Sangfor Network Secure

Hardening Guide

Product Version	8.0.85
Document Version	1.0
Released on	Sept. 2, 2024
Author	Randolf Raguingan

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This is a guide for the security enhancement of the Sangfor Network Secure.

Intended Audience

This security guide is intended for security administrators, IT auditors, and platform deployment personnel who are involved in developing, deploying, assessing, or securing solutions that incorporate Sangfor Network Secure.

Change Log

Date	Change Description
Sept. 2, 2024	This is the first release of this document.

Table of Contents

System Settings

1.1 Ensure Password Expiration is set to 90 days

Description:

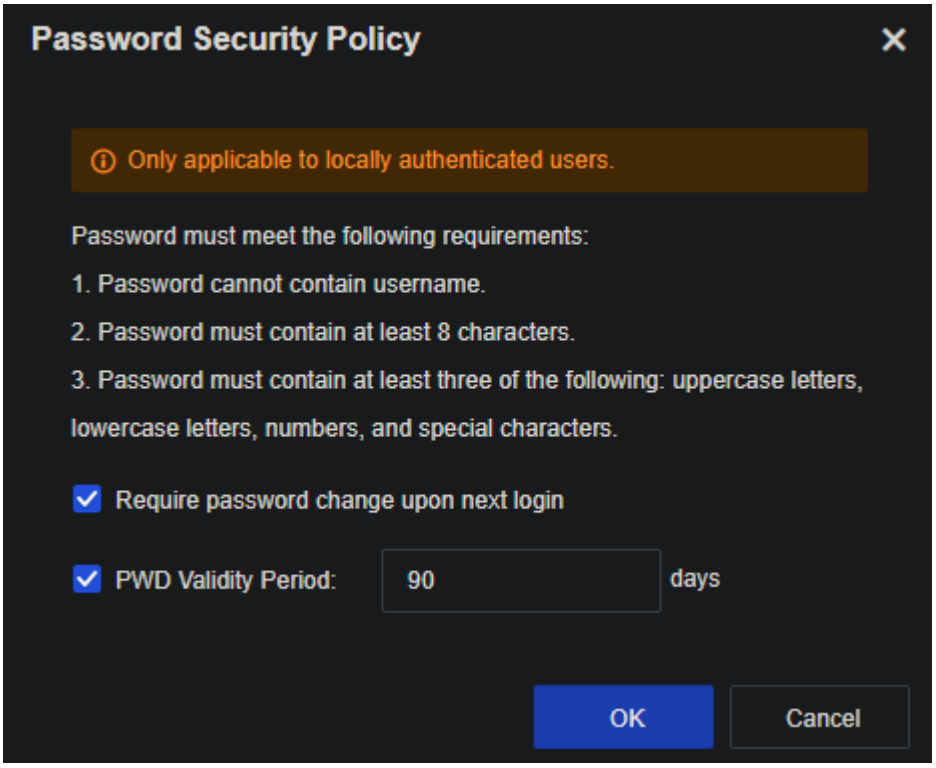
To enhance the security of your Sangfor firewall, it is crucial to enforce a password expiration policy that limits the lifespan of user passwords. Setting the password expiration to 90 days ensures that passwords are regularly updated, reducing the risk of unauthorized access due to compromised or outdated credentials

Rationale:

Setting a 90-day password expiration policy helps prevent unauthorized access by ensuring passwords are regularly updated. This reduces the risk of compromised credentials being used over long periods and encourages the use of stronger, more secure passwords. Aligning with CIS benchmarks, this practice enhances overall security and supports compliance with best practices for protecting network resources.

Remediation:

System > Administrator > Password Security Policy > PWD Validity Period



1.2 Ensure Web Session timeout is set to less than or equal to 10 minutes

Description:

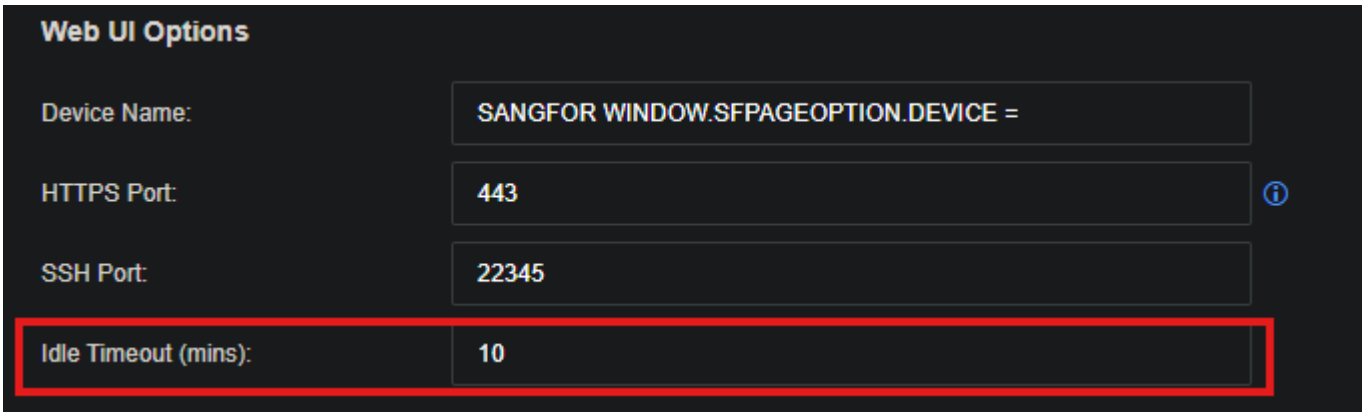
Set the WebUI Session Timeout value for device management to 10 minutes or less to automatically close inactive sessions.

Rationale:

An unattended computer with an open administrative session to the device could allow an unauthorized user access to the firewall's management interface.

Remediation:

System > General Settings > Web UI Options > Idle Timeout (mins)



1.3 Ensure management GUI listens on secure TLS version

Description:

As we move towards better encryption capabilities, we need to also ensure GUI access is properly secured. TLS 1.3 is currently the most secure SSL/TLS supported version for SSL-encrypted administrator access (at this time of writing).

Rationale:

Use higher version of SSL/TLS to prevent MiTM attacks.

