols.

Non-volumetric DDoS Attack

Distributed Denial-of-Service (DDoS) attacks can cripple networks and security devices like firewalls. Not only are networked capabilities potentially diminished during the attacks, but services like those that manage security and access controls can suffer. Results can include unauthorized firewall and resource access (besides unavailable services). There are several types of DDoS attacks, only two of which will be warranted by SonicWall: *Protocol* and *Application*.

There are three primary types of DDoS attacks:

1. Volumetric. This attack sends massive amounts of data to saturate bandwidth and overwhelm service. Because attack (and defense) success depends on variables outside SonicWall's control, **we won't guarantee total protection against it**.
2. Protocol. This attack targets specific protocols. The firewall is warranted against loss due to business disruption, depending on the firewall configuration and whether an existing IPS signature is deployed.
3. Application. This attack targets specific applications and service ports to overwhelm and deny access. As with warranting against a Protocol DDoS attack, the firewall is warranted against loss due to business disruption, depending on the firewall configuration and whether an existing IPS signature is deployed.

Enable and configure the following features to minimize the risk of service disruption through DDoS protocol and application attacks: IPS, Control Plane Flood Protection, Data Flood Protection, ICMP Flood Protection, GEO-IP Filtering, and Botnet Filtering. Please remember that flood control is dynamic and should be configured carefully based on the environment and business requirements.

Intrusion Prevention Service (IPS)

Configuration

1. Navigate to **Policy | Security Services | Intrusion Prevention**.
2. Under IPS GLOBAL SETTINGS, Enable the option **Enable IPS**.
3. Enable **Prevent** and **Detect** all for **High** and **Medium Priority** Attacks.
4. Enable **Detect** all for **Low Priority** attacks.
5. Click **Accept**

SONICWALL TZ 670 HOME MONITOR DEVICE NETWORK OBJECT POLICY

Lab_TZ670 / Policy / Security Services / Intrusion Prevention

This firewall is currently being managed by GMS / NSM. Configuration Non-C

Status / Settings Signatures

Enable the Intrusion Prevention Service per zone from the [Object > Match Objects > Zones](#) page.

IPS STATUS

Signature Database Downloaded

Signature Database Timestamp UTC 10/04/2024 15:14:30.000 Update

Last Checked 10/07/2024 18:51:23.816

IPS Service Expiration Date 08/23/2026

IPS GLOBAL SETTINGS

Enable IPS ☒

Configure Res

| # | SIGNATURE GROUPS | PREVENT ALL | DETECT ALL | LOG REDUNDANCY FILTER (SECONDS) |
|---|-------------------------|-------------------------------------|-------------------------------------|---------------------------------|
| 1 | High Priority Attacks | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 2 | Medium Priority Attacks | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 3 | Low Priority Attacks | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 60 |

Cancel Accept

Control Plane Flood Protection

Configuration

1. Navigate to **Network | Firewall | Advanced | Connections** tab.
2. Select **Enable Control Plane Flood Protection**.
3. Click **Accept**.

SONICWALL TZ 670 HOME MONITOR DEVICE NETWORK OBJECT POLICY

Lab_TZ670 / Network / Firewall / Advanced

This firewall is currently being managed by GMS / NSM. Configuration Non-C

Settings Connections IPv6

CONNECTIONS

☐ Maximum SPI Connections (DPI services disabled)
☒ Maximum DPI Connections (DPI services enabled)
☐ DPI Connections (DPI services enabled with additional performance optimizations)

Visualization Maximum Connector

| # | APPFLOW | EXTERNAL COLLECTOR | MAXIMUM SPI CONNECTIONS | MAXIMUM DPI CONNECTIONS | DPI CONNECTIONS |
|---|---------|--------------------|-------------------------|-------------------------|-----------------|
| 1 | Yes | Yes | 1125000 | 375000 (current) | 375000 |
| 2 | No | No | 1500000 | 500000 | 500000 |
| 3 | Yes | No | 1125000 | 375000 | 375000 |
| 4 | No | Yes | 1200000 | 400000 | 400000 |

Total: 4 item(s)

