Symantec
A Division of Broadcom

SGOS 7.2.x Security Best Practices

Table of Contents

About Security Best Practices

Your appliance examines much of the traffic that passes through your network and attaches to other devices on your network; thus, it is very important to manage it securely. This documentation describes best-effort security considerations for your deployment. Consult your organization's security requirements when deploying appliances in your environment.

TIP
All command line interface (CLI) examples in this document are executed in configuration mode. To enter config mode, issue the following commands:

```
> enable
Enable Password: password
#configure terminal
Enter configuration commands, one per line. End with CTRL-Z.
#(config)
```

Before implementing the best practices described in this documentation, and as needed to maintain your deployment, refer to supporting documents available at https://techdocs.broadcom.com.

Physical Location and Networking

Secure the appliance location and networking configuration.

- **Secure the physical location where the appliance is deployed.**
  Limit access to a few top-level administrators. When possible, make sure that their access is monitored.
- **Avoid deploying an appliance with a direct connection to the Internet.**
  When possible, deploy the appliance behind a firewall to protect it from Internet-based attacks.
- **Configure management access to the appliance.**
  Methods to control access include:
  – (On applicable models) Restricting physical access to the system and requiring a PIN to access the front panel. Use the following CLI commands:

    ```
    #(config)security front-panel-pin PIN
      ok
    ```

    Alternatively, refer to “Requiring a PIN for the Front Panel” in the *SGOS Administration Guide*.
  – Restricting the IP addresses that are permitted to connect to the CLI. Use the following CLI commands:

    ```
    #(config)security allowed-access add allowed_IP allowed_IP_mask
      ok
    ```

    Alternatively, refer to “Limiting Workstation Access” in the *SGOS Administration Guide*.
  – Requiring a password to secure the Setup Console. Refer to “Securing the Serial Port” in the *SGOS Administration Guide*.
- **Prepare your network infrastructure for the connections to and from your appliance.**
  Refer to the Appendix in "Accessing the Appliance" chapter in the *SGOS Administration Guide* for a list of ports used by the appliance.
- **Disable unused network interfaces.**
  The appliance supports disabling and enabling specific adapters and VLAN IP addresses. Disable the interfaces in the Management Console by selecting **Configuration > Network > Adapters > Interfaces**. Alternatively, use the following CLI commands:

  ```
  #(config)interface interface_number
  #(config interface interface_number)disable
    ok
  ```

  All interfaces are enabled by default; thus, you can disable adapters that are not in use.

Administer and Monitor the Appliance

Use best-effort security settings for global configurations.

- **Isolate the browser.**
  ProxySG administrators access the appliance's Management Console through a web browser. For better security, do not allow the browser to access the Internet. This ensures that no web applications can glean login information or other details used in the connection to the Management Console.
- **Limit the inactivity timeout.**
  Configure inactivity timeouts:
  – For the CLI (default is 5 minutes):
  Configuration > Authentication > Console Access > Enforce CLI auto-logout
  – For the Management Console (default is 15 minutes):
  Configuration > Authentication > Console Access > Enforce Web auto-logout
  Alternatively, use the following CLI commands:

```
#(config)security management web-timeout value_in_minutes
  ok
#(config)security management cli-timeout value_in_minutes
  ok
```

  In addition, you can configure inactivity timeouts per authentication realm. Refer to "Managing Users/Logging Out Users" in *SGOS Administration Guide* for more information.
- **Do not use the ProxySG's built-in console user account for day-to-day operations.**
  The ProxySG built-in console user account does not enforce a user lockout after an excessive number of failed authentication attempts. An attacker can exploit this to repeatedly guess the console user account password. For best security, create a long, random password for this account and keep it in a secure place. Then, provide the console username and password to only a select few administrators to use only when necessary. See "Specify a minimum length for all administrator passwords" below for information on configuring passwords.
  The built-in account has additional privileges which bypass `<Admin>` authentication policy, which means that any administrative authentication policy you write will not apply to built-in user account access. For best security, create administrative authentication policy to manage administrators' access to the Management Console and SSH console. For information on using `<Admin>` authentication policy, see "Create separate administrator accounts for day-to-day operations" below.
  The built-in console user account should be used only as a fallback, for example, if access through all other administrator accounts is lost. Stop using the built-in account after restoring access through other administrator accounts.
- **Create separate administrator accounts for day-to-day operations.**
  Create separate accounts for all administrators either in a local authentication realm on the appliance or on an external authentication server accessed via IWA or LDAP, and use these accounts for normal system configuration and maintenance. Perform the following steps for additional safeguards:
  Write `<Admin>` authentication policy for local accounts, including assigning read-only read-only access for some administrator roles. For example, you could configure a policy rule that includes a group of administrators in a source object and the **Allow Read-Only Access** action object.
  You can also specify lockout times and maximum failed authentication attempts for local realm users:

```
#(config local-user-list local_user_list) lockout-duration <seconds>
#(config local-user-list local_user_list) max-failed-attempts <number_of_attempts>
```