Remediation:

System > General Settings > Web UI Options > TLS Protocol

1.4 Ensure default Admin ports are changed

Description:

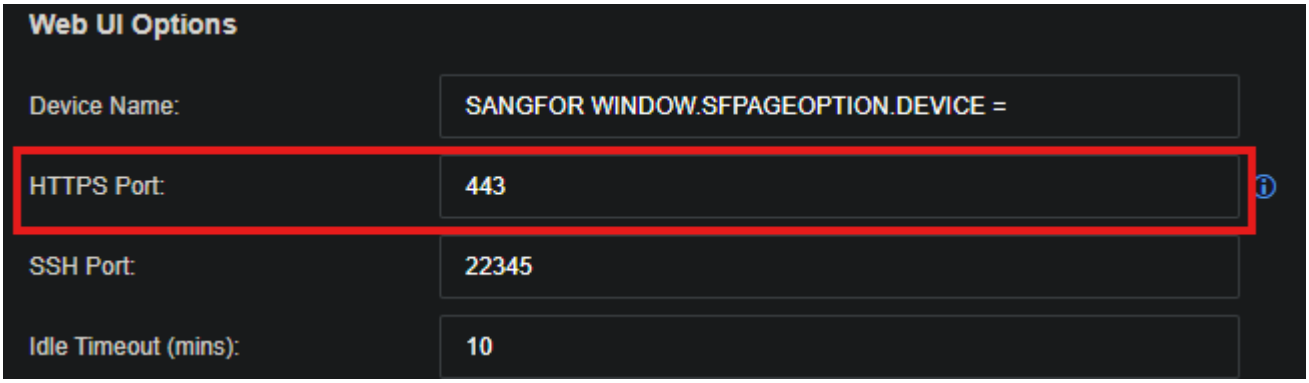
By default, Sangfor Network Secure ports listen on the common port 443.

Rationale:

To increase the security of the Sangfor Network Secure, changing the default port helps obscure administrative interfaces, making it more challenging for attackers to identify and exploit these services.

Remediation:

System > General Settings > Web UI Options > HTTPS Port



1.5 Ensure time zone is properly configured

Description:

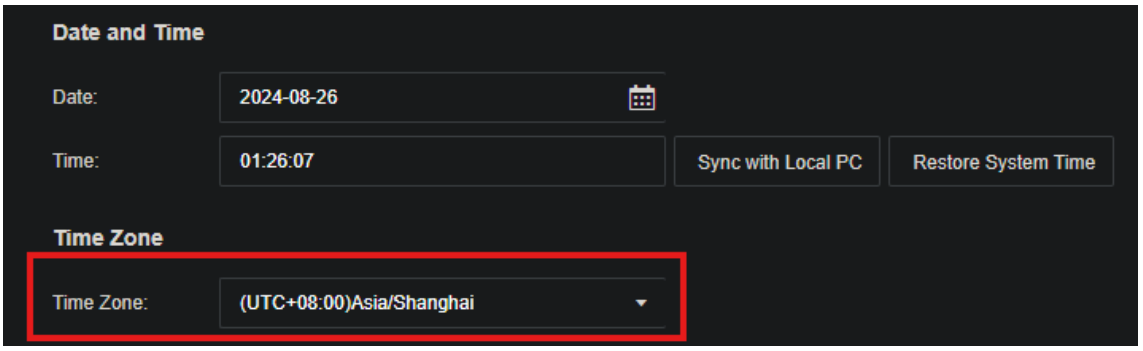
Sets the local time zone information so that the time displayed by the device is more relevant to those who are viewing it.

Rationale:

Having a correct time set on the device is important for two main reasons. The first reason is that digital certificates compare this time to the range defined by their Valid from and Valid To fields to define a specific validity period. The second reason is to have relevant time stamps when logging information. Whether you are sending messages to a Syslog server, sending messages to an SNMP monitoring station, or performing packet captures, timestamps have little usefulness if you cannot be certain of their accuracy.

Remediation:

System > General Settings > System Time > Time Zone



1.6 Ensure latest firmware is installed

Description:

Check against the Sangfor community website to make sure that the latest stable firmware is installed.

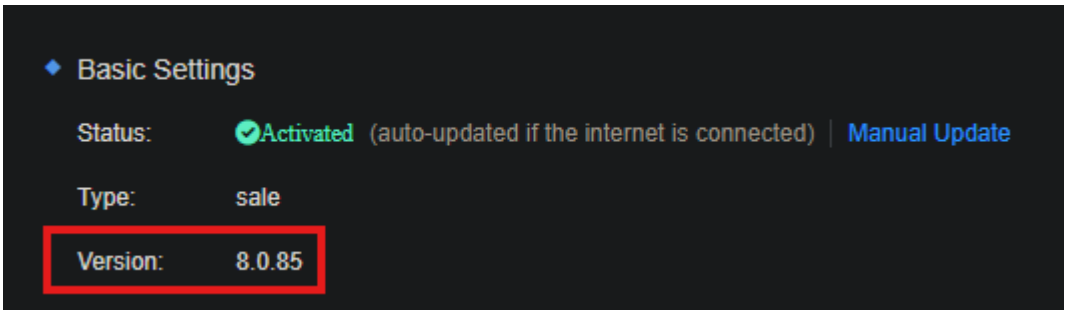
https://community.sangfor.com/

Rationale:

Sangfor periodically updates the Network Secure firmware to introduce new features and address critical issues. Once your Sangfor Network Secure unit is registered, firmware updates can be downloaded from the Sangfor Community website. Keeping the firmware up to date is essential to prevent exploitation of newly discovered vulnerabilities.

Remediation:

System > General Settings > Licensing > Version



1.7 Ensure admin accounts with different privileges have their correct profiles assigned

Description:

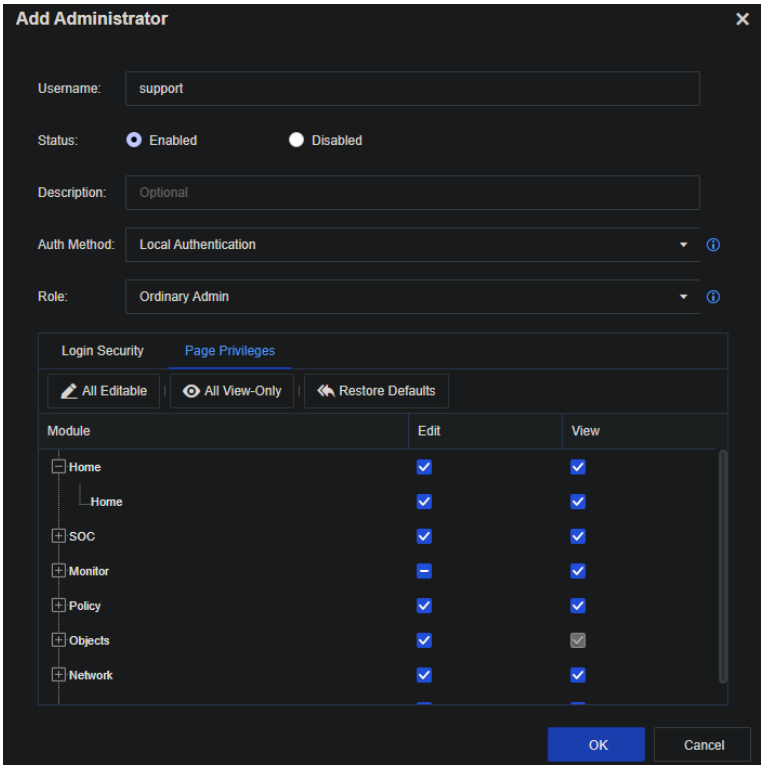
Verify that users with access to the Sangfor should only have the minimum privileges required for that user.

Rationale:

In certain organizations, it is essential to establish various levels of administrative accounts. For instance, junior IT staff in tier 1 support should have limited access compared to senior administrators in tier 3 support, who require full system access.