CONTROL PLANE FLOOD PROTECTION

Enable Control Plane Flood Protection ☒

Control Plane Flood Protection Threshold (CPU %) % ⓘ

Cancel Accept

Data Flood Protection

UDP Flood Protection

Configuration

1. Navigate to **Network | Firewall | Flood Protection | UDP** tab.
2. Under UDP FLOOD PROTECTION, *enable UDP Flood Protection*. *Note that this must be enabled to activate the other UDP Flood Protection options.*
3. Set the *UDP Flood Attack Threshold*. The maximum number of UDP packets allowed per second to be sent to a host, range, or subnet that triggers UDP Flood Protection. Exceeding this threshold triggers ICMP Flood Protection. The minimum value is 50, the maximum is 1000000, and the default value is 1000.
4. Configure the *UDP Flood Attack Protected Destination List*. Select Any to apply the Attack Threshold to the sum of UDP packets passing through the firewall.
5. Click **Accept**.

Note: Due to the nature of their large UDP packets used for voice and video, traffic for some collaboration products, such as Microsoft Teams, Zoom, etc., might be considered a UDP flood and dropped after configuring UDP flood protection. If you experience this, please exclude traffic for those applications by following the steps in the following KB: <https://www.sonicwall.com/support/knowledge-base/microsoft-teams-randomly-dropping-video-conferencing-applications/200727073315443>

SONICWALL Lab_TZ670 / Network / Firewall / Flood Protection

This firewall is currently being managed by GMS / NSM. Configuration Non-Cr

TCP **UDP** ICMP

IPv4 IPv6

UDP SETTINGS

Default UDP Connection Timeout 30 seconds

UDP FLOOD PROTECTION

Enable UDP Flood Protection ☒

UDP Flood Attack Threshold 1000 UDP Packets / Sec

UDP Flood Attack Blocking Time 2 seconds

UDP Flood Attack Protected Destination List --- Select an Address Object ---

Cancel Accept

UDP TRAFFIC STATISTICS Clear Statistics

| | |
|---------------------------------------|-----------|
| Connections Opened | 12664526 |
| Connections Closed | 12664445 |
| Total UDP Packets | 196857971 |
| Validated Packets Passed | 196857634 |
| Malformed Packets Dropped | 337 |
| Average UDP Packet Rate (Packets/Sec) | 27 |
| UDP Floods In Progress | 0 |
| Total UDP Floods Detected | 0 |
| Total UDP Flood Packets Rejected | 0 |

ICMP Flood Protection

Configuration

1. Navigate to **Network | Flood Protection | ICMP** tab.
2. Select **Enable ICMP Flood Protection**.
3. Click **Accept**.

The screenshot shows the SonicWall configuration interface for ICMP Flood Protection. The left sidebar contains the navigation menu with options like System, Firewall, VoIP, DNS, SDWAN, Cloud Secure Edge, IPSec VPN, and SSL VPN. The main panel is titled 'Lab_TZ670 / Network / Firewall / Flood Protection' and has tabs for TCP, UDP, and ICMP. The ICMP tab is selected, showing the 'ICMP FLOOD PROTECTION' settings. The 'Enable ICMP Flood Protection' toggle is turned on. The 'ICMP Flood Attack Threshold' is set to 200 ICMP Packets / Sec, and the 'ICMP Flood Attack Blocking Time' is set to 2 seconds. The 'ICMP Flood Attack Protected Destination List' is set to '--- Select an Address Object ---'. There are 'Cancel' and 'Accept' buttons at the bottom. Below the settings is the 'ICMP TRAFFIC STATISTICS' section, which includes a table of statistics and a 'Clear Statistics' link.