  For best security, create a secure password for each administrator account. See "Specify a minimum length for all administrator passwords" below for information on configuring passwords.
- **Specify a minimum length for all administrator passwords.**

Because the appliance does not enforce password complexity by default, use the following CLI command to specify a minimum length for all passwords:

```
#(config)security password-min-len <length>
  Note: existing passwords are not automatically updated to meet this new length
ok
```

The password can be up to 64 characters long. As the CLI notes, existing passwords are not updated; update any existing passwords to meet the new required length.

- **Limit use of SNMP protocol to SNMPv3 only.**
  - Use only SNMPv3 for system activity reporting. Earlier versions of SNMP do not support authentication or encryption of the messages, and even send the community string as plaintext over the network. Enabling SNMPv1 and SNMPv2c exposes system activity communication to third parties. Only SNMPv3 offers authentication and encryption.

    To disable SNMPv1 and SNMPv2vc, use the following CLI commands:

    ```
    #(config)snmp
    #(config snmp)protocol snmpv1 disable
      ok
    #(config snmp)protocol snmpv2c disable
      ok
    ```

    Refer to “Configuring SNMP Communities” in the *SGOS Administration Guide* for details about configuration.
  - When configuring SNMPv3 users, select both Authentication and Privacy modes.
    - Choose SHA over MD5 when choosing the secure hash for Authentication mode, as this is the more secure of the available hashes.
    - Choose AES over DES when choosing the encryption algorithm for Privacy mode, as this is the more secure of the available algorithms.
    - Enhanced security of SNMPv3 is based on each user having authentication and privacy passphrases.

    Refer to “Configuring SNMP Users for SNMPv3” in the *SGOS Administration Guide* for details. Alternatively, use the following CLI commands:

    ```
    #(config)snmp
    #(config snmp)edit user user
    #(config snmp user user)authentication passphrase passphrase
      ok
    #(config snmp user user)authentication mode sha
      ok
    #(config snmp user user)privacy passphrase passphrase
      ok
    #(config snmp user user)privacy mode aes
      ok
    ```

    NOTE
    If you must create new community strings while unsecure SNMPv1 and/or SNMPv2c are enabled, do not provide read-write Authorization level unless doing so is unavoidable. Instead of giving the new community strings a non-trivial Authorization level (such as read-only or read-write), consider defining Access Control Lists to reduce the attack vector for malicious users. Refer to "Adding Community Strings for SNMPv1 and SNMPv2c" in the *SGOS Administration Guide* for details.
- **Secure SSH connections.**

  The appliance can accept management Secure Shell (SSH) connections. Since SGOS 6.7.2, it also has the ability to initiate SSH connections, for example, when uploading access logs over SCP . administrators can manage passwords, keys, and ciphers to secure SSH communication.

  Do the following for inbound connections on SSH console:

– Use public key-pair authentication instead of password authentication. The former is more secure for several reasons (for example, it is not susceptible to phishing, has a lower risk of human error, does not involve over-the-wire transfer).
– For better security, if creating the host key pair with an RSA key, specify a key size of 2048, 3072, or 4096 bits.
  If a lower-bit key is currently configured for the SSH console, remove it:
  ```
  # (config ssh-console) delete host-keypair rsa
  ```
  Then, create an RSA key with a size of 2048 bits or 3072 bits, as in the following example:
  ```
  # (config ssh-console) create host-keypair rsa 3072
  ```
  If using the Management Console to create the host key pair, go to **Configuration > Authentication > SSH Inbound Connections > SSH Host Keys**. If a lower-bit key is currently specified in the RSA Host Key Pair section, select **Delete** to remove it before creating a new key. To create a new key, select **2048** , **3072**, or **4096**. Refer to “Managing the SSH Host Key Pairs” in the *SGOS Administration Guide* for more information.
– Use stronger ciphers and HMACs for communication. By default, the appliance ships with five enabled ciphers and ten enabled HMACs. Enable additional ciphers and HMACs only if necessary and disable them after use if the connection is temporary. Refer to “Managing SSH Ciphers for Inbound Connections” and “Managing SSH HMACs for Inbound Connections” in the *SGOS Administration Guide* for details.