Remediation:

System > Administrator > Add administrator > Page Privileges



1.8 Ensure no expired subscription licenses

Description:

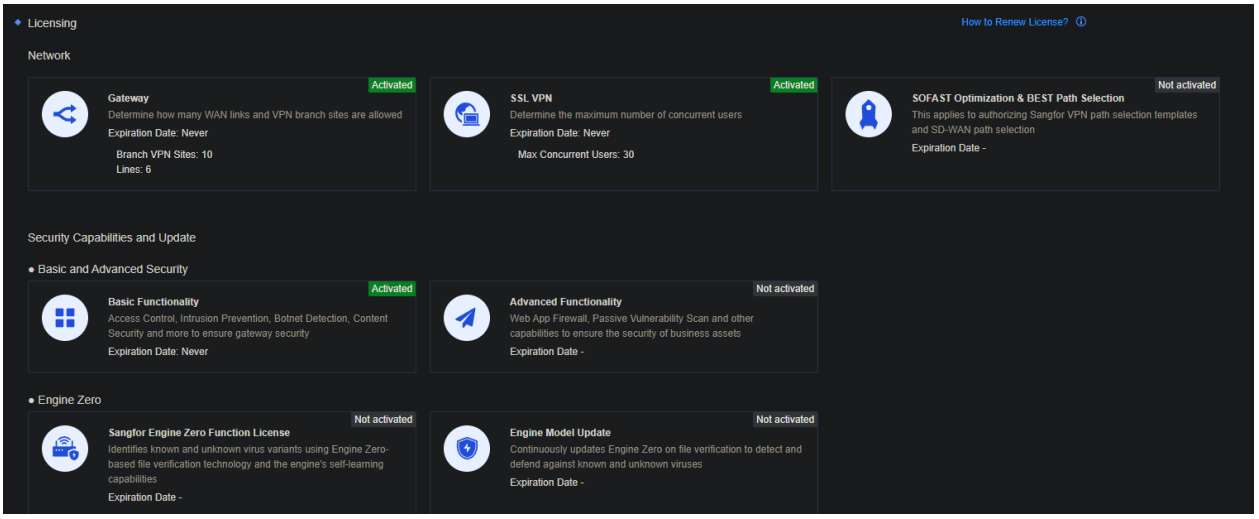
Licensing is used to activate various features on the Sangfor Network Secure.

Rationale:

An active subscription guarantees that the device receives up-to-date signatures for both known and emerging threats and remains functional for services requiring cloud-based updates. Furthermore, it ensures continued access to technical support and maintains warranty coverage as long as the license remains valid.

Remediation:

System > General Settings > Licensing



1.9 Ensure hostname is set

Description:

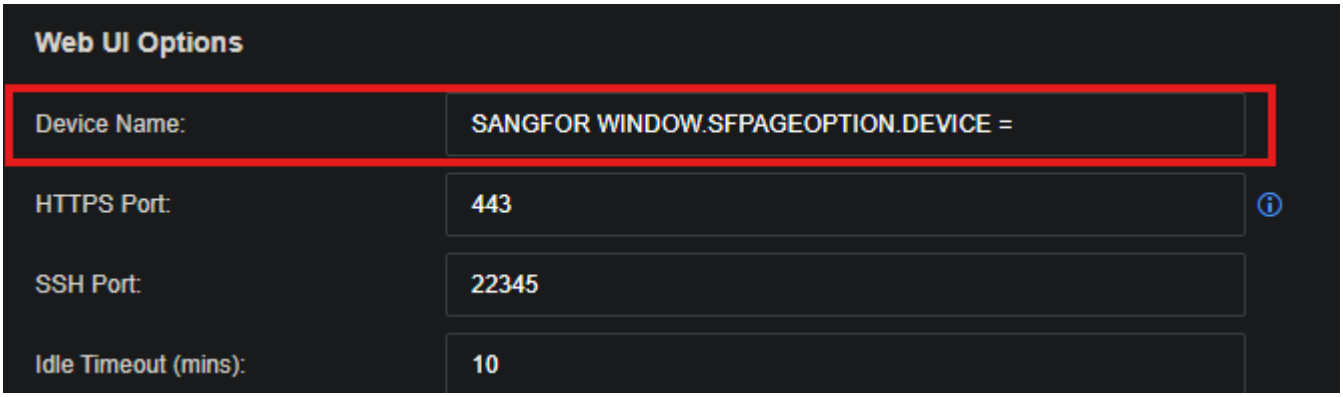
Change the default device name.

Rationale:

The device name plays an important role in asset inventory and identification as a security requirement. It is also crucial in the public keys and certificate deployments, as well as when correlating logs from different systems during an incident handling.

Remediation:

System > General Settings > Web UI > Device Name



Network Settings

2.1 Ensure Secure DNS Configuration

Description:

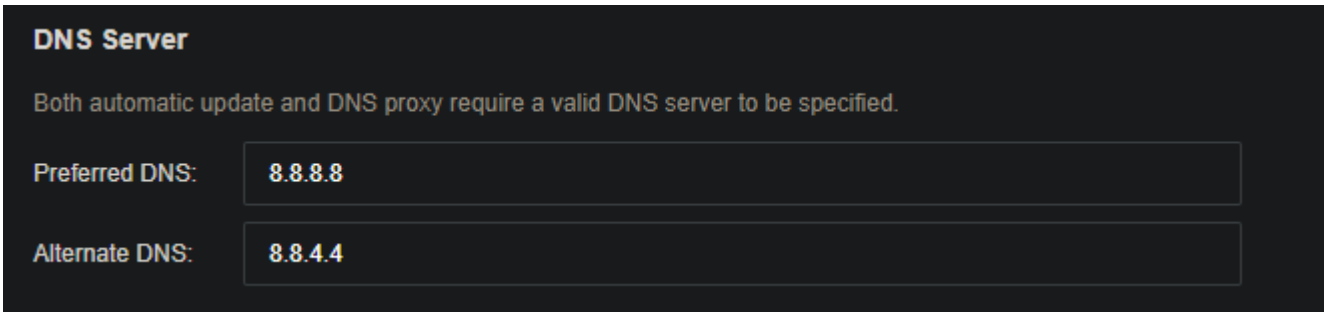
Sangfor Network Secure utilizes the Domain Name Service (DNS) to convert host names into IP addresses. To enable DNS resolution, you must configure the primary DNS server for your system, with options to also specify secondary and tertiary DNS servers. During name resolution, the system queries the primary DNS server first. In the event of a failure or timeout, the system will then query the secondary DNS server.

Rationale:

The purpose is to perform the resolution of system hostnames to Internet Protocol (IP) addresses using trusted DNS servers.