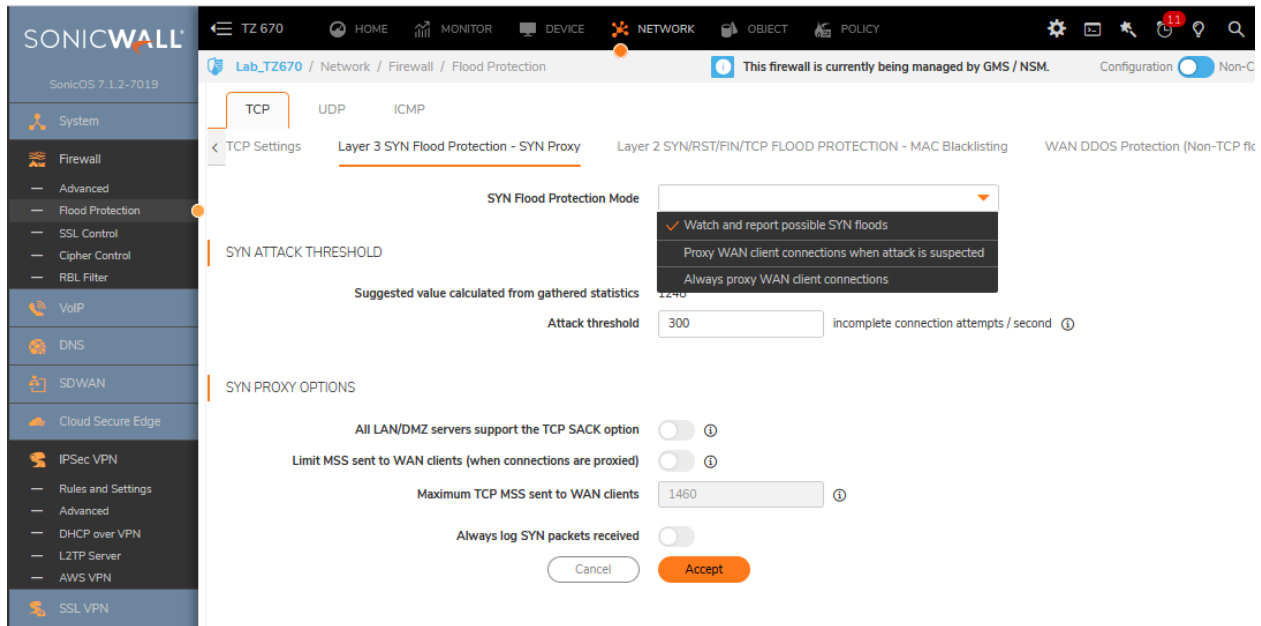
| ICMP TRAFFIC STATISTICS | |
|--|----------|
| Connections Opened | 15345992 |
| Connections Closed | 15345989 |
| Total ICMP Packets | 19013586 |
| Validated Packets Passed | 19013586 |
| Malformed Packets Dropped | 0 |
| Average ICMP Packet Rate (Packets/Sec) | 2 |
| ICMP Floods In Progress | 0 |
| Total ICMP Floods Detected | 0 |
| Total ICMP Flood Packets Rejected | 0 |

TCP Flood Protection

Configuration

1. Navigate to **Network | Flood Protection | TCP** tab.
2. Click on the **Layer 3 SYN Flood Protection – SYN Proxy** sub-tab.
3. Set **SYN Flood Protection Mode** to *Proxy WAN Client Connections when attack is suspected*.
4. Click **Accept**.