Do the following for the outbound SSH client:

– To make an outbound connection, the appliance requires known host specification, including a key pair for every host. If communication with a specific host is temporary, delete it when it is no longer required. Refer to “Delete Known Hosts” in the *SGOS Administration Guide*.
– Use stronger ciphers and HMACs for communication. By default, the appliance ships with six enabled ciphers and ten enabled HMACs. Enable additional ciphers and HMACs only if necessary and disable them after use if the connection is temporary. Refer to “Managing SSH Ciphers for Outbound Connections” in the *SGOS Administration Guide* for details.
– The appliance allows you to prioritize ciphers and HMACs for outbound connections and a conformant SSH server should honor this prioritization. The ciphers in the Available list are listed in order of cipher strength. Replicate this order in the Selected ciphers list.
  After an upgrade or downgrade, the Selected list of ciphers and HMACs may change. General rules are described in appropriate sections in the *SGOS Administration Guide*.

- **Secure communication with SSL device profiles.**
  By default, the appliance ships with three predefined SSL profiles for secure non-proxy communication. This communication includes peer-to-peer communication as well as communication with external services. The default profile can only be edited, but you can create new profiles.
  Do the following for SSL device profiles:
  – By default, the appliance does not include weak ciphers in device SSL profiles. When editing an existing profile or creating a new profile, do not add weak ciphers to the profile configuration.
  – When creating a new profile, limit the TLS protocol version to the strongest that is supported by the remote SSL host.
  – When creating a new profile, leave the peer verification option enabled. With peer verification enabled, the appliance will perform a set of checks to ensure any received certificates are both trusted (as determined by the CA certificates contained within the specified CCL) and valid (that is, not expired).
- **Enable all email and other alerts.**
  Direct emails and alerts to addresses and services that can be viewed by multiple administrators.
- **Set maximum number of failed attempts for the local user database.**
  Configure a local user database so that each user account is automatically disabled if too many failed login attempts occur within a specified period, which might indicate a brute-force password attack on the appliance. To modify security settings, use the following CLI:
  ```
  #(config)security local-user-list edit list_name
  #(config local-user-list list_name)max-failed-attempts number_of_attempts
  ```

```
  ok
#(config local-user-list list_name)lockout-duration duration_in_seconds
  ok
#(config local-user-list list_name)reset-interval interval_in_seconds
  ok
```

Make sure that your settings adhere to your corporate password security policy.

- **Configure separate authentication realms for administrators and end users.**
  Configure different local realms for administrative and end-user (proxy) authentication. This precaution ensures that administrators are not locked out in case of a brute-force password-guessing attack by an end user attempting to authenticate to the proxy.
- **Set failed attempts and other secure authentication parameters for external authentication services.**
  Refer to the *SGOS Administration Guide* for specific external authentication service setup.
- **Use Content Security Policy for threat protection.**
  See Use Security Policy for details.
- **Use HTTPS for ICAP scanning (Secure ICAP).**
  Secure ICAP communication when setting up Content Analysis . Select **Always use secure connections** when setting up or modifying the existing malware scanning service. Refer to “Selecting the Connection Security Mode” in the *SGOS Administration Guide*.
- **Secure access log uploads.**
  The appliance offers various options to secure access log transfer:
  – Configure a secure upload client to keep data confidential. The appliance supports several upload clients: Custom, HTTP, FTP, SCP, and Kafka. All the clients include the **Use secure connections (SSL)** option. Enable this option.
  – Encrypt the access log to keep data confidential. Refer to “Encrypting the Access Log” in the *SGOS Administration Guide*. If configuring a secure upload client is not possible, use this feature instead.
  – Sign the access log to ensure data integrity. Refer to “Digitally Signing Access Logs” in *SGOS Administration Guide*.
- **Secure policy downloads via remote URL.**
  The appliance provides three methods for downloading and installing policies: from a text editor, from a local file, and via a remote URL. If you update policy via remote URL, use the HTTPS protocol to protect the privacy and integrity of the installed policy.
  In the Management Console (**Configuration > Policy > Policy Files > Policy Files** and **Configuration > Policy > Policy Files > Visual Policy Files**), specify a URL in the form *`https://policy_file_path`* for the appropriate policy file type.
  Alternatively, specify the URL using the CLI command:

```
#(config)policy policy_file -path url
```

  In addition to the policy file types supported in the Management Console, the CLI allows you to configure URLs for the landlord, tenant, and VPM classification policy files.
  If you use a device profile other than the default SSL security profile for policy download, follow the recommendations in Secure communication with SSL device profiles.

Secure the HTTPS Management Console

Secure the HTTPS Management Console (web interface).

- **Do not enable HTTP web management.**
  By default, only HTTPS web administration is enabled. Do not enable the HTTP Management Console. If it is enabled, disable it following instructions in “Creating a Management Service” in the *SGOS Administration Guide*.
- **Introduce a separate entity certificate for the management port.**
  Do not rely on the self-signed certificate provided by default. The appliance ships with a predefined default keyring with a certificate serving as the entity certificate for management services, as well as a Certificate Authority (CA) certificate for emulated SSL certificates. Before deploying the appliance, create a new entity certificate for management services with a signing algorithm and keys confirming your corporate security policy. See “Creating a Keyring” in the *SGOS Administration Guide* on how to create new keyrings and import certificates.
- **Use a more secure TLS version to harden the SSL connection.**
  By default, only TLSv1.1, TLSv1.2, and TLSv1.3 are enabled and supported. Disable TLSv1.1 and using the more secure TLSv1.2 or TLSv1.3.
- **Use more secure cipher suites to harden the SSL connection.**
  By default, the HTTPS Management Console comes with 22 ciphers enabled. Disable all ciphers that operate in CBC mode and enabling more secure ciphers that operate in GCM, CCM, or stream mode. For example, enable the following list of ciphers:
  – tls_aes_256_gcm_sha384
  – tls_chacha20_poly1305_sha256
  – tls_aes_128_gcm_sha256
  – tls_aes_128_ccm_8_sha256
  – tls_aes_128_ccm_sha256
  – ecdhe-rsa-aes256-gcm-sha384
  – ecdhe-rsa-aes128-gcm-sha256
  – aes128-gcm-sha256
  – aes256-gcm-sha384
  – dhe-rsa-aes128-gcm-sha256
  – dhe-rsa-aes256-gcm-sha384

SSL Proxy Best Practices

Use best practices for SSL connections.

- **Use more secure TLS versions to harden the SSL connection.**
  By default, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 are all enabled for SSL proxy traffic. The use of SSLv3, TLSv1.0, or TLS 1.1 is not recommended due to various vulnerabilities in these protocol versions.
  For best security, use the following CPL gestures:

```
<ssl>
  client.connection.negotiated_ssl_version=(SSLV3,TLSv1,TLSv1.1) force_deny
<ssl>
  server.connection.negotiated_ssl_version=(SSLV3,TLSv1,TLSv1.1) force_deny
```

  Before disabling SSLv3, TLSv1.0, and TLS 1.1, verify that all clients and servers with traffic going through the appliance support TLSv1.2 or later.
- **Use more secure cipher suites to harden the SSL connection.**
  The appliance uses the first cipher suite offered by a client, even if it is a lower grade. For better security, allow only cipher suites that meet your minimum acceptable level of security. the HTTPS Management Console comes with 22 ciphers enabled. Disable all ciphers that operate in CBC mode and enabling more secure ciphers that operate in GCM, CCM, or stream mode. For example, enable the following list of ciphers:
  – tls_aes_256_gcm_sha384
  – tls_chacha20_poly1305_sha256
  – tls_aes_128_gcm_sha256
  – tls_aes_128_ccm_8_sha256
  – tls_aes_128_ccm_sha256
  – ecdhe-rsa-aes256-gcm-sha384
  – ecdhe-rsa-aes128-gcm-sha256
  – aes128-gcm-sha256
  – aes256-gcm-sha384
  – dhe-rsa-aes128-gcm-sha256
  – dhe-rsa-aes256-gcm-sha384
  In addition, four less secure ciphers are supported (ECDHE-RSA-RC4-SHA, DES-CBC3-SHA, RC4-SHA, RC4-MD5) but not enabled. Do not enable the less secure ciphers.
- Use CPL such as the following to harden the list of cipher suites:

```
<ssl>
  client.connection.negotiated_cipher.strength=(low,medium) force_deny

<ssl>
  server.connection.negotiated_cipher.strength=(low,medium) force_deny
```

CAUTION
Denying all low and medium strength ciphers might prevent communication with older clients or servers. If this occurs, review the allowed ciphers and adjust the previous policy to enable appropriate ciphers for successful traffic flow.

In releases prior to SGOS 7.2.x, Symantec recommended the following policy, which is no longer recommended because the listed cipher suites are no longer available.

NOTE
If your policy contains the following CPL or reference to the deprecated low strength ciphers, remove the references. If the references are not removed, policy will compile and a warning message will be issued.

```
<ssl>
```

```
  client.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5, \
    EXP-DES-CBC-SHA) force_deny

<ssl>
  server.connection.negotiated_cipher=(EXP-RC4-MD5,EXP-RC2-CBC-MD5, \
    EXP-DES-CBC-SHA) force_deny
```

For more information, refer to documentation on behavior changes in SGOS 7.2.x.

CAUTION
Even with the recommended CPL gestures in policy, scanners scanning the SSL proxy port might identify weak ciphers and/or vulnerable protocol versions. These false positives arise due to how the appliance handles SSL negotiations. When scanning the port, the scanner targets the appliance as if it were an origin content server (OCS). The appliance responds with a successful negotiation of the (potentially weak) cipher suite and (potentially old) SSL/TLS version—even when it intends to reject the request—in order to return the reason for the rejection to the client. In this case, no request information is ever sent to the actual OCS using a weak cipher.

- **Create a certificate signed by a trusted CA.**
  Do not rely on the self-signed certificate provided by default. Before deploying your appliance, create a new SSL interception keyring and replace the built-in self-signed certificate with one signed by a CA conforming to your PKI and your security policy. Follow instructions in “Create a CA-Signed Certificate” in the *First Steps Deployment Guide* to generate a CSR and issue the appropriate certificate.
- **Do not disable server certificate validation.**
  In a forward proxy deployment, server certificate validation is enabled by default. The following certificate parameters are validated: expiration, untrusted issuer, revocation and—in a non-tunneling case—hostname mismatch. Do not write policy that disables server certificate validation.

  NOTE
  Refer to "SSL Proxy Best Practices" in *SSL Proxy Deployment Guide* for descriptions of various specialized scenarios and how to handle them.

Reverse Proxy Best Practices

The *ProxySG Reverse Proxy Deployment Guide* provides guidance for various deployment scenarios and best practices. Follow the instructions in the deployment guide and take the following additional steps:

- **Disable unused services.**
  In a reverse proxy deployment, the appliance IP address is usually visible to the Internet; thus, it is important to enable only the proxy services that are in use. Every enabled proxy service port will be visible to external scanners.
- **Use more secure TLS versions to harden the SSL communication for the HTTPS Reverse Proxy service.**
  Disable TLSv1.0 due to various vulnerabilities in that protocol version.
  – Downstream connection: By default, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 are enabled for accepting downstream connections by the HTTPS Reverse Proxy service. To disable TLSv1.0 in the HTTPS reverse proxy service, refer to “Creating an HTTPS Reverse Proxy Service” in the *SGOS Administration Guide*.
  – Upstream connection: If HTTPS is used for upstream connections to the OCS, disable TLSv1.0 through SSL Client settings. Refer to “Editing an SSL Client” in the *SGOS Administration Guide*. Alternatively, use the following CLI commands:

```
#(config)ssl
#(config ssl)edit ssl-client default

#(config ssl default)protocol tlsv1.1 tlsv1.2 tlsv1.3
  ok
```

- **Use more secure cipher suites to harden the SSL communication for the HTTPS Reverse Proxy service.**
  As with SSL device profiles, the appliance by default does not include weak ciphers in the default SSL client. When editing an existing SSL client or creating a new one, do not add weak ciphers to the profile configuration. If weak ciphers were previously enabled, disable them through SSL Client settings. Refer to “Changing the Cipher Suite of the SSL CLI” in the *SGOS Administration Guide*. Alternatively, use the following CLI commands:

```
#(config)ssl

#(config ssl)edit ssl-client default

#(config ssl default)cipher-suite


Cipher#  Use        Description               Strength
-------  ---  --------------------------  --------
1        yes     ECDHE-RSA-AES256-SHA384      High
2        yes     ECDHE-RSA-AES128-SHA256      High
3        yes     ECDHE-RSA-AES256-GCM-SHA384  High
…

Select cipher numbers to use, separated by commas:
```

- **Enable client certificate validation.**
  For mutual authentication, enable client certificate validation using either of two methods:
  – Implicitly, when creating/editing the HTTP Reverse Proxy service. Refer to “Creating an HTTPS Reverse Proxy Service” in the *SGOS Administration Guide*.
  – Explicitly, using the following CPL:

```
<ssl>
  client.certificate.validate(yes)
```

Web Application Firewall Best Practices

The *Web Application Firewall Solutions Guide* provides guidance for various deployment scenarios and best practices. Follow the instructions in the guide and take the following additional steps:

- **Implement all of steps in Reverse Proxy Best Practices**#unique_7/unique_7_Connect_42_Reverse.
- **Make sure that your Application Protection subscription is updated.**
  Update the Application Protection subscription using the following CLI:

```
#(config)application-protection
#(config application-protection)view
Version:                20170126
Notify Only:            Enabled
License Type:           Demo
Licensed Until:         Sun, 08 Jul 2018 00:00:00 UTC
Service:                Enabled
Download method:        Direct
Last successful download:
  New version 20171025 is available. Initiate a manual download to update to this new version.
```

  If the output does not indicate an outdated database or other download issue, you do not have to initiate a new download. In the example above, the database is out-of-date. Download a new database using the following CLI:

```
#(config application-protection)download get-now force
Time:                 Thu, 18 Jan 2018 14:58:28 UTC
Downloaded from:      https://subscription.es.bluecoat.com/application-protection/database
```

  Alternatively, refer to “Verifying the Database Download” in the *SGOS Administration Guide*.

Use Security Policy

Two pre-configured policies, Access Security Policy and Content Security Policy, are available in this release. These policies are configured through the web Visual Policy Manager (VPM) and require minimal manual input and deployment time. Use this feature to implement best-practices security coverage out of the box, and to facilitate setup, deployment, and testing of policies.

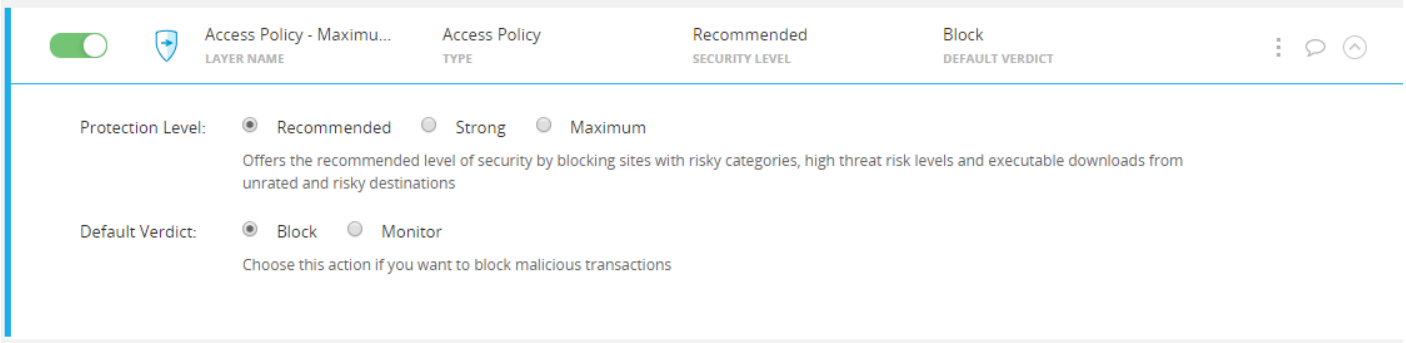
This feature provides the following benefits over manually writing policy:

- Implementation time; effect is immediately apparent and especially useful in evaluation deployments and mid-sized organizations.
- Applies security policy to protect users first, allowing you to customize your policy with more complex rules as you learn how to use VPM/CPL.
- Incorporates existing best practices published by Symantec leveraging URL Threat Risk Levels, URL categories, and content scanning recommendations.
- Offloads managing and updating of policy to Symantec (via the Policy Services subscription on SGOS).

The underlying policy definitions required for this feature are delivered through the Policy Services subscription. Both Access and Content Security policies are disabled by default.

For more information on this feature, refer to the *ProxySG Web Visual Policy Manager Reference* and the "Using Policy Services" chapter in the *SGOS Administration Guide* (7.x).

- **Activate Access Security policy.**
  The following example shows options for an initial Access Security policy activation in the web VPM:



  After adding the policy layer, select one of the three security levels:
  - **Recommended**: Offers the recommended level of security by blocking sites with risky categories, high threat risk levels, and executable downloads from unrated and risky destinations.
  - **Strong**: Includes the Recommended security protection, plus additional categories and threat risk levels.
  - **Maximum**: Includes the Strong security protection, plus additional categories and threat risk levels. This protection level may result in a higher level of false positives, requiring some custom policy overrides for users that require access to ambiguous sites.

  Once activated, the policy is in effect and starts blocking dangerous transactions based on the selected level. Two action modes determine whether a request will be blocked or monitored:
  - **Block**: The transaction is denied and the client receives an exception page (force_exception)
  - **Monitor**: The transaction is not denied. Instead, the policy populates the `x-bluecoat-access-security-policy-action` and `x-bluecoat-access-security-policy-reason` fields in the access log.

  Refer to these log fields to help validate the policy in complex environments where the outright deployment in block mode is not considered acceptable, and an additional phase of monitoring the real-world results is desired.

The operation of Security Policy depends on the selected level. In detection coverage, each level is the superset of the previous level.

Refer to https://knowledge.broadcom.com/external/article/174668 for a summary of the requests that are blocked or monitored at each protection level.

- **Identify Access Security policy exceptions.**

  When a transaction is blocked due to Access Security policy, an exception such as the following exception occurs:

  Access Denied (policy_denied)

  Request is blocked by Access Security Policy. Recommended Security Level - Request blocked - Problematic category.

  Additional information:
  HTTP Method - GET
  Client - 10.160.5.219
  URL - http://elite-hackers.com/
  URL Category - Malicious Sources/Malnets
  Threat Risk Level - 10.

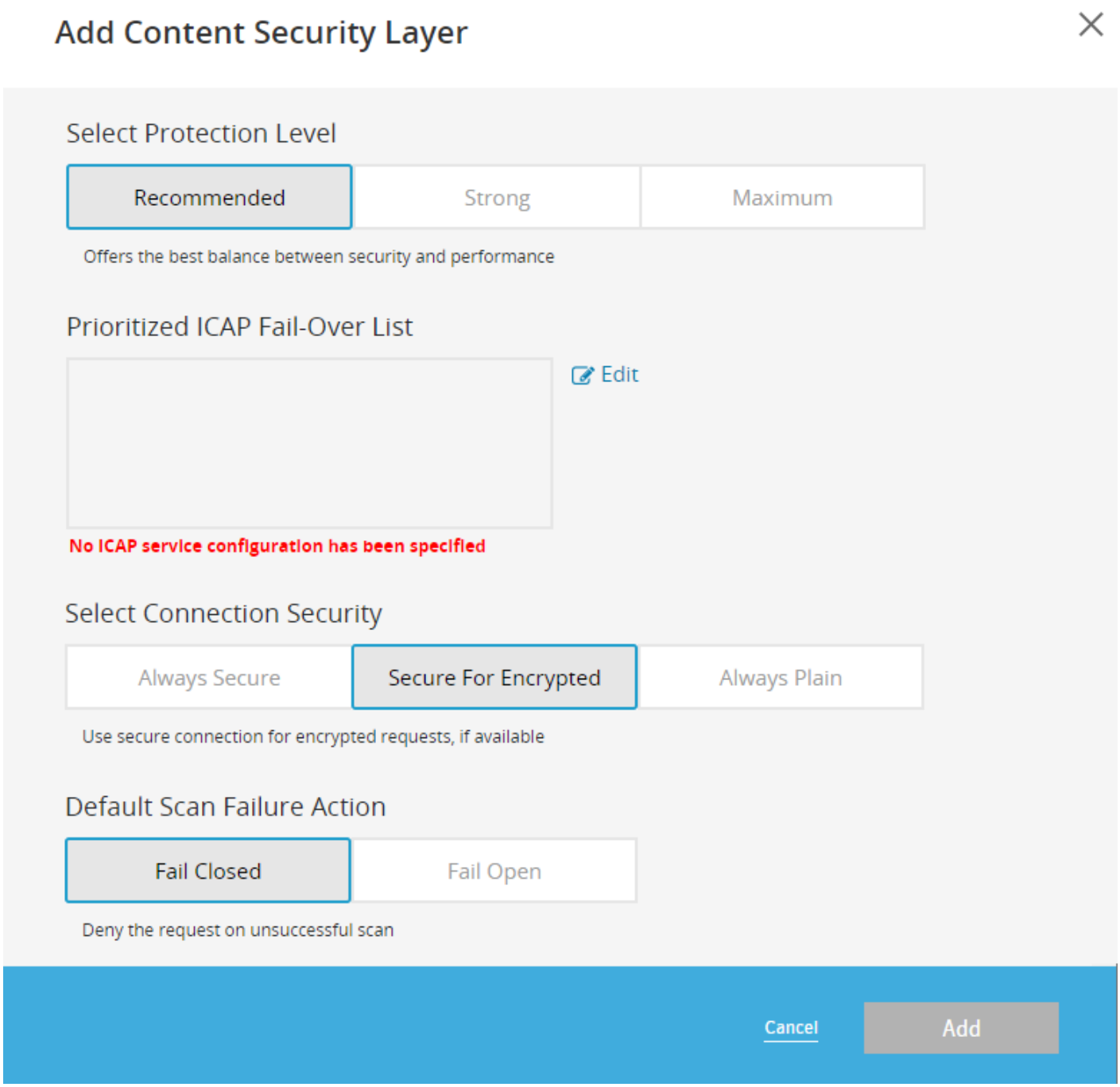
  Transaction ID: c27001ec614d1217-0000000000000169-000000005ce8006d

  For assistance, contact your network support team.

  The exception includes basic actionable information about the blocked transaction.

- **Activate Content Security Policy.**

  The following example shows options for an initial Content Security policy activation in the web VPM:



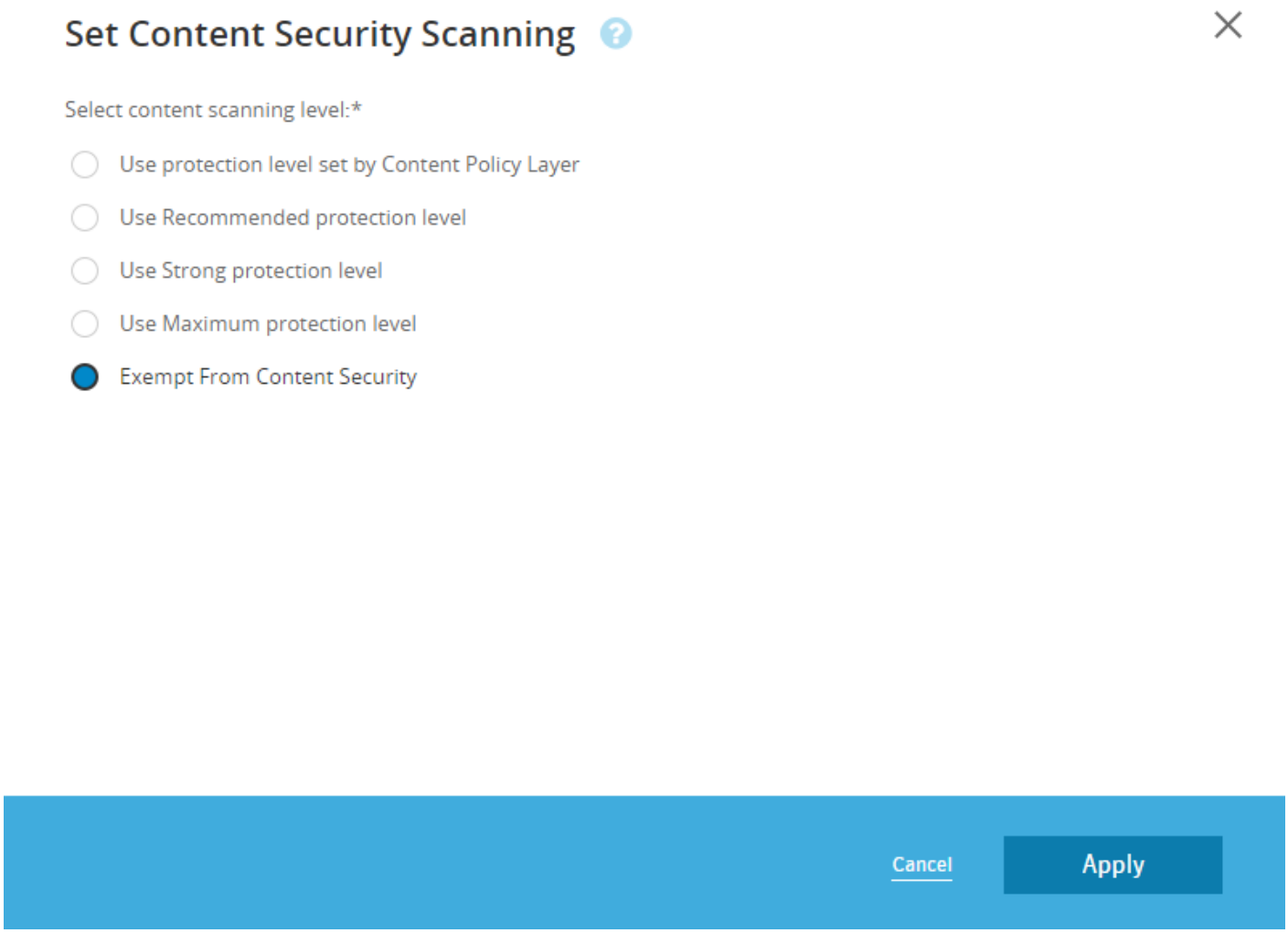
After adding the policy layer, select one of the three security levels:

– **Recommended**: Offers the best balance between security and performance.
– **Strong**: Includes the Recommended security protection, plus additional scanning for images and includes scanning for additional web applications.
– **Maximum**: Includes the Strong security protection, plus additional scanning for all destinations .

The **Prioritized ICAP Fail-Over List** accepts a prioritized list of ICAP services or groups, where the first healthy service or group in the list is chosen for content analysis. ICAP servers and ICAP service groups (for load balancing to multiple ICAP servers) must be created through the Management Console or CLI first before they are selected here.

Refer to https://knowledge.broadcom.com/external/article/174669 for a summary of security and performance at each protection level, as well as what is bypassed at each level.

- **Override Content Security Policy.**
  You can override the global protection level for Content Security Policy. In the web VPM, add a **Web Content Layer** and configure a **Set Content Security Scanning** action object.



- **Create exemptions to reduce false positives.**
  To help reduce false positives, you can add exemption rules to specific policy layers.

Security Policy Type	Policy Layer for Exemption Rule	Action Object
Access Security	Web Access Layer	Exempt From Access Security
Content Security	Web Content Layer	Set Content Security Scanning

For example, a specific user or user group can be exempted. Using exemption rules has no effect on policy while Security Policy is disabled.

WARNING
When building the exemption, you must consider policy timing. For example, if an exemption is based on response type and Access Security Policy blocks the transaction at an earlier time because the request is classified as a security category or high URL Threat Risk Level, the exemption will not apply.


Symantec
A Division of Broadcom