Integrating Content Analysis with other Symantec Products: ProxySG and Malware Analysis

Content Analysis Version 2.4
# Contents

## Introduction ........................................................................................................... 5
   Audience .................................................................................................................. 5

## Supported Symantec Devices and Operating Systems ........................................ 5
   Hardware Platforms .................................................................................................. 5
   Software Versions ..................................................................................................... 6

## Benefits of Using Symantec's Integrated Solution ............................................. 7
   About Malware .......................................................................................................... 8

## The Symantec Threat Protection Solution .......................................................... 8
   Supported Anti-Malware Engines ............................................................................. 9
   Scanning Services: RESPMOD vs. REQMOD ....................................................... 9
   Communication Between the ProxySG and Content Analysis Appliances ........... 9

## Deployment ............................................................................................................. 11
   Deployment Guidelines ............................................................................................ 12
      One ProxySG to One Content Analysis Appliance .............................................. 12
      Redundant Appliance Topologies ........................................................................ 13
   Deployment Workflow .............................................................................................. 17
      Configure and Install the ProxySG Appliance ...................................................... 17
      Configure and Install the Content Analysis Appliance ........................................ 19
      Install and Configure the Malware Analysis Appliance ...................................... 20

## Configure Symantec Appliances to Communicate ............................................. 22
   Enable Secure ICAP Connections .......................................................................... 23
   Configure ICAP Policy on a ProxySG Appliance .................................................... 29
      Automatically Configure an ICAP Service on the ProxySG ................................ 30
      Manually Configure an ICAP Service on the ProxySG ....................................... 36
      Configure ICAP Policy ......................................................................................... 39
      Configure Scanning Exemption Policies .............................................................. 42
   Test the Threat Protection Policy ............................................................................ 46
   Configure Malware Analysis .................................................................................... 48

## Monitor ICAP Scanning ......................................................................................... 51
   Display ICAP Graphs and Statistics on the ProxySG ............................................. 52
      Display Content Analysis ICAP Graphs on the ProxySG .................................... 52
      Display ICAP Statistical Data ............................................................................... 54
      Monitor ICAP-Enabled Sessions on the ProxySG ............................................... 55
   View Statistics on the Content Analysis Appliance ............................................. 57
      View Cache Hits .................................................................................................. 57
View the Sandboxing Report ................................................................. 58
View the File Reputation Report ......................................................... 59
View the Predictive Analysis Report ...................................................... 60
View the Whitelist and Blacklist Reports ................................................ 61
View Number of Bytes Scanned ............................................................ 62
View Number of Objects Scanned .......................................................... 63

View Malware Reports in Symantec Management Center and Reporter ............... 65

Fine-Tune the Configuration .................................................................. 69

Improve the User Experience ................................................................. 70
Patience Pages ...................................................................................... 70
Data Trickling ....................................................................................... 70
Deciding Between Data Trickling and Patience Pages ................................. 71
Deferred Scanning ............................................................................... 72
Configure ICAP Feedback ..................................................................... 73
Enable Deferred Scanning .................................................................... 74

Configure Email Alerts .......................................................................... 74
Configure E-Mail Settings ..................................................................... 76

Customize the Malware Scanning Policy .................................................... 77
Example: Customize the Malware Scanning Policy ..................................... 78

Create User-Based ICAP Policy ............................................................... 79
Enable Web Authentication ................................................................... 80
Create Authorization Rules .................................................................. 81

Implement a Request Modification ICAP Service ..................................... 85
Create an ICAP Request Service ............................................................ 85
Create an ICAP Request Policy - Forward Proxy/DLP ................................. 86

Load Balance Multiple Content Analysis Appliances .................................. 90
About ICAP Service Groups .................................................................. 90
Weighting ............................................................................................. 91
Load Balancing .................................................................................... 91
Example 1 ............................................................................................ 92
Example 2 ............................................................................................ 92
Specify Weight within an ICAP Service Group ......................................... 92
Create Load Balancing Policy ................................................................. 93

Configure Content Analysis Failover ....................................................... 95
Create Content Analysis Failover Policy .................................................. 95

Configuration Best Practices ................................................................. 98
Conserve Scanning Resources ................................................................. 99
Symantec Content Analysis 2.4

Scan-and-Serve Policy Using Mirroring ................................................................. 99
Avoid Processing of Canceled Connections ............................................................ 102
Antivirus Scanning Best Practices ........................................................................ 102
  Vendor-Specific Settings ...................................................................................... 103
Sandboxing Best Practices ..................................................................................... 103

Troubleshoot ProxySG+Content Analysis Integration Problems .......................... 105
  Content Analysis is not scanning web traffic ....................................................... 106
  Users cannot access any websites ...................................................................... 106
  ProxySG runs out of memory during heavy traffic load ........................................ 110
  Scans are taking too long .................................................................................... 110
  Content Analysis is not getting virus updates ..................................................... 110
  Firefox bypasses Content Analysis processing .................................................. 111
Introduction

Symantec Content Analysis, Blue Coat ProxySG, and Symantec Malware Analysis appliances work in concert to provide a cohesive threat protection solution. This document provides conceptual information about malware threats, deployment guidelines and configuration steps for getting the Symantec appliances to communicate with each other. It also includes best practices to consider when deploying this integrated solution.

This integration guide supplements existing product-specific guides. For details and instructions on each product, use the context-sensitive online help or refer to the following guides:

- Content Analysis WebGuide
- Blue Coat ProxySG SGOS Administration Guide
- Malware Analysis Administration Guide
- The Quick Start Guide poster for each Symantec appliance

You can download these manuals from MySymantec at:


Audience

The intended audience for this document is current and potential customers seeking to understand Symantec’s threat protection solution; it provides configuration information to help integrate Content Analysis, ProxySG, and Malware Analysis in your network.

This document assumes you are knowledgeable with basic network concepts and terminology. Basic familiarity with Symantec products is also recommended but not a prerequisite.

Supported Symantec Devices and Operating Systems

As of the production of this document, the integration guide covers the following Symantec products and software releases.

Hardware Platforms

The integration guide assumes you are using the supported models below:

- **ProxySG**—SG-S200, SG-S400, SG-S500, SG300, SG600, SG900, SG9000, VSWG
- **Content Analysis**—CAS-S200, CAS-S400, CAS-S500, CAS-V100 (CAS-VA)
- **Malware Analysis**—MAA-S400
Symantec Content Analysis 2.4

Software Versions

This guide assumes that the following software versions are installed on your Symantec appliances:

- **ProxySG**—SGOS 6.5 or later
- **Content Analysis**—version 2.4 or later
- **Malware Analysis**—version 4.2 or later

Some of the features such as ICAP mirroring policy and using the built-in threat protection policy on the ProxySG are not available in earlier versions. If you are consulting this guide and your software is more current than the ones listed above, review the release notes for that release to learn about any new features not yet implemented in this guide.
Benefits of Using Symantec's Integrated Solution

This chapter includes conceptual information about malware and describes benefits of using the integrated Symantec threat protection solution.

About Malware ........................................................................................................................................... 8
The Symantec Threat Protection Solution .................................................................................................. 8
Supported Anti-Malware Engines .............................................................................................................. 9
Scanning Services: RESPMOD vs. REQMOD ........................................................................................... 9
Communication Between the ProxySG and Content Analysis Appliances .............................................. 9
About Malware

Malware is malicious software designed to infiltrate or damage a computer system without the owner’s informed consent. The majority of malware comes from two vectors: hidden downloads in popular and trusted websites, and malware distribution through social networking, peer-to-peer (P2P), infected websites, and web mail.