Remediation:

Network > DNS > DNS Servers



2.2 Ensure unused interfaces are disabled

Description:

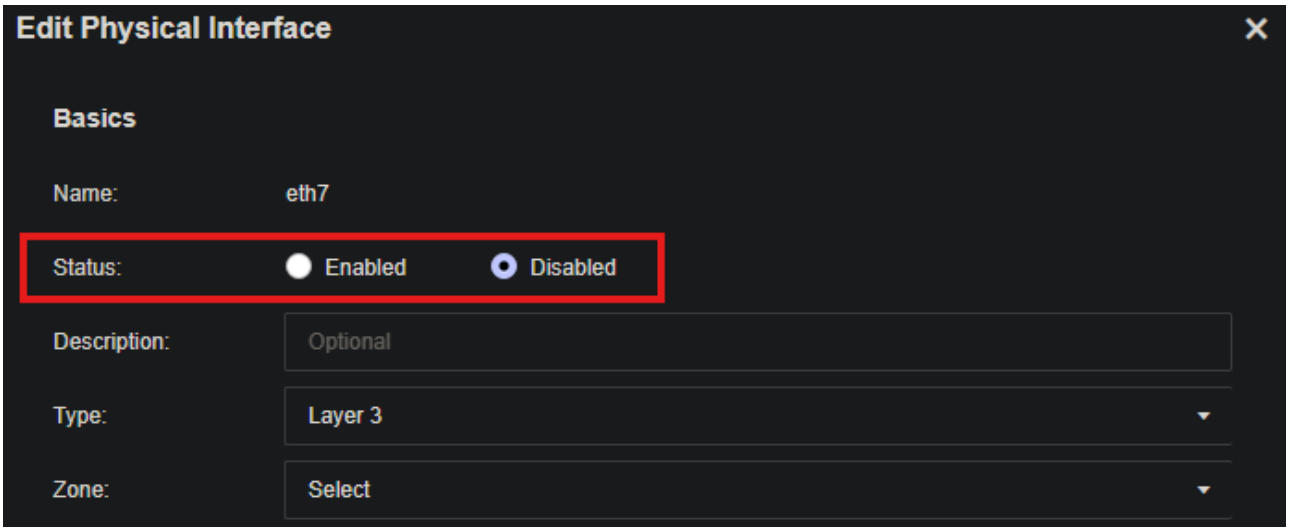
Disables the unused interfaces.

Rationale:

Disabling unused network interfaces complements physical security measures by adding an extra layer of protection against unauthorized access. If an attacker gains physical access to a network device and discovers an active, unused interface, they could exploit this open path to compromise the system.

Remediation:

Network > Interfaces > Status



2.3 Ensure IPv6 is disabled if not used

Description:

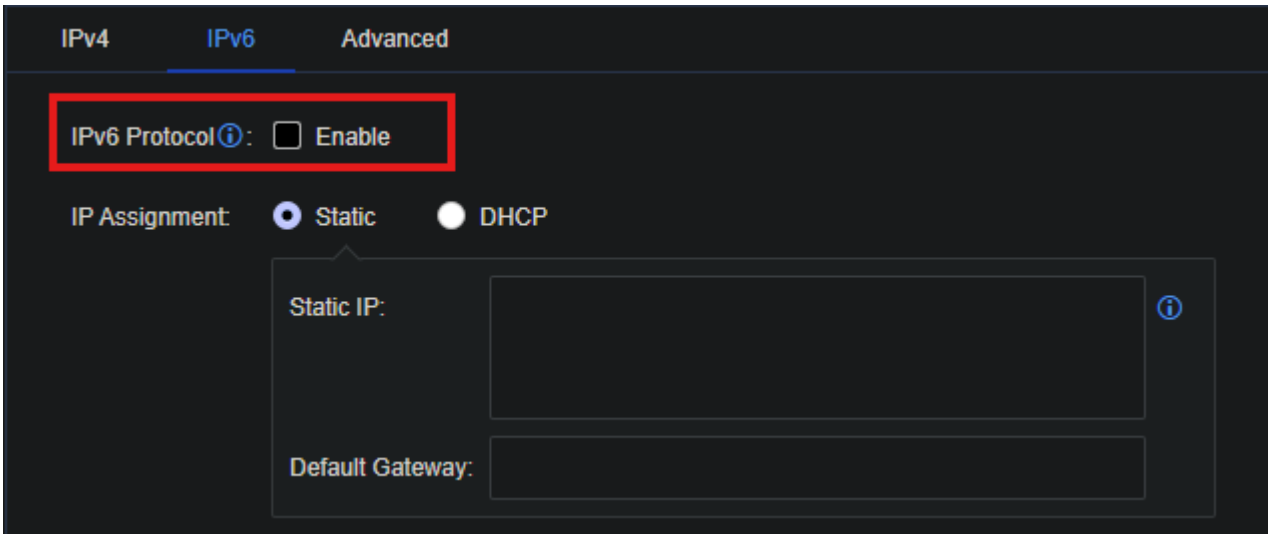
Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

Rationale:

If IPv6 is not required for your network operations or dual-stack configuration is not in use, it is advisable to disable IPv6 to minimize the system's attack surface. Leaving IPv6 enabled, even when it's not in use, can introduce potential vulnerabilities and expose the system to unnecessary risks.

Remediation:

Network > Interfaces > IPv6



2.4 Disable all management related to WAN Port

Description:

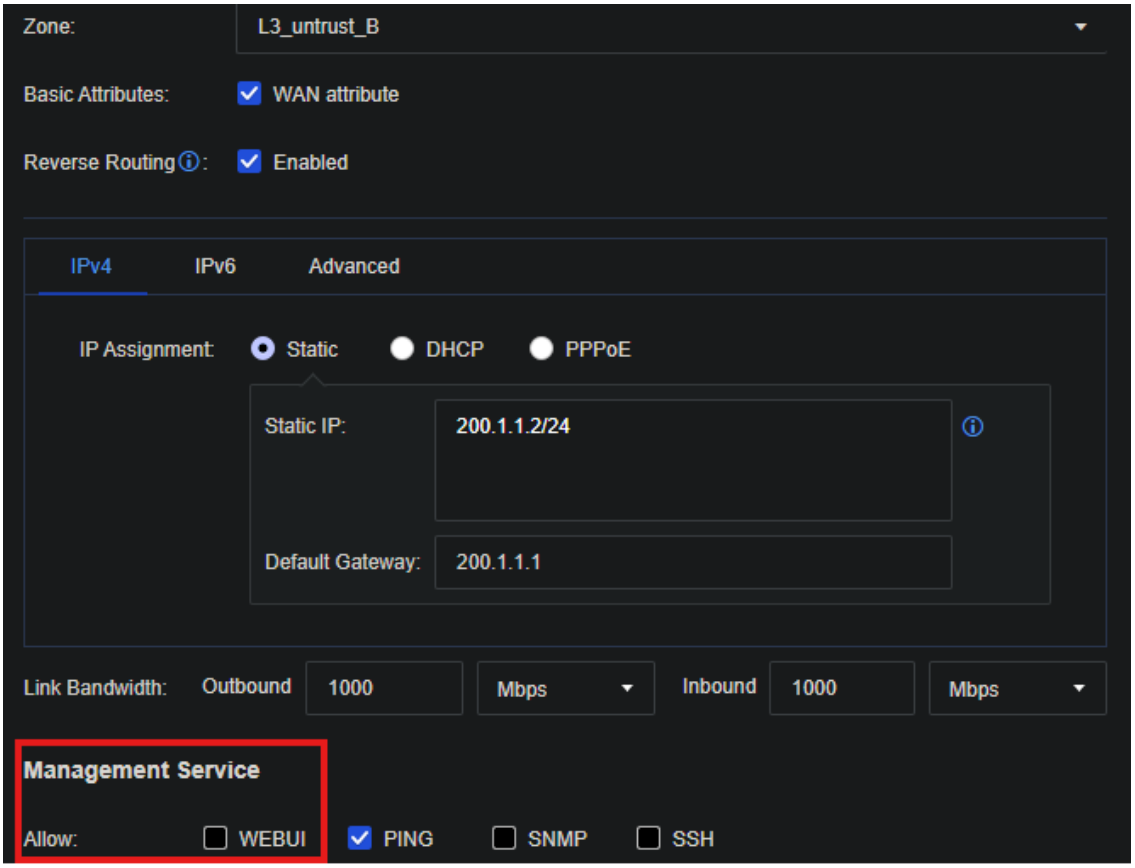
Enabling management services like HTTPS, ping, and SSH on a WAN interface increases security risks. To protect against unauthorized access and potential attacks, these services should be disabled on WAN interfaces and restricted to internal networks.