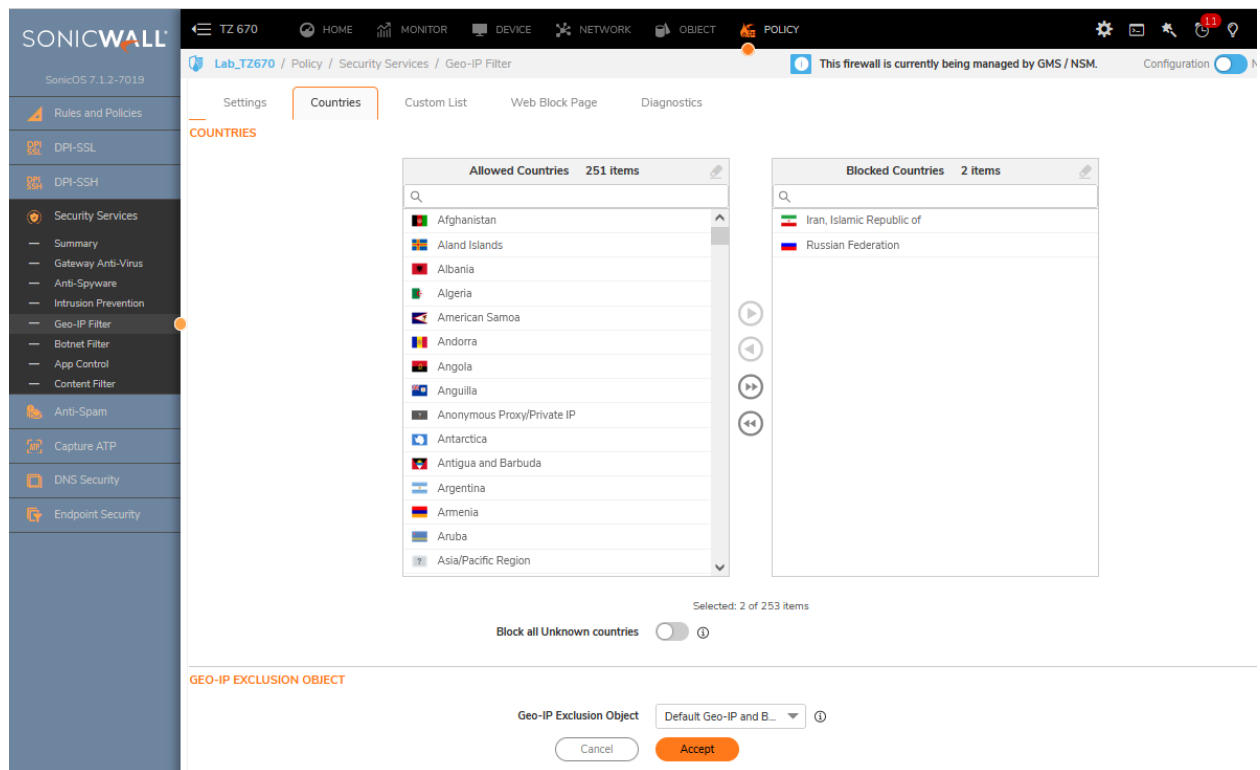
CAUTION: Proxy WAN Connections will block external users who trigger the Flood Protection feature from connecting to internal resources. If there is a chance any user can generate a false positive for this feature, it is recommended to leave TCP Flood Protection in Watch and Report mode.



GEO-IP Filter

Configuration

1. Navigate to **Policy | Security Services | Geo-IP Filter | Settings** tab.
2. Enable **Block connections to/from countries selected in the Countries tab**.
3. Navigate to the **Countries** tab and select the countries to block from the table provided under the **Countries—Allowed Countries** column. Then, drag and drop the country name to the **Blocked Countries** column. See below for a list of recommended countries to block.
4. Click **Accept**.



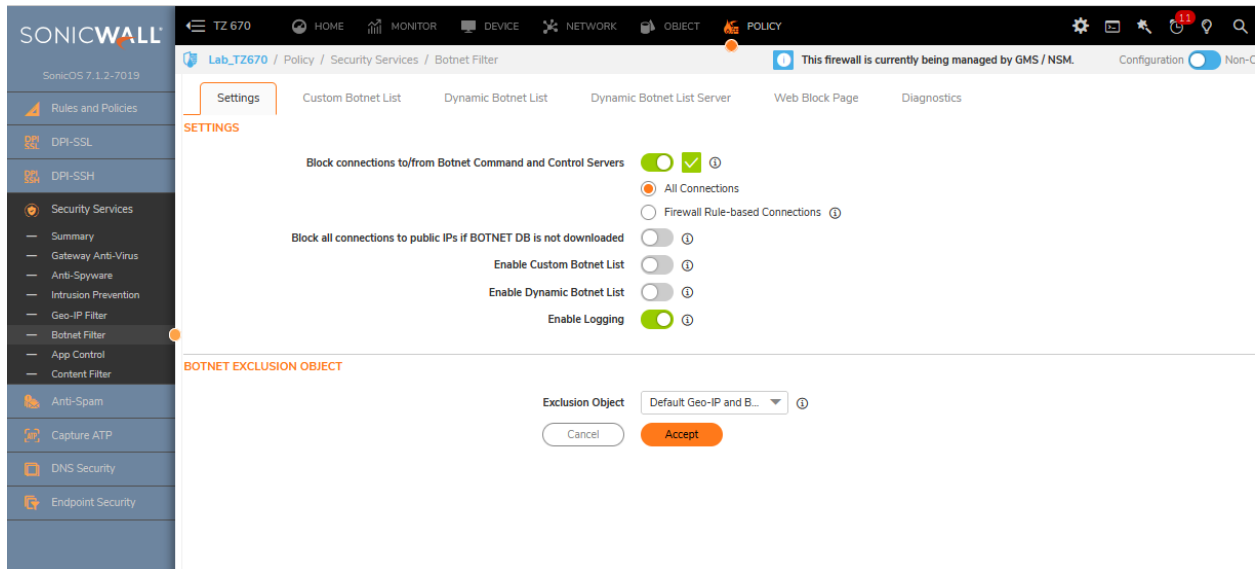
GEO-IP Country Recommendations

Consider configuring the GEO-IP Engine to block all but these eleven countries: Austria, Canada, Europe, France, Germany, Ireland, Sweden, Switzerland, United Kingdom, United States, and United States Minor Outlying Is. At a **minimum**, block these countries: Afghanistan, Brazil, Colombia, China, India, Iran, Iraq, Lebanon, Libya, Lithuania, North Korea (if listed), Romania, Russian Federation, Serbia, Somalia, Sudan, Syria, Turkey, and Ukraine.

Botnet Filter

Configuration

1. Navigate to **Policy | Security Services | Botnet Filter | Settings** tab.
2. Enable **Block connections to/from Botnet Command and Control Servers**.
3. Click **Accept**.



Additional Mitigating Requirements

Access/Admin Port Changes

A good security practice is to change the access ports for Firewall Management (MGMT), SSLVPN, and SSH access as follows. Note: Administrative access must only be enabled on specific interfaces or remote-access methods where it's actually needed!

1. **MGMT:** Navigate to **Device | Administration | Management** tab and change the HTTPS Port numbers in the **WEB MANAGEMENT SETTINGS** section (Note: Never manage the firewall over HTTP!).

The screenshot displays the SonicWall Management interface for a device named 'Lab_TZ670'. The left sidebar shows the navigation menu with 'Administration' selected. The top navigation bar includes tabs for 'Firewall Administrator', 'Login / Multiple Administrators', 'SonicOS API', 'Management' (which is active), and 'Login by Certificate'. A status message at the top right states: 'This firewall is currently being managed by GMS / NSM.' The main content area is divided into three sections: 'WEB MANAGEMENT SETTINGS', 'BACKEND SERVER COMMUNICATION', and 'SSH MANAGEMENT SETTINGS'. In the 'WEB MANAGEMENT SETTINGS' section, there is a toggle for 'Allow management via HTTP' which is currently disabled. Below this, the 'HTTP Port' is set to 80, and the 'HTTPS Port' is set to 8443. The 'Certificate Selection' dropdown is set to 'Lab_TZ670'. There are buttons for 'End Config Mode', 'Delete Cookies', and 'Regenerate Certificate'. The 'BACKEND SERVER COMMUNICATION' section has an 'Interface Selection' dropdown set to 'ANY'. The 'SSH MANAGEMENT SETTINGS' section has an 'SSH Port' set to 22, with 'Cancel' and 'Accept' buttons.

SONICWALL
SonicOS 7.1.2-7019

TZ 670 HOME MONITOR **DEVICE** NETWORK OBJECT POLICY

Lab_TZ670 / Device / Settings / Administration

This firewall is currently being managed by GMS / NSM.

Firewall Administrator Login / Multiple Administrators SonicOS API **Management** Login by Certificate

WEB MANAGEMENT SETTINGS

Allow management via HTTP ☐

HTTP Port 80

HTTPS Port 8443

Certificate Selection Lab_TZ670 ⓘ

End Config Mode Delete Cookies Regenerate Certificate

BACKEND SERVER COMMUNICATION

Interface Selection ANY

SSH MANAGEMENT SETTINGS

SSH Port 22

Cancel Accept

2. **SSLVPN:** Navigate to **Network | SSL VPN | Server Settings | SSL VPN SERVER SETTINGS** section, and change the SSL VPN Port. **Note:** *Enable Web Management over SSL VPN* should only be enabled if absolutely necessary (leave it disabled otherwise).

SONICWALL TZ 670 HOME MONITOR DEVICE NETWORK OBJECT POLICY

Lab_TZ670 / Network / SSL VPN / Server Settings

This firewall is currently being managed by GMS / NSM. Configuration

SSL VPN STATUS ON ZONES

This is the SSL VPN Access status on each Zone. Green indicates active SSL-VPN status. Enable or disable SSL-VPN access by toggling the zone below.

| | |
|-------------------|-------------------------------------|
| LAN | <input checked="" type="checkbox"/> |
| WAN | <input checked="" type="checkbox"/> |
| DMZ | <input type="checkbox"/> |
| WLAN | <input type="checkbox"/> |
| MGMT | <input type="checkbox"/> |
| Switch Management | <input type="checkbox"/> |
| SMA Outside | <input type="checkbox"/> |
| Lab Wireless | <input type="checkbox"/> |
| Guest_Wireless | <input type="checkbox"/> |
| Orbinet | <input type="checkbox"/> |

SSL VPN SERVER SETTINGS

| | | | |
|------------------------------|------------|------------------------------------|--------------------------|
| SSL VPN Port | 4433 | Enable Web Management over SSL VPN | <input type="checkbox"/> |
| Certificate Selection | Lab_TZ670 | Enable SSH Management over SSL VPN | <input type="checkbox"/> |
| Authentication Type | Password | Mouse Inactivity Check | <input type="checkbox"/> |
| User Domain | mylablocal | | |
| Inactivity Timeout (minutes) | 10 | | |

RADIUS USER SETTINGS

- SSH:** Navigate to **Device | Administration | Management** tab, and change the HTTPS Port numbers in the **SSH MANAGEMENT SETTINGS** section (Note: Never manage the firewall over HTTP!)

SONICWALL TZ 670 HOME MONITOR DEVICE NETWORK OBJECT POLICY

Lab_TZ670 / Device / Settings / Administration

This firewall is currently being managed by GMS / NSM.

Firewall Administrator Login / Multiple Administrators SonicOS API **Management** Login by Certificate

WEB MANAGEMENT SETTINGS

Allow management via HTTP ☐

HTTP Port 80

HTTPS Port 8443

Certificate Selection Lab_TZ670

End Config Mode Delete Cookies Regenerate Certificate

BACKEND SERVER COMMUNICATION

Interface Selection ANY

SSH MANAGEMENT SETTINGS

SSH Port 22

Cancel Accept

Cloud Backups

Enabling cloud backups of configuration files will help ensure there's an adequate audit trail to prove the firewall configuration meets Cysurance's requirements. To facilitate cloud backups, navigate to the **Device | Settings | Firmware and Settings | Cloud Backups** tab and toggle on the *Cloud Backup* option.

The screenshot displays the SonicWall management interface. The top navigation bar includes tabs for TZ 670, HOME, MONITOR, DEVICE, NETWORK, OBJECT, and POLICY. The left sidebar lists various settings categories under FIREWALL and EXTERNAL CONTROLLERS. The main content area is titled 'Lab_TZ670 / Device / Settings / Firmware and Settings'. It features three sub-tabs: 'Firmware & Local Backups', 'Cloud Backups' (which is selected), and 'Settings'. A 'Cloud Backup' toggle switch is turned on, and a 'Create Backup' button is visible. Below this, a table lists backup entries with columns for ID, Firmware Version, Configuration Backup Date, Username, Comments, Backup Type, and Actions.

| # | FIRMWARE VERSION | CONFIGURATION BACKUP DATE | USERNAME | COMMENTS | BACKUP TYPE | ACTIONS |
|---|---|---------------------------|----------|------------------------------------|-------------|---------|
| 1 | 7.1.2-7019-R6288 (3 Configuration Files available) | | System | This is the cloud backup firmware. | | |
| 2 | 7.0.1-5119-R4713 (3 Configuration Files available) | | System | This is the cloud backup firmware. | | |
| 3 | 7.1.1-7051-R5653 (3 Configuration Files available) | | System | This is the cloud backup firmware. | | |
| 4 | 7.0.1-5145-R5175 (3 Configuration Files available) | | System | This is the cloud backup firmware. | | |
| 5 | 7.1.1-7047-R5557 (3 Configuration Files available) | | System | This is the cloud backup firmware. | | |
| 6 | 7.1.1-7040-R5387 (3 Configuration Files available) | | System | This is the cloud backup firmware. | | |

Periodic Diagnostic Reporting

Enabling *Periodic secure diagnostic reporting for support purposes* may aid in proving the state of the firewall configuration during a breach. Enable it here: **Device | Diagnostics | Tech Support Report** and enable *Periodic secure diagnostic reporting for support purposes* in the **TECH SUPPORT REPORT** section.