The following table lists common types of malware.

<table>
<thead>
<tr>
<th>Malware</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>Software that automatically displays advertisements on a computer</td>
</tr>
<tr>
<td>Keylogger</td>
<td>A program that secretly records a user's activity (keystrokes) to steal passwords and other sensitive data</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Software that encrypts data in an unreadable format and then demands payment in exchange for the decryption key (the ransom)</td>
</tr>
<tr>
<td>Rogue security software</td>
<td>Software that pretends to be an antivirus program to remove malware infections, but actually, it is the malware. Oftentimes, it will turn off the real antivirus software.</td>
</tr>
<tr>
<td>Spyware</td>
<td>Computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user’s interaction with the computer, without the user's consent</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>Software that appears to perform a desirable function but in fact performs undisclosed malicious functions. A computer worm or virus may be a Trojan horse.</td>
</tr>
<tr>
<td>Worm</td>
<td>A self-replicating computer program that uses a network to send copies of itself to other nodes, without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms destroy data and files on the computer.</td>
</tr>
<tr>
<td>Virus</td>
<td>Software that attaches itself to an existing program and can copy itself and infect a computer without a user’s permission or knowledge</td>
</tr>
</tbody>
</table>

The Symantec Threat Protection Solution

A new breed of hackers – including cybercriminals, nation states, hacktivists, and insiders – are perpetrating increasingly sophisticated, targeted, and effective exploits on enterprises. This shift in the threat landscape requires a security platform that combines prevention with more effective attack detection, preparedness, and response. Symantec offers a three-prong security solution in which the appliances have been designed, tested, and manufactured for compatibility:

- **ProxySG appliance** with its extensive web content controls, compares files against the Symantec WebFilter and Global Intelligence Network (GIN) databases. If the domain hosting the file has been categorized as a malware source, the file download is denied and the user is notified. If the domain is not recognized, the file is sent to Content Analysis for inspection.
Benefits of Using Symantec's Integrated Solution

- **Content Analysis** (CA) appliances offer advanced malware detection at the gateway. CA uses multiple in-house and third-party detection modules to provide a layered defense-in-depth strategy protecting against targeted/unknown attacks, viruses, worms, trojans, and spyware.

- **Malware Analysis** (MA) sandboxing appliance provides both emulated and full virtual environments in which samples are detonated. By observing what happens after the detonation, MA is able to detect malicious behaviors that static methods alone cannot identify.

**Supported Anti-Malware Engines**

Symantec Content Analysis provides the option to use one or two anti-malware engines from the following anti-malware industry leaders:

- Symantec
- Kaspersky
- Sophos
- McAfee

Tests show that adding a second anti-malware engine results in a ~12% increase in malware capture. The most complete coverage can be achieved with two engines on the perimeter and an engine from a third vendor on endpoint devices.

**Scanning Services: RESPMOD vs. REQMOD**

Content Analysis can scan content with two types of services: response modification and request modification.

Most web malware deployments involve the use of a response modification (RESPMOD) service. A response modification service analyzes inbound client requests. That is, the response that is fetched from the origin content server is scanned for malicious content before it is delivered to the user who requested the content. If the content is verified as clean (and also allowable by corporate policy), the client receives the web objects (that comprise web pages). If malware scanning detects malicious content, the response is quarantined, the objects are not cached, the event is logged, and the client receives a message indicating that a virus was found.

A request modification (REQMOD) service is typically used to scan outbound web requests or web mail attachments before users post them to file servers such as Gmail and Outlook servers. A request modification service mainly prevents data leak in an enterprise.

**Communication Between the ProxySG and Content Analysis Appliances**

Symantec’s Content Analysis and Blue Coat ProxySG appliances communicate using Internet Content Adaptation Protocol (ICAP). ICAP is an open standard protocol that allows content engines to send HTTP-based content to an
ICAP server for performing value-added services such as virus scanning.

The ProxySG is the ICAP client, and Content Analysis is the ICAP server. The ProxySG forwards web content that needs to be scanned to Content Analysis. Content Analysis filters and adapts the content and returns it to the ProxySG. The scanned content is then served to the user who requested the content and is cached on the ProxySG.

Once an object is cached, it is not scanned again until either the object contents change or the AV database changes. The AV database is a pattern file that allows antivirus software to identify viruses. Whenever the database changes, Content Analysis needs to rescan any requested objects that are in the cache, because the new database might contain updates on emerging malware threats.

For a non-cacheable object, Content Analysis scans the object and creates a secure hash of the file’s contents. Content Analysis compares the file’s hash against a database that is constructed as a result of scanning objects. The object will not be scanned again unless either its hash changes (indicating the content has changed) or the AV database changes.

For frequently accessed web content, this integrated solution eliminates network threats and reduces bandwidth usage and latency by serving objects from the cache.
Deployment

This chapter illustrates several deployment topologies for incorporating one or more ProxySG and Content Analysis appliances in your network.

**Note:** The ProxySG can be deployed in explicit or transparent mode. In explicit mode, each client web browser is explicitly configured to use the ProxySG as a proxy server. In transparent mode, the client web browser does not know the traffic is being processed by a machine other than the origin content server. Transparent proxy requires that you use a bridge, a Layer-4 switch, or Web Cache Communication Protocol (WCCP) to redirect traffic to the ProxySG.

Also included in this section are high-level guidelines and workflows for physically installing the appliances into your network.
Symantec Content Analysis 2.4

Deployment Guidelines

When planning the installation of your Symantec appliances, consider the following deployment guidelines:

- Symantec recommends that all ProxySG appliances reside on the same subnet as Content Analysis, even in cases where multiple ProxySG appliances are load balanced with multiple Content Analysis appliances. Although you can put the Content Analysis appliance in California and the ProxySG in New York, performance will suffer. For optimal performance, the ProxySG and Content Analysis appliances must be physically and logically close to each other; Symantec recommends that Content Analysis be on the next-hop VLAN.

- Before installing Content Analysis, install the ProxySG in your network, and verify that it is intercepting traffic.

- Content Analysis must have access to the Internet for system and pattern file updates.

- Malware Analysis must have at least one sandbox or Windows sandbox environment configured before Content Analysis can use it to analyze data.

One ProxySG to One Content Analysis Appliance

This basic deployment has one ProxySG appliance, one Content Analysis appliance, and a Malware Analysis appliance. It is suitable for a small enterprise or network segment.

This deployment is the easiest to configure and is the least expensive to deploy because it does not require redundant appliances to be purchased. However, due to its lack of redundancy, this deployment has the following limitations:
- No web malware scanning if the Content Analysis appliance goes down. Depending on the policy you implement on the ProxySG, when the Content Analysis appliance fails, users either receive unscanned content or see exception pages noting that the content cannot be delivered.

- No load balancing for ICAP scanning if the Content Analysis appliance gets overwhelmed with ICAP requests.

- No failover if the ProxySG goes down.