Rationale:

Management related services should only be enabled on management interface. This is part of defending the firewall from attacks and reducing the attack surface.

Remediation:

Network > Interfaces > WAN interface



Security Settings

3.1 Ensure maximum number of failed attempts allowed is set to 5 or fewer

Description:

This only takes effect if Deny access after failed attempts is enabled. The number of failed logins attempts that a user is allowed before being locked out. After making that many successive failed attempts, future attempts will fail. When one login attempt succeeds, counting of failed attempts stops, and the count is reset to zero.

Rationale:

Repeated failed login attempts could either be a valid user who has forgotten the password, or a malicious attempt to gain access to the system. For this reason, this setting should be as restrictive as possible to mitigate brute force attack attempts to discover a user's password.

Remediation:

System > General Settings > Web UI > Login Security > Max login attempts

3.2 Ensure logging is enabled on all firewall policies

Description:

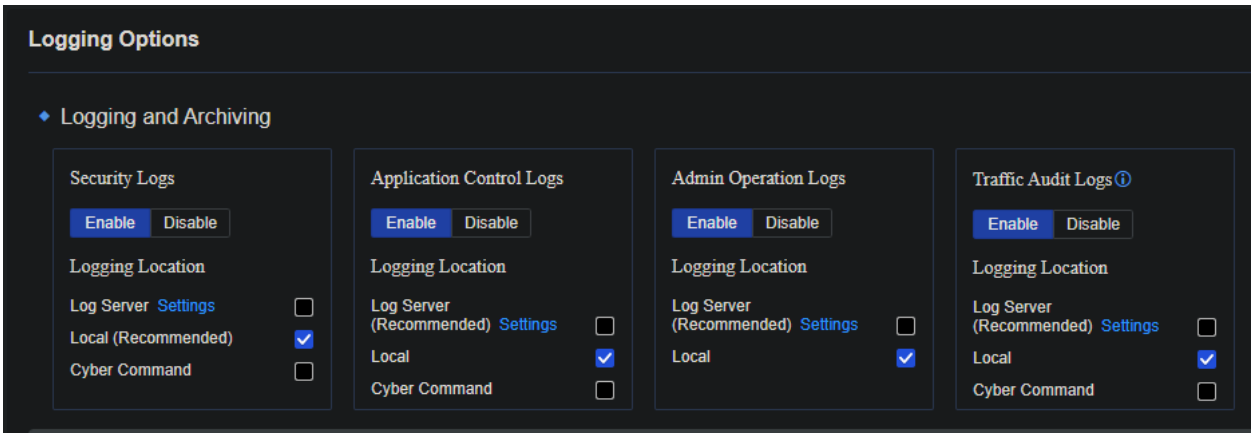
The Sangfor Network Secure offers comprehensive logging for traffic, system, and network protection activities. Logs can be used to analyze network activity, identify security issues, and mitigate network abuse. You can choose to store logs locally, send them to Sangfor aCloud, or forward them to third-party syslog servers. Logs can be filtered by module or feature, or you can opt to include all logs.

Rationale:

Comprehensive logging is essential for monitoring network activity and detecting security issues. By storing or forwarding logs, you can analyze traffic, identify potential threats, and address network abuse effectively.

Remediation:

Monitor > Loggins Options



3.3 Ensure that anti-Dos/DDOS is enabled to protect the physical firewall

Description:

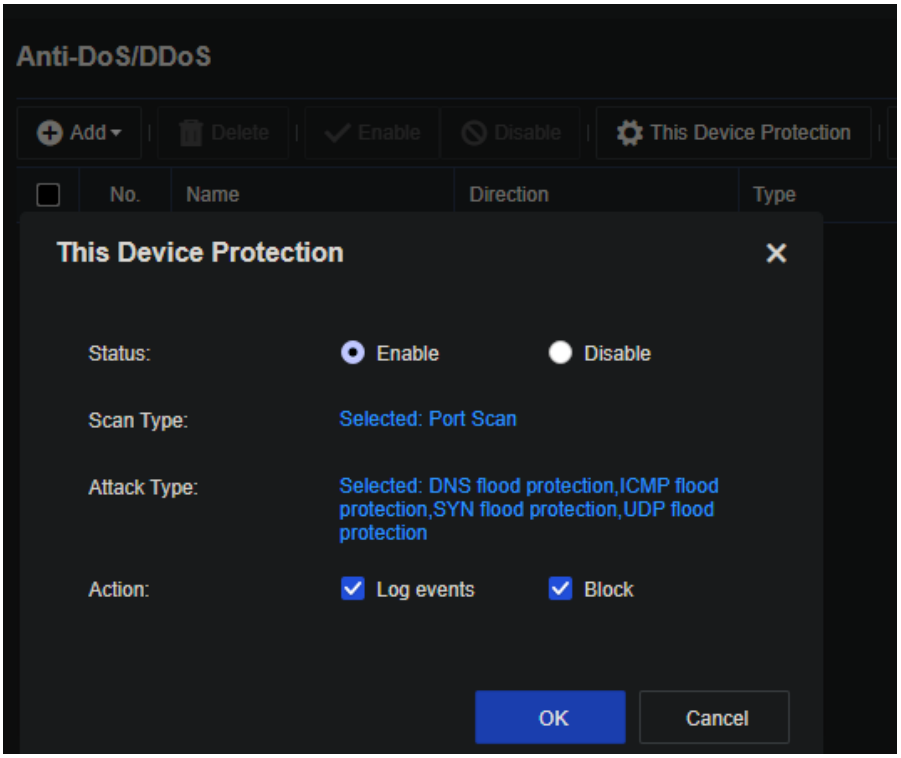
Enable anti-DDoS/DoS protections on the firewall to defend against denial-of-service attacks and enhance the firewall's resilience. This measure helps prevent service disruptions and maintains the security and availability of your network infrastructure.

Rationale:

Enabling anti-DDoS/DoS protections on the firewall is crucial for defending against denial-of-service attacks, which can overwhelm and disrupt network services. These protections help ensure the firewall remains operational and effective, maintaining both the security and availability of the network infrastructure.

Remediation:

Policies > Network Security > Anti-Dos/DDOS > This Device Protection



3.4 Apply IPS security policies for Internet and Server Scenario

Description:

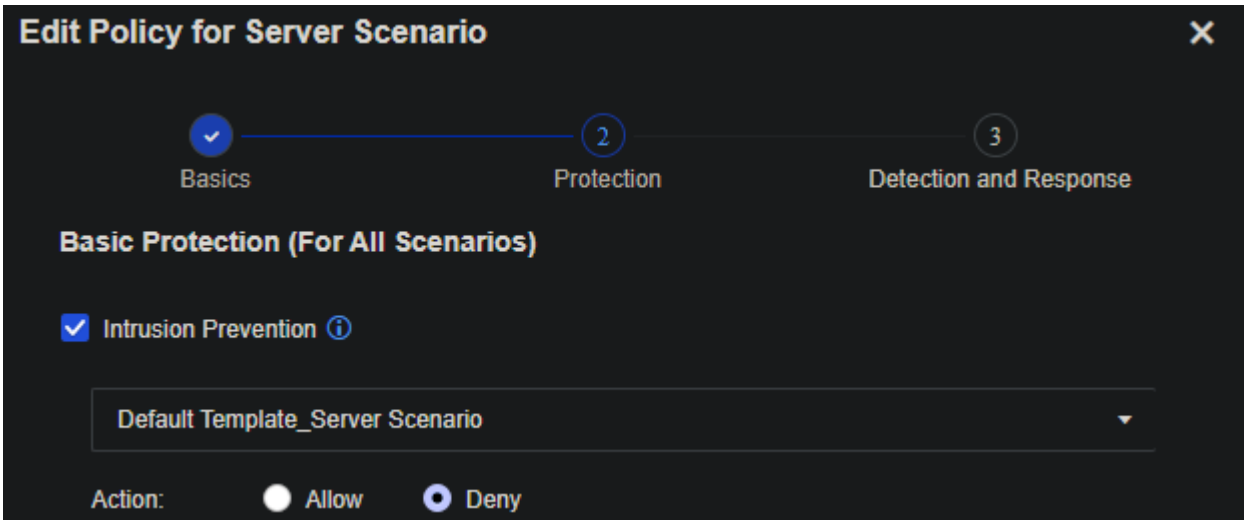
Ensuring that traffic traversing between networks on the Sangfor Network Secure have an IPS security profile inspecting it.

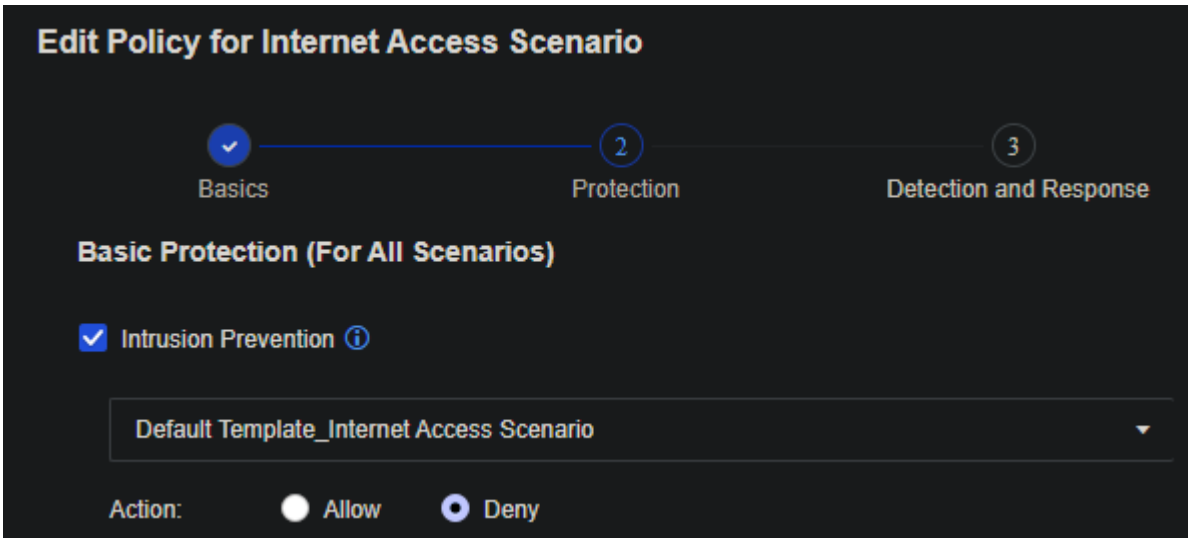
Rationale:

Traffic traversing between interfaces on the Sangfor Network Secure should have firewall policies enforced with an IPS security profile applied. This approach ensures that all inter-interface traffic is monitored and protected against threats, leveraging the Intrusion Prevention System (IPS) to detect and block malicious activity.

Remediation:

Policies > Network Security > Policies





3.5 Detect botnet connection

Description:

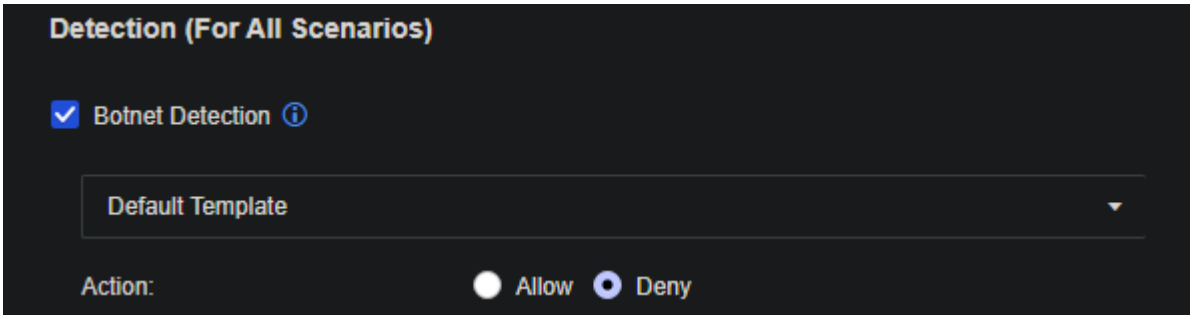
Enable botnet detection on the firewall to identify and block connections to known botnet servers, enhancing protection against malicious activities and preserving network integrity.

Rationale:

Enabling botnet detection on the firewall is essential for identifying and blocking connections to known botnet servers. This measure helps prevent malicious activities such as distributed denial-of-service (DDoS) attacks, data theft, and unauthorized access by disrupting communication with command-and-control servers.

Remediation:

Policies > Network Security > Policies



3.6 Ensure ARP spoofing protection is enabled

Description:

Enable ARP spoofing protection on the Sangfor Network Secure to prevent unauthorized devices from intercepting or manipulating network traffic. This protection helps to secure Address Resolution Protocol (ARP) communications, ensuring that IP addresses are accurately mapped to the correct MAC addresses and reducing the risk of man-in-the-middle attacks

Rationale:

By enabling this protection, you prevent attackers from intercepting or redirecting network traffic, thus maintaining the integrity of data transmission and enhancing overall network security. This measure helps ensure that network communications remain private and reliable, protecting against potential breaches and data loss.

Remediation:

Network > ARP > ARP spoofing protection

3.7 Ensure Web filter is set to block high risk categories

Description:

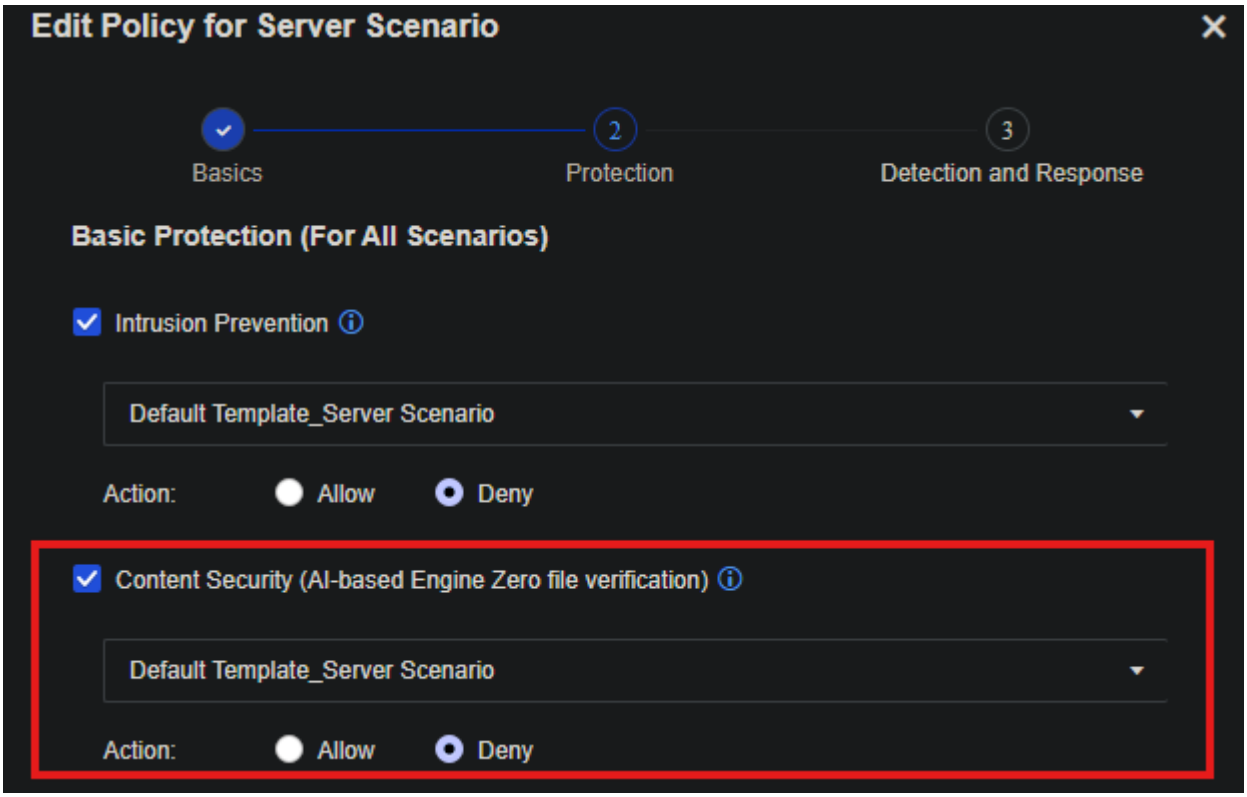
Configure the web filter on the Sangfor Network Secure to block high-risk categories, such as phishing, malware, and adult content. This setting helps prevent access to potentially harmful or inappropriate websites, reducing exposure to cyber threats and ensuring a safer browsing environment.

Rationale:

Blocking high-risk web categories is essential for mitigating security threats and protecting network users from harmful content. By restricting access to sites associated with phishing, malware, and other high-risk activities, you reduce the likelihood of cyberattacks and data breaches. This proactive measure helps maintain a secure and productive network environment, safeguarding both the integrity of your systems and the safety of your users.

Remediation:

Policies > Network Security > Policies



3.8 Block high risk categories on Application Control

Description:

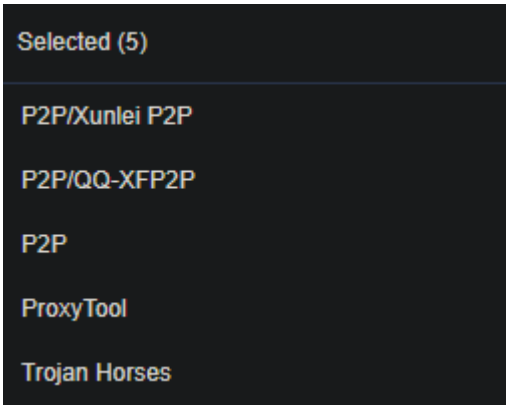
Configure Application Control on the Sangfor Network Secure to block high-risk application categories, such as peer-to-peer file sharing, and anonymizing services. This setting prevents the use of applications known to pose significant security risks or consume excessive bandwidth.

Rationale:

Blocking high-risk application categories is crucial for minimizing exposure to security threats and ensuring network stability. This measure helps maintain a secure, efficient network environment and protects against vulnerabilities associated with high-risk applications.

Remediation:

Policies > Access Control > Application Control



3.9 Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode"

Description:

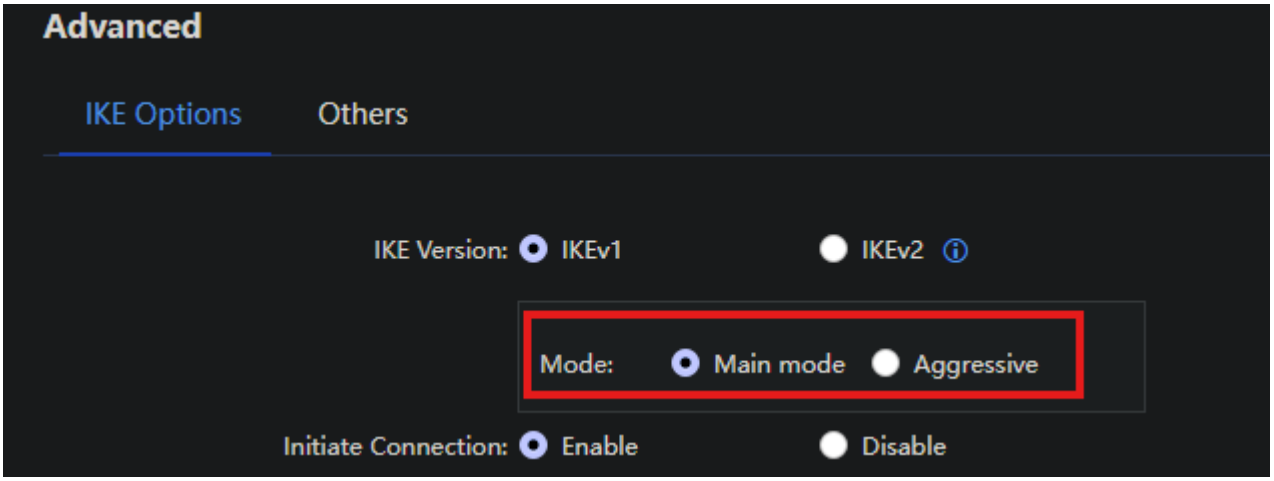
Configuring Site-to-Site IPSec VPNs with "Aggressive Mode" poses several security risks, primarily due to its reduced level of security compared to "Main Mode." Aggressive Mode accelerates the initial phase of the VPN connection by exchanging fewer messages, which can lead to faster setup but at the cost of security.

Rationale:

Configuring Site-to-Site IPSec VPNs with "Aggressive Mode" introduces security risks because it uses fewer exchanges during the key establishment process, making it more susceptible to man-in-the-middle attacks and reducing overall encryption strength. By avoiding Aggressive Mode and using "Main Mode," you ensure a more secure key exchange with stronger authentication and reduced risk of interception or unauthorized access.

Remediation:

Network > Sangfor/IPsec VPN > IPSec VPN



3.10 Ensure Ransomware protection is enabled

Description:

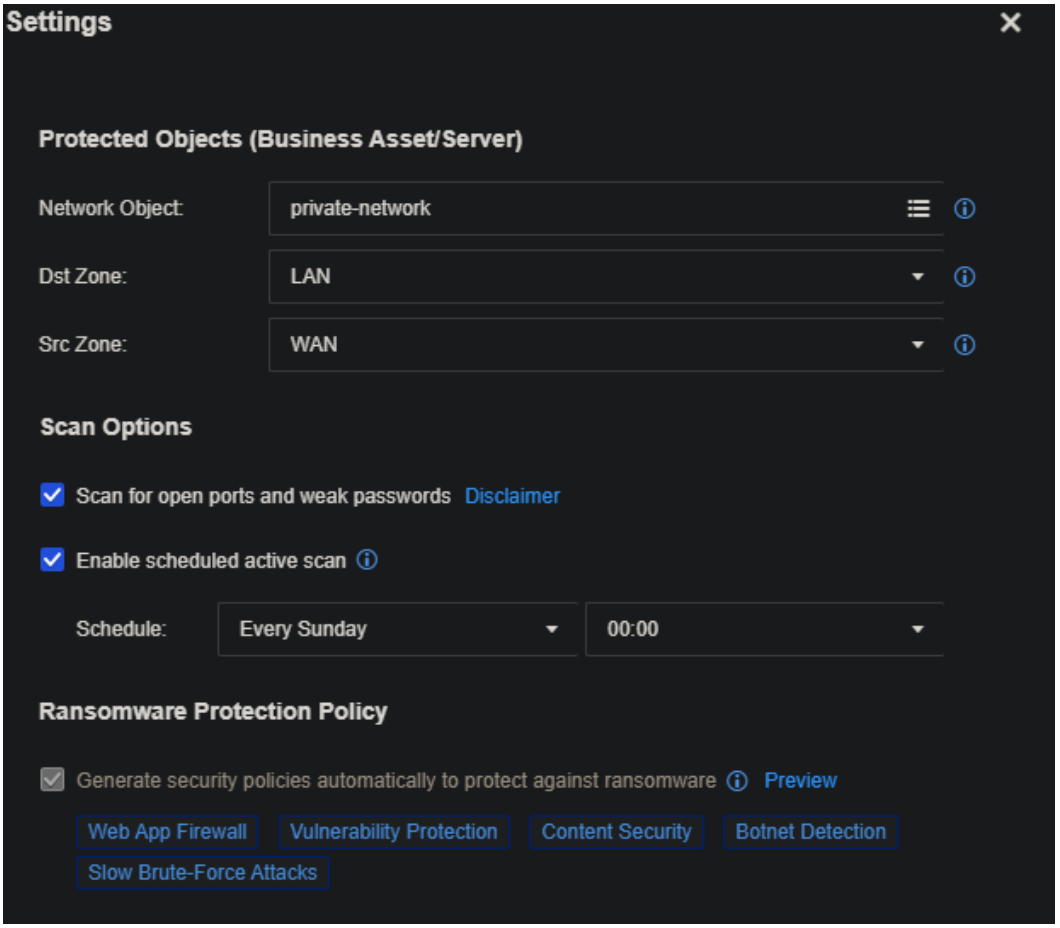
Enable ransomware protection on the Sangfor Network Secure to utilize its built-in scanning functions that identify open ports, vulnerabilities, and weak passwords across specified IP addresses. This feature helps detect potential entry points and weaknesses in your network that could be exploited by ransomware and other malicious threats.

Rationale:

Activating ransomware protection with its scanning functions is essential for proactively identifying and addressing security gaps that could be targeted by ransomware. By scanning for open ports, vulnerabilities, and weak passwords, you uncover and mitigate potential risks before they can be exploited. This reduces the likelihood of successful ransomware attacks, enhances overall network security, and protects critical data from being compromised or held hostage.

Remediation:

SOC > Specialized Protection > Ransomware Protection



3.11 Ensure that unused policies are reviewed regularly

Description:

Firewalls policies should be reviewed regularly to ensure they align with current business needs. Disable and log any unused policies. It's recommended to perform this review twice a year or in line with Business Continuity Plan (BCP) practices.

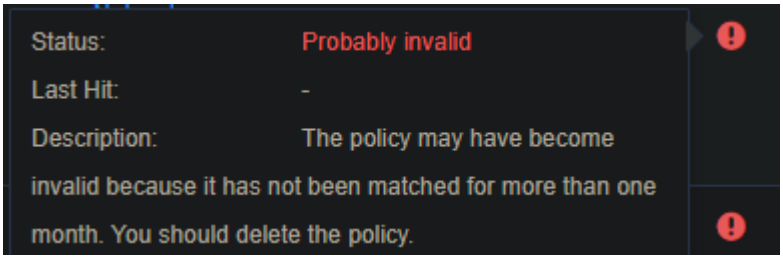
Rationale:

By reviewing policies regularly, we can determine if the policies are still needed by the business purpose. Thus, we can keep the firewall policies lean and efficient. It also prevents traffic being allowed or blocked accidently.

Remediation:

The remediation is to review and decide if you should delete unused policies.

Example:




SANGFOR