**Virtual appliance deployment:**

![Diagram of virtual appliance deployment]

**Redundant Appliance Topologies**

Larger enterprises may require redundancy in the network: multiple ProxySG and/or multiple Content Analysis appliances. Redundant appliances address the limitations of the single-CAS/single-ProxySG deployment. The ProxySG can load balance web scanning between multiple Content Analysis appliances or designate a sequence of Content Analysis appliances as failover devices should the primary Content Analysis go offline. Similarly, secondary ProxySG appliances can be configured as failover devices should the primary ProxySG go down or can provide further proxy support in the network.

The options for redundant topologies are:

- Multiple Content Analysis appliances with a single ProxySG. This is the most common type of redundant topology in a Symantec integrated deployment. For configuration details, see "Load Balance Multiple Content Analysis Appliances" on page 90 and "Configure Content Analysis Failover" on page 95.

- Multiple ProxySG appliances to one Content Analysis

- Multiple ProxySG appliances to multiple Content Analysis appliances
Diagrams for Redundant Topologies

The ProxySG and Content Analysis appliances are available in different capacities. Symantec provides sizing information to assist you with determining the correct combination of appliances to deploy.

The following images represent the redundant topology options listed above.

One ProxySG to multiple Content Analysis appliances
Enterprises that need ProxySG failover, without redundant Content Analysis appliances, might use the following type of topology.

Multiple ProxySG appliances to one Content Analysis
Symantec Content Analysis 2.4

Enterprises with hundreds to thousands of users require the processing power of multiple ProxySG and Content Analysis devices, which work together to provide efficient scanning power plus failover capability.

Multiple ProxySG appliances to multiple Content Analysis appliances

For information on configuring failover on the ProxySG, refer to the SGOS Administration Guide (Configuring Failover).
Deployment Workflow

This chapter describes the high-level steps to install and perform basic configuration on the ProxySG, Content Analysis, and Malware Analysis appliances. Before you proceed with installing Content Analysis, install the ProxySG in the network, and verify that it is functioning as a secure web gateway. For detailed information, refer to the Quick Start Guide for your hardware platform.

Configure and Install the ProxySG Appliance ................................................................. 17
Configure and Install the Content Analysis Appliance ......................................................... 19
Install and Configure the Malware Analysis Appliance ......................................................... 20

Configure and Install the ProxySG Appliance

The following procedure provides high-level steps for performing the initial configuration and physical installation of the ProxySG appliance.

Note: If deploying a virtual appliance, refer to the Secure Web Gateway Virtual Appliance Initial Configuration Guide.

1. Rack-mount the ProxySG and connect the appliance to the network. Refer to the ProxySG Quick Start Guide for specific steps.

2. With a serial console connection, run the initial setup wizard, and configure the ProxySG with basic network settings.

3. License the appliance:
   a. Open a web browser and navigate to: https://services.bluecoat.com/eservice_enu/licensing/register.cgi
   b. Enter your MySymantec credentials.
   c. Follow the onscreen instructions to register your appliance and download a license.

4. Log in to the ProxySG Management Console.
   a. Open a supported web browser. (Note: Google Chrome is not supported.)
   b. Enter the IP address you assigned to the ProxySG followed by port number 8082. For example: https://192.0.2.2:8082

5. Verify a successful configuration.
Symantec Content Analysis 2.4

a. In the Management Console, select **Statistics > Summary > Efficiency**. Verify that each configured interface is up.

b. Click the **Device** tab. Verify connectivity to the DNS server and other external devices.

c. Make sure the ProxySG health status is green (OK).

The following example intercepts explicit HTTP traffic on port 8080 and creates a rule to allow this traffic.

6. Set the Explicit HTTP service to intercept.

   a. Select **Configuration > Services > Proxy Services**.

   b. Open the Standard service group, and locate the Explicit HTTP service.

   c. Select the **All -> Explicit:8080** port, and choose **Intercept**.

   d. Click **Apply**.

7. Open the Visual Policy Manager.

   a. Select **Configuration > Policy > Visual Policy Manager**.

   b. Click **Launch**.

8. Add a rule in the web access layer to allow traffic received on the Explicit HTTP service port (8080).

   a. Select **Policy > Add Web Access Layer**.

   b. Right-click the Source field and select **Set > New > Proxy IP Address/Port**.

   c. In the **Port** field, enter **8080** and click **OK**.
9. Install the policy.
   a. Click Install Policy.
   b. Click OK.
   c. Close the VPM window.

10. Verify that the ProxySG is seeing network traffic.
    a. Make sure there are clients running traffic. (The browser must be explicitly or transparently redirected to the ProxySG appliance.)
    b. Select Statistics > Sessions > Active Sessions.
    c. Click Show. The Proxied Sessions table should list the active sessions of current traffic.

11. If necessary, upgrade to SGOS 6.5 or later. This Integration Guide assumes the ProxySG is running SGOS 6.5 or later.
    a. Select Maintenance > Upgrade.
    b. For details, refer to the SGOS Administration Guide (Maintaining the ProxySG).

Configure and Install the Content Analysis Appliance

The following procedure provides high-level steps for performing the initial configuration and physical installation of the Content Analysis appliance.

**Note:** If deploying a virtual appliance, refer to the Content Analysis Virtual Appliance Installation Guide on the Symantec Product Documentation page.

1. Rack-mount the Content Analysis appliance and connect it to the ProxySG and the network. Refer to the Content Analysis Quick Start Guide for specific steps.
2. With a serial console connection, run the initial setup wizard, and configure Content Analysis with basic
Symantec Content Analysis 2.4

network settings.

3. Log in to the Content Analysis browser interface and download the license.
   a. Open a web browser.
   b. Enter the IP address you assigned to Content Analysis followed by port number 8082. For example: https://192.100.4.4:8082
   c. Click Download License from Blue Coat. The appliance automatically downloads and installs the license.

4. Activate and view services (Antivirus, File Reputation, Sandboxing, Predictive Analysis) you have purchased.
   a. Go to the Network Protection Licensing Portal at https://services.bluecoat.com/eservice_enu/licensing/register.cgi to associate the activation code provided in your e-fulfillment letter with your appliance serial number. If you fail to do this, subscription elements of your license will not be available.
   b. Go to System > Licensing. The License information page displays. Each licensable service shows the following details:
      Status: The availability of a service component and the expiration date
      Active: The activation status of the component
   c. Select a service component check box to activate it.
   d. Click Save Changes.

Install and Configure the Malware Analysis Appliance

When Content Analysis detects a suspicious file that’s not on the whitelist and doesn’t match any known malware signatures, the appliance can forward the file to an external sandbox, such as SymantecMalware Analysis, for further analysis. The sandbox provides a virtualized or emulated Windows environment where files can be safely tested for malware.

The following procedure provides high-level steps for performing the initial configuration and physical installation of the Malware Analysis appliance.

1. Rack mount the Malware Analysis appliance and connect it to the network. Refer to the Malware Analysis Quick Start Guide for specific steps.

2. Configure the Malware Analysis appliance with basic network settings. With a serial console connection, run the initial setup wizard. Refer to the Malware Analysis Quick Start Guide for specific steps.
3. Log in to the Malware Analysis web interface.
   
a. Open a web browser.

   b. Enter the IP address you assigned to the appliance (or the one that was assigned through DHCP). For example: https://192.0.2.3

   c. Accept the self-signed certificate when prompted by your web browser.

   d. Input the default admin web interface username and password: admin | admin

   e. Click **Login**

4. Follow the prompts to install the Windows license(s) and complete the installation.

5. Upload the .NDF license file to activate the appliance. The .NDF license file is attached to the entitlement email that you should have received.

6. Verify a successful configuration.

7. Activate all reputation services (Web and File) and make sure WebPulse is enabled.

8. Create or modify profiles as needed to replicate production environments or to test the behavior of malware across different configurations. Refer to the *Symantec Malware Analysis Administration Guide* for details.

9. Configure default task settings.
Configure Symantec Appliances to Communicate

After Symantec appliances are deployed, you can configure them to communicate with one another. On the ProxySG appliance, you must create an ICAP service that identifies the Content Analysis appliance and then add a rule to your policy that defines this service for ICAP response; alternatively, you can enable malware scanning on the ProxySG appliance which performs both tasks for you. To configure communication between Content Analysis and Malware Analysis appliances, you identify the MA appliance to be used for sandboxing.

Enable Secure ICAP Connections .......................................................... 23
Configure ICAP Policy on a ProxySG Appliance ....................................... 29
  Automatically Configure an ICAP Service on the ProxySG ..................... 30
  Manually Configure an ICAP Service on the ProxySG .......................... 36
Configure ICAP Policy ........................................................................ 39
Configure Scanning Exemption Policies ............................................... 42
Test the Threat Protection Policy ...................................................... 46
Configure Malware Analysis ............................................................... 48
Enable Secure ICAP Connections

Secure ICAP configuration is available in Settings > ICAP.

Content Analysis receives data from the ProxySG appliance through an Internet Content Adaptation Protocol (ICAP) connection. This occurs on port 1344, which is the typical TCP port for plain ICAP communication. For heightened security, you can enable a secure connection between Content Analysis and the ProxySG appliance.

**Caution:** Secure ICAP introduces a significant performance penalty. When security is of concern, an alternative is to deploy the Content Analysis and ProxySG appliances on a segmented network, to which no outside access is permitted. Only when properly segmented does Symantec recommend enabling plain text ICAP connections.

Configure Content Analysis to receive secure ICAP connections

1. Log in to Content Analysis.
2. Select Settings > ICAP.
3. Secure the connection.
a. Select secure.

Note: Secure ICAP has a significant impact to performance.

b. The default secure Port is 11344. You can change the port, but be advised that this change must occur on both ends of the transaction: Content Analysis and the ProxySG secure ICAP service.

c. (Optional) Select plain to allow non-secure services (such as HTTP and FTP) to be scanned using the plain ICAP connection. (Secure services, such as HTTPS, will be scanned using the secure ICAP connection.)

d. Check your preferred TLS/SSL versions to support for the secure connection. Symantec recommends avoiding TLS 1.0 and below.
e. (optional) Click **Cipher Selection** to set your preferred security ciphers for your secure ICAP connection. The **Cipher Selection** window opens.

![Cipher Selection Table]

f. The available ciphers are listed under **Cipher**. **Strength** denotes the cryptographic strength of each cipher. Put a check in the box to the left of your preferred ciphers.

**Note:** For optimal security, Symantec recommends that only high strength ciphers be used.

g. Use the up and down arrows under **Priority** to change the list order. When negotiating a secure connection, Content Analysis will prefer the enabled ciphers at the top of the list first. As cipher negotiation takes place, if the topmost ciphers are not supported by the client, (the ProxySG appliance, in most cases) it will use the next available cipher in the list until a match is made.

h. Scroll to the bottom of the list and click **Save**.

i. Click **Save Changes**.

4. Generate a self-signed certificate.
   If your organization has a Certification Authority, you can generate and sign a Certificate Authority-signed certificate for Content Analysis, and install it on the appliance. See step 5 below.
Symantec Content Analysis 2.4


b. The Current Information tab displays what is currently in the appliance certificate. If any information is incorrect, click Create Certificate.

c. Enter the certificate identity information.

d. Enter a recipient Email address. This should be the administrator who gets notified if there are problems with the certificate.

e. Select a Date valid value. This is the expiry date for the certificate.

f. Set the Size value, which is the key length used to encrypt the certificate. Available key lengths are 2048 and 4096.

g. Click Save Changes to generate the certificate. The appliance resets the ICAP service to support the new certificate. A dialog displays a countdown timer for 30 seconds while the service restarts.

h. Click Current Information and Download Public Key to save the certificate file to your local system.

5. (Optional/Recommended) Install a Certificate Authority-signed certificate.

a. Create a CSR with your organization’s certificate information, and have it signed as a server certificate by a Certificate Authority.

b. Click Certificate Management > Import Certificate and click Browse.
Configure Symantec Appliances to Communicate

Install the certificate on the ProxySG appliance and enable a secure ICAP configuration.

1. Log in to the ProxySG Management Console.

2. Select Configuration > SSL > CA Certificates > CA Certificates.

3. Import the certificate you created in steps 3 or 4 in "Configure Content Analysis to receive secure ICAP connections" on page 23.
   a. Click Import. The Management Console displays the Import External Certificate dialog.
   b. Name the certificate.
   c. Open the Content Analysis appliance certificate in a text editor on your system and copy all text including: -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----.
Symantec Content Analysis 2.4

d. Click **Paste From Clipboard** to add the certificate to the **CA Certificate PEM** field.

e. Click **OK** to close the dialog; click **Apply**.

4. Add the certificate to the approval list.

   a. Select **Configuration > SSL > CA Certificates > CA Certificate Lists**.

   b. Click **New** and enter **AV_Approval CA**.

   c. Select your new certificate from the list on the left and click **Add>>** to add the certificate to this CA certificate list.

   d. Click **OK**; click **Apply**.

5. Create a device profile to use the certificate and CA Certificate List (CCL).

   a. Select **Configuration > SSL > Device Profiles**.

   b. Click **New** and name the new profile **AV_SSL**.

   c. Select **default** as the **Keyring**.

   d. Select the **CCL** you created in step 4, **AV_Approval CA**.

   e. Select the same TLS settings as you did for secure connections on the Content Analysis appliance.

   f. Click **OK**, then **Apply**.

   **Note**: If SSL connections fail in initial testing, remove the **Verify peer** check mark (enabled by default).

6. **SGOS 6.5**: Select **Configuration > External Services > ICAP**.

   **SGOS 6.6** and higher: Select **Configuration > Content Analysis > ICAP**.

7. Select your ICAP service object in the list and click **Edit**.

8. Add a check next to **This service supports secure ICAP connections**.

9. Select **AV_SSL** from the **SSL Device Profile** drop-down menu. Click **OK**, then **Apply**.
Configure ICAP Policy on a ProxySG Appliance

Traffic is sent from the ProxySG to Content Analysis using the Internet Content Adaptation Protocol (ICAP).

![Diagram showing traffic flow from ProxySG to Content Analysis]

**Note:** A ProxySG appliance that communicates with Content Analysis should be running SGOS 6.5.2.x or higher.

To have Content Analysis scan the traffic your users request, configure the ProxySG to identify the types of data it will scan. You can either use **manual** or **automatic** configuration. The manual configuration requires that you create policy to trigger the ICAP connection for destination URLs, categories, and file types. The configuration relies on the **Malware Scanning** configuration on the ProxySG appliance to provide a threshold configuration to determine how strict content scanning will be.
Symantec Content Analysis 2.4

Tip: Symantec provides customizable policy templates to help you configure CPL policy that bypasses content scanning for low-risk/high-volume content. These best practices provide a more secure policy model for bypassing content scanning; the policy lowers risk, improves user experience, and conserves scanning resources. The policy model contains three predefined security levels that you can choose from: Basic, Medium, and High. The policy takes advantage of various detection mechanisms such as URL Threat Risk Levels, URL Category, URL, Web Application, Application Group, and streaming detection and file types. For instructions on implementing this policy, see Secure Web Gateway - Content Analysis Policy Best Practice. Note that this policy requires that you use manual ICAP configuration on the ProxySG appliance; automatic configuration creates policy that conflicts with the best practice policy.

Automatically Configure an ICAP Service on the ProxySG

The ProxySG malware scanning solution uses a set of predefined ICAP scanning and threat detection policies to protect your network and users from malicious content. Once malware scanning is enabled, your appliance will send traffic to your ICAP device (either ProxyAV or Content Analysis) to be scanned for malware and threats.

Configure Malware Scanning in SGOS 6.5

1. Log in to the ProxySG Management Console.
2. Select Configuration > Threat Protection > Malware Scanning.
3. Add the Content Analysis appliance.
a. Click **New**. The management console displays the Add ProxyAV ICAP Server dialog.

b. Enter the **IP address** or host name for Content Analysis.

c. Select the **ProxyAV Ports** per your deployment (applies to Content Analysis appliances).
   - The default is **Plain ICAP connections**.
   - If you enabled (or plan to enable) a **Secure ICAP connections** between the ProxySG appliance and Content Analysis, select that option.
   - (Optional) If you enable secure connections, you can select the plain ICAP connections option as well. When you do so, non-secure services, such as HTTP and FTP, are scanned using the plain ICAP connection and secure services, such as HTTPS, are scanned using the secure ICAP connection.

d. Click **OK**.

4. The Malware options on the bottom of the page are now selectable.
a. (Optional) Change the protection level from the default of **High performance** to **Maximum protection**, if you want to scan all files, rather than those that are typically vectors for viral attacks. This can unnecessarily cause Content Analysis to use more resources than necessary as it has to scan all data users request from the Internet. If your organization does not have a policy that requires all data to be scanned, use the **High performance** protection level setting.

b. The **Connection Security** options apply if you have enabled secure ICAP. You can instruct the ProxySG appliance when to use secure connections.

c. For the best security, Symantec recommends leaving the default **Actions on Unsuccessful Scan** option to **Deny the client request**.

5. Select the **Enable Malware Scanning** box.

6. Click **Apply**.

**Configure Malware Scanning in SGOS 6.6 and 6.7**

1. Log in to the ProxySG Management Console.

2. Select **Configuration > Threat Protection > Malware Scanning**.

3. Add the Content Analysis appliance.
a. Click **New**. The Add CAS/ProxyAV ICAP Server dialog opens.

b. Enter the **IP address** or hostname for Content Analysis.

c. Select the **CAS/ProxyAV Ports** per your deployment (applies to Content Analysis appliances).

- The default is **plain ICAP connections**.
- If you enabled (or plan to enable) **secure ICAP connections** between the ProxySG appliance and Content Analysis, select that option.
- If you enable secure connections, you can select both options so that in the event there is a certificate mismatch or other error, the AV scan occurs over the plain connection. If you select only Secure, the ProxySG appliance does not forward the scan request in the event of a secure connection error.

d. Click **OK**.

4. To enable Malware Scanning, select **Use external content analysis services**.

5. The options on the bottom of the page are now selectable.
a. (Optional) Change the protection level from the default of High performance to Maximum protection, to scan all files, rather than those that are typically vectors for viral attacks. This can unnecessarily cause Content Analysis to use more resources than necessary as it has to scan all data users request from the Internet. If your organization does not have a policy that requires all data to be scanned, use the High performance protection level setting.

b. For the highest security, Symantec recommends leaving the default Actions on unsuccessful scan option to Deny the client request.

6. Click Apply.

Modify the ICAP Configuration

With Malware Scanning enabled, the next step is to check the settings on the ICAP service object, and modify as necessary.

1. In the ProxySG management console:

   SGOS 6.5: Select Configuration > External Services > ICAP.

   SGOS 6.6: Select Configuration > Content Analysis > ICAP.

2. Here, you'll notice that there is a service called proxyav1. This service was created when you added a new ICAP server. Select proxyav1 and click Edit. The Edit ICAP Service proxyav1 dialog opens.
3. When integrating Content Analysis with Symantec Endpoint Protection Manager (SEPM), you must tell the ProxySG appliance to send the client address so that SEPM can identify whether the IP address is a managed endpoint.

Enable the **Client address** check box in the *ICAP v1.0 Options* section.

4. Adjust other settings, as required. For example, you may want to change the **Maximum number of connections**.
5. Click OK and Apply to save the ICAP service settings.

View Malware Scanning Policy

To verify that the Malware Scanning policy has been applied to your configuration, view the policy:

1. In the ProxySG Management Console, select Configuration > Policy > Policy Files.
2. Next to Current Policy, click View. The policy is displayed in a new window.
3. Search for malware_scanning. You should find CPL code similar to the following:

   `<Cache BC_malware_scanning_solution>
   policy.BC_malware_scanning_solution
   <Proxy BC_malware_scanning_solution_proxy>
   policy.BC_malware_scanning_solution_proxy`

**Note:** The definitions for the malware scanning policy appear further down in the CPL.

For information on defining policy to exempt specific URLs, categories, or file types from being ICAP scanned, see "Configure Scanning Exemption Policies " on page 42.

Manually Configure an ICAP Service on the ProxySG

The ProxySG appliance requires an ICAP service object to communicate with Content Analysis.
Configure Symantec Appliances to Communicate

**Note:** If you plan to enable secure ICAP, this topic assumes that you have completed the steps in "Enable Secure ICAP Connections" on page 23.

1. Log in to the ProxySG Management Console.

2. Add a new ICAP service.
   a. SGOS 6.5: Select **Configuration > External Services > ICAP**.
      SGOS 6.6 or higher: Select **Configuration > Content Analysis > ICAP**.
   b. Click **New**. The Add list Item dialog opens.
   c. Enter a name for the Content Analysis service and click **OK**.
   d. Click **Apply**.

3. Select the new entry in the list and click **Edit**. The **Edit ICAP Service** dialog opens.

![Edit ICAP Service dialog](image-url)
a. Enter the **Service URL**, which is the Content Analysis ICAP address. The format is as follows: `icap://<IP_address>/<ICAP_service>`, where `IP_address` is the Content Analysis IP address or hostname and `ICAP_service` is the name of the CAS appliance (CAS by default).

   **Note:** Starting in SGOS 6.6, the Service URL does not require the `ICAP_service` when the ICAP server is Content Analysis or ProxyAV. You can simply enter `icap://<IP_address>/`.

b. Set the maximum number of ICAP connections to establish with Content Analysis. Refer to the table below to determine the best value for this field. The table lists recommended and maximum supported ICAP connections each model of Content Analysis appliance can support at one time. If more than one ProxySG appliance communicates with your Content Analysis appliance, divide the maximum number of connections among them.

<table>
<thead>
<tr>
<th>Model</th>
<th>Recommended ICAP Connections</th>
<th>Maximum ICAP Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS-S200-A1</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CAS-S400-A1</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CAS-S400-A2</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>CAS-S400-A3</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>CAS-S400-A4</td>
<td>300</td>
<td>400</td>
</tr>
<tr>
<td>CAS-S500-A1</td>
<td>400</td>
<td>500</td>
</tr>
<tr>
<td>CAS-V100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>(CAS-VA)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   **Caution:** *Sense settings* can also be used to define the maximum number of ICAP connections, however it will always return a value of 100 (in SGOS 6.6 or higher) or 250 (in SGOS 6.5) connections. This value may be too high for some models of Content Analysis, and can result in queued connections and potential instability.

c. In the **Connection timeout** field, enter the number of seconds the ProxySG waits for replies from Content Analysis. The default timeout is 70 seconds, but you will likely want to set a higher value because large (several hundred MB) archives can easily take more than 70 seconds. If Content Analysis gets a large file that takes more than the configured timeout to scan, the ProxySG will close the...
Configure Symantec Appliances to Communicate

connection, and the user will not get the file. The value you enter for the timeout is related to the maximum file size configured on Content Analysis; larger file sizes require longer to scan so the connection timeout should be higher. If you allow only 100 MB file sizes, 70 seconds would be a sufficient timeout value. But if you allow 2 GB files, a timeout value of 70 would be too low. The range is 1 to 65535.

d. Select Defer scanning at threshold to set the threshold at which the ProxySG defers the oldest ICAP connection that has not yet received a full object. When enabled, the defer threshold scanning defaults to 80 percent. For more information about scanning deferral, see “Deferred Scanning” on page 72.

e. Select the ICAP Service Ports per your deployment.

- The default service is a plain ICAP connection.

- If you enabled (or plan to enable) a secure ICAP connection between the ProxySG appliance and Content Analysis, select that option and from the SSL Device Profile drop-down list, select the profile you created.

- (Optional) If you enable secure connections, you can select the plain ICAP connections option as well. When you do so, non-secure services, such as HTTP and FTP, are scanned using the plain ICAP connection and secure services, such as HTTPS, are scanned using the secure ICAP connection.

f. Set the ICAP method to be used. To scan traffic as users receive it from the Internet, select response modification. To scan traffic as users send it to the Internet, select request modification.

g. Select Send options—Client address, Server address, Authenticated user, and Authenticated groups—to forward this information with each file sent to Content Analysis. This ensures that all threat reporting bears the appropriate information.

| Note: When integrating Content Analysis with Symantec Endpoint Protection Manager (SEPM), you must tell the ProxySG appliance to send the client address so that SEPM can identify whether the IP address is a managed endpoint. |

h. Click OK to close the dialog.

4. Click Apply.

Configure ICAP Policy

Once you have defined an ICAP response service, you can use policy on the ProxySG appliance to send traffic to Content Analysis.
Create a default rule to send traffic to the Content Analysis with ICAP

1. Open the ProxySG Visual Policy Manager.
   a. Log in to the ProxySG Management Console.
   b. Select Configuration > Policy > Visual Policy Manager.
   c. Click Launch. The Visual Policy Manager opens in a new window.

2. Select Policy > Add Web Content layer.

3. Name the new layer ICAP Scan.

4. Right-click the Action field in the rule.
   - SGOS 6.5: Select Set > New > Set ICAP Response Service.
   - SGOS 6.6 or higher: Select Set > New > Perform Response Analysis.
5. Select the ICAP service you created in the Management Console and click Add to move it to the box on the right.

6. Choose a failure method:

   Deny the client request (fail closed)

   SGOS 6.5: Continue without further ICAP processing (fail open)

   SGOS 6.6 or higher: Continue without further response processing (fail open)

7. Click OK, OK.
8. Install the policy.
   a. Click Install Policy.
   b. Click OK.
   c. Close the VPM window.

Configure Scanning Exemption Policies

Whether you've used an automatic ICAP configuration with the Malware Scanning option in SGOS 6.x, or manually configured an ICAP response modification rule in the VPM, you may find that your organization needs to exempt specific destinations from ICAP scanning. If a destination URL, category, or file type is trusted, you can configure policy to negate it from being scanned. The examples provided in this topic detail the steps to configure the most common types of ICAP exemptions.

Exempt a Domain from Scanning

1. Open the ProxySG Visual Policy Manager.
   a. Log in to the ProxySG Management Console.
   b. Select Configuration > Policy > Visual Policy Manager.
   c. Click Launch. The Visual Policy Manager opens in a new window.

2. If you used the automatic method of enabling Malware Scanning, you will need to add a new web content layer.
   b. Name the layer ICAP Scan.

3. Or, if you manually configured Content Analysis scanning and policy, add a new rule to your ICAP Scan policy layer.
   a. Click Add rule.
   b. Click Move up to position the new rule above the ICAP scan rule.

4. Right-click the Action field in the new rule, and choose one of the following:
- SGOS 6.5: Select **Set > New > Set ICAP Response Service**.
- SGOS 6.6 or higher: Select **Set > New > Perform Response Analysis**.

5. Name the new object **DoNotScan** and choose one of the following:
   - SGOS 6.5: Select **Do not Use any ICAP response service**.
   - SGOS 6.6 and later: Select **Do not perform response analysis**.

### SGOS 6.6 Screen

6. Click **OK**, and **OK**.

7. Right-click the **Destination** field in this new rule. Select **Set > New > Request URL**.
8. Enter www.symantec.com (replace with a domain you would like to exempt from ICAP scanning). Click Add, Close, and OK.

9. Repeat for other URLs.

10. Install the policy.

Tip: The web content layer only allows exemptions based on destinations. To make an exemption based on source, use a web access layer instead of a web content layer.

Exempt a Category from Scanning

Because some media streams come without end, sending those streams to an ICAP appliance for scanning can lead to delays in processing other traffic. As a best practice measure, follow these steps to defer the streaming media category from being ICAP scanned.

1. In your ICAP Scan layer, add a new rule and position it above the scanning rule.

2. Right-click the Destination field in this new rule, and click Set > New > Request URL Category.

   Extend the Blue Coat categories list, select TV/Video Streams. Name the object TV/Video Stream Category.

3. Click OK, OK.

4. Right-click the Action field, and select Set. Choose DoNotScan from the list of existing objects.

5. Install the policy.

Use Policy to React to Specific ICAP Scan Results

SGOS 6.5.2.1 introduced the option to define policy to take action based on the results of ICAP scanning. This
example policy allows users to download archive files such as ZIP, RAR, or GZ, if they are password protected and from a trusted domain.

**Note:** To take action on ICAP scan results, your ICAP request modification rule (or Malware Scanning configuration) must have the **Continue without ICAP/Malware Scanning** option enabled.

1. Add a new **Web Access Layer** and name it **ICAP Error Actions**.
2. Select **Edit > Reorder Layers**. Position the ICAP Error Actions layer below your ICAP Scan layer.
3. Right-click the **Destination** field, and select **Set > New > Request URL**.
4. Enter the domain name of the URL in question. In this case, we’ll use **www.example.com**. Click **Add**, **Close**, and **OK**.
5. Right-click the **Service** field in the new rule, and select **Set > New > ICAP Error Code**.
6. Select **Selected errors**, choose **Password Protected Archive**, click **Add**, **OK**, and **OK**.

7. Right-click the **Action** field and select **Allow**.
8. Install the policy.

Test the Threat Protection Policy

Before proceeding with further configuration, test the basic deployment to verify Content Analysis is scanning content and detecting malware based on your selections in configuration.

1. Log in to Content Analysis.

2. Confirm that Content Analysis is scanning files. Select **Statistics > Objects**: the Total Scanned value should increment as clients make web requests. (The browser must be explicitly or transparently redirected to the ProxySG appliance.)

3. Log in to the ProxySG Management Console.

4. Prepare the ProxySG for test validation by enabling access logging.
   a. Select **Configuration > Access Logging > General > Default Logging**.
   b. Enable the **Enable Access Logging** check box.
   c. Click **Apply**.

5. Display the log, so that log entries can be viewed during testing.
   a. Select **Statistics > Access Logging > Log Tail**.
   b. Select the appropriate HTTP access log (*main* is the default log).
   c. Click **Start Tail**.

6. Request an “infected” test file.

**Note:** The file is not actually infected but has a virus signature that identifies it as infected for testing purposes.
a. Open a browser that is either explicitly or transparently redirected to the ProxySG.


c. Click the **Download Anti-Malware Testfile** link.

d. Read the information about the test files, and select one of the files to download (such as eicar.com).

7. Confirm that you were not provided with the “infected” file.

A page should display indicating that Content Analysis has detected a virus in the file, and that the file has been dropped.

8. Check the ProxySG access log.

   a. Go to the ProxySG's Access Log Tail window.

   b. Verify that the access log entry for the eicar file contains an entry for virus detection.

```
2019-03-12 17:39:51 382 10.9.16.75 - - virus_detected PROXIED "none"
http://www.eicar.org/anti_virus_test_file.htm 200 TCP_DENIED GET
  text/html;%20charset=%220%22 http www.eicar.org 80 /download/eicar.com.txt - txt
  "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)"
203.0.113.76 1000 383 "EICAR test file"
```

9. Check the Content Analysis ICAP request history.

   a. Go to the Content Analysis browser window.

   b. Select **Statistics > Historical Connections**.

   c. Click **Refresh**.

   d. Locate the request for the eicar file.

   e. Verify that the Result field contains VIRUS.

10. Request the same “infected” test file and verify that ProxySG does not send a previously-scanned object to Content Analysis since the response for the object is now in the ProxySG’s cache.

    a. Request the same “infected” test file.

    b. Go to the Content Analysis Historical Connections window.

    c. Click **Refresh** and verify that there is NOT a second request for the eicar file. (Since the response for the object was served from the ProxySG cache, it should not have been sent to Content Analysis for scanning.)
Configure Malware Analysis

To configure Content Analysis to send unknown suspicious files to one or more standalone Symantec Malware Analysis appliances for further analysis, you specify the IP address of the appliance and enable the profiles and tasks you want to test with. The Symantec Malware Analysis server can either be a standalone Malware Analysis appliance or a Content Analysis appliance that is dedicated to sandboxing.

Content Analysis uses HTTPS to communicate with a Symantec Malware Analysis sandbox. The standalone Malware Analysis appliance uses TCP port 443, whereas a Content Analysis appliance dedicated to sandboxing will use TCP port 8082 by default.

Prior to adding a Malware Analysis appliance or a dedicated Content Analysis appliance you must create an administrator-level API key on the target appliance that is associated with the admin account.

Generate the API Key

1. Log in to the CLI of the target appliance with administrator credentials and enter *enable* mode.
2. Run one of the following commands:
   - Content Analysis 2.2 or Malware Analysis:
     
     `ma-actions api-key create administrator`
   - Content Analysis 2.3 and later:
     
     `ma-actions api-key create user admin role administrator`
3. Copy the API key and its identifier to a separate file. You cannot recover this key after you close the CLI interface.

Add the Appliance

1. In Content Analysis, select **Services > Sandboxing > Symantec Malware Analysis.**
2. To define a server, click **Add** in the **Servers** panel. The **Add Server** dialog opens.
3. Do the following:
   - Provide the **Server** IP address or hostname.
   - For **Port** accept the default of 8082 if you are connecting to an external Content Analysis appliance that is dedicated to on-box sandboxing, or enter 443 for a standalone Malware Analysis appliance.
   - Provide the **API Key** that you generated earlier.
4. (optional) Click **Test** to validate the configuration. Close the validation window
5. Click **Add**. The Malware Analysis server is listed in the **Servers** panel.
Configure Symantec Appliances to Communicate

Tip: Click the Malware Analysis IP address to log in to its Management Console.

6. (optional) repeat steps 2-5 to add additional Malware Analysis appliances to your sandbox configuration.

7. Check Use proxy settings if your MA server is on the Internet, and if your network requires Internet-bound requests to pass through a proxy. This relies on the Content Analysis proxy configuration in Settings > Proxy. By default, data sent to an MA sandbox server is sent directly.

8. (optional) Select Submit to SandBox to enable MA’s emulation feature.

- MA offers two environment types: IntelliVM, which executes files in a full Windows XP, Windows 7, or Windows 8 Virtual Machine, and SandBox, which executes files in an emulated Windows environment. Each malware scanning environment identifies malicious URLs and activities performed when a suspicious file is executed. However, only IntelliVM profiles fully replicate a user workstation. Some malware behaves differently when executed in a SandBox environment than a Windows workstation, and that difference can result in some files not being properly identified as malware. However, with only SandBox emulation enabled, MA scanning will be faster and use fewer resources than with IntelliVM profiles.

- If you enable SandBox and IntelliVM profiles, Malware Analysis will execute suspicious files in both environments.

- For maximum protection, send suspicious files to both the MA SandBox as well as the configured IntelliVM profiles. However, keep in mind that IntelliVM profiles are very labor intensive.

9. To set the Threat Threshold, move the slider to the left or right. The default value is 7.
Files that score at or above the threshold are considered threats, while those files that score below the threshold are considered safe.

10. Enable the tasks you want to test with. A task is an execution of a sample file or URL in a defined environment (operating system profile plus testing plugin script). A plugin contains a specific set of actions or applications that are tested during sandbox evaluation. If you enable more than one task, each enabled MA will execute suspicious files in each IntelliVM profile as well as in sandbox emulation, if that option is enabled. For each additional plugin with the same profile, Content Analysis will generate an additional task per profile on Malware Analysis. Refer to your Malware Analysis documentation for details on the available plugins.

11. Verify that each Malware Analysis server is enabled; select the check box in the Enabled column if necessary.

12. Click Save Changes.

13. Click General Settings and enable Malware Analysis in the Sandbox Services panel.

14. Click Save Changes.

Caution: Make sure that the naming for each IntelliVM profile on each MA is consistent. If one MA has a Windows 8 profile with the name "Windows8", every enabled MA must have a Windows 8 IntelliVM profile with that same name. Content Analysis will report an error if an enabled profile does not exist on all enabled Malware Analysis appliances.

Tip: To confirm that Content Analysis is sending files to Malware Analysis for processing, look at the Sandboxing report on Content Analysis (Statistics > Sandboxing). You should see values other than zero in the Total Submitted bubble and on the Files submitted to sandboxing graph.
Monitor ICAP Scanning

This chapter describes different ways to monitor ICAP scanning – on the ProxySG, on Content Analysis, in Management Center, and in Reporter.

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display ICAP Graphs and Statistics on the ProxySG</td>
<td>52</td>
</tr>
<tr>
<td>Display Content Analysis ICAP Graphs on the ProxySG</td>
<td>52</td>
</tr>
<tr>
<td>Display ICAP Statistical Data</td>
<td>54</td>
</tr>
<tr>
<td>Monitor ICAP-Enabled Sessions on the ProxySG</td>
<td>55</td>
</tr>
<tr>
<td>View Statistics on the Content Analysis Appliance</td>
<td>57</td>
</tr>
<tr>
<td>View Cache Hits</td>
<td>57</td>
</tr>
<tr>
<td>View the Sandboxing Report</td>
<td>58</td>
</tr>
<tr>
<td>View the File Reputation Report</td>
<td>59</td>
</tr>
<tr>
<td>View the Predictive Analysis Report</td>
<td>60</td>
</tr>
<tr>
<td>View the Whitelist and Blacklist Reports</td>
<td>61</td>
</tr>
<tr>
<td>View Number of Bytes Scanned</td>
<td>62</td>
</tr>
<tr>
<td>View Number of Objects Scanned</td>
<td>63</td>
</tr>
<tr>
<td>View Malware Reports in Symantec Management Center and Reporter</td>
<td>65</td>
</tr>
</tbody>
</table>
Symantec Content Analysis 2.4

Display ICAP Graphs and Statistics on the ProxySG

On the ProxySG, you can display a variety of ICAP statistics in bar chart form as well as in a statistical table. The table below defines the ICAP statistics that the ProxySG tracks for each ICAP service and service group.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain Requests</td>
<td>ICAP scanning transactions that are not encrypted</td>
</tr>
<tr>
<td>Secure Requests</td>
<td>ICAP scanning transactions that are encrypted and tunneled over SSL</td>
</tr>
<tr>
<td>Deferred Requests</td>
<td>ICAP scanning transactions that have been deferred until the full object has been received</td>
</tr>
<tr>
<td>Queued Requests</td>
<td>ICAP scanning transactions that are waiting until a connection is available</td>
</tr>
<tr>
<td>Successful Requests</td>
<td>ICAP scanning transactions that completed successfully</td>
</tr>
<tr>
<td>Failed Requests</td>
<td>ICAP scanning transactions that failed because of a scanning timeout, connection failure, server error, or a variety of other situations</td>
</tr>
<tr>
<td>Bytes Sent</td>
<td>Bytes of ICAP data sent to the ICAP service or service group</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Bytes Sent does not include secure ICAP traffic.</td>
</tr>
<tr>
<td>Bytes Received</td>
<td>Bytes of data received from the ICAP service or service group</td>
</tr>
<tr>
<td>Plain Connections</td>
<td>Number of connections between the ProxySG and the ProxyAV across which plain ICAP scanning requests are sent</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This statistic is not tracked for service groups.</td>
</tr>
<tr>
<td>Secure Connections</td>
<td>Number of connections between the ProxySG and the ProxyAV across which encrypted ICAP scanning requests are sent</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This statistic is not tracked for service groups.</td>
</tr>
</tbody>
</table>

Display Content Analysis ICAP Graphs on the ProxySG

Content Analysis ICAP graphs can be used as diagnostic and troubleshooting tools. For instance, if the Active Requests graph shows excessive queued ICAP requests on a regular basis, this may indicate the need for a higher capacity Content Analysis appliance.

1. Log in to the ProxySG Management Console.

2. To display ICAP graphs:
Monitor ICAP Scanning

- SGOS 6.5: Select **Statistics > ICAP**.
- SGOS 6.6 or higher: Select **Statistics > Content Analysis**.

3. Choose what you want to graph: **Services** or **Service Groups**.

4. To define the time period, display the **Duration** drop-down list, and choose from **Last Hour**, **Last Day**, **Last Week**, **Last Month**, or **Last Year**.

5. To select the type of graph, click one of the following tabs:

   - **Active Requests**—Plain, secure, deferred, and queued active ICAP transactions (sampled once per minute)
   - **Connections**—Plain and secure ICAP connections (sampled once per minute)
   - **Completed Requests**—Successful and failed completed ICAP transactions
   - **Bytes**—Bytes sent to the ICAP service and received from the ICAP service

Each statistic displays as a different color on the stacked bar graph. By default, all relevant statistics are displayed.
6. In the Name column in the table beneath the graph, select the name of what you want to graph:
   - The service name
   - The service group name
   - The Totals row (graphs all services or service groups)

7. (Optional) Disable check boxes next to any statistics you don’t want displayed on the graph.

**Additional Information**

- While the ICAP statistics screen is displayed, you can view new graphs by selecting different services, service groups, time periods, or graph types.
- Graphs automatically refresh every minute. This may be noticeable only on graphs with the Last Hour duration.
- To see the actual statistics associated with a bar on the graph, hover the mouse pointer anywhere on the bar. A box showing the statistics and total appears at the mouse pointer.

**Display ICAP Statistical Data**

If you are more interested in the data than graphs, the ICAP statistics screen displays this information as well; beneath the graph is a concise table that displays the number of successful and failed requests and number of bytes sent and received for each service or service group during the selected time period. The table also calculates totals for each statistic across all services or service groups.
1. Log in to the ProxySG Management Console.

2. To display ICAP statistics:

   SGOS 6.5: Select **Statistics > ICAP**.
   
   SGOS 6.6 or higher: Select **Statistics > Content Analysis**.

3. To define the time period, display the **Duration** drop-down list, and choose from **Last Hour**, **Last Day**, **Last Week**, **Last Month**, or **Last Year**.

   ![Duration: Last Hour](dropdown.png)

4. In the **Name** column in the table beneath the graph, select the name of what you want statistics for:
   - The service name
   - The service group name
   - The Totals row (all services or service groups)

5. Review the statistics. For the time period you selected, the ProxySG displays statistics for individual services as well as totals for all services.

   ![Statistics Table](table.png)

Monitor ICAP-Enabled Sessions on the ProxySG

For detailed information about active and errored sessions that have ICAP scanning enabled, view the Active Sessions and Errored Sessions pages. You can filter the session list to display only the ICAP-enabled sessions, so that you can easily view the ICAP state of each session (transferring, deferred, scanning, completed) and see fine-grained details (such as client IP address, server name, bytes, savings, and protocol).

Additional ICAP filters are available as well. You can also filter by:

- Type of ICAP service: REQMOD (request) or RESPMOD (response)
- Service name
- ICAP status (for example, display only the deferred connections)

Note that these additional filters are optional. If you leave all the options set to **Any**, all ICAP-enabled sessions will be displayed.
Symantec Content Analysis 2.4

By default, the Active Sessions screen displays all active sessions. When analyzing ICAP functionality, it’s helpful to filter the list to display only ICAP-enabled sessions.

1. Log in to the ProxySG Management Console.
2. To display active sessions, select **Statistics > Sessions > Active Sessions > Proxied Sessions**.
3. Select the ICAP filter.

```
Filter: ICAP
```

4. (Optional) Filter by type of ICAP service. Choose **REQMOD** or **RESPMOD**. Or choose **Any** to display both types of services.
5. (Optional) Filter by service name. Select the service name from the **Service** drop-down list, or choose **Any** to display all services.
6. (Optional) Select the ICAP state from the **Status** drop-down list: **transferring**, **deferred**, **scanning**, **completed**. Or choose **Any** to display all types of connections.

```
<table>
<thead>
<tr>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
</tr>
<tr>
<td>Any</td>
</tr>
<tr>
<td>transferring</td>
</tr>
<tr>
<td>deferred</td>
</tr>
<tr>
<td>scanning</td>
</tr>
<tr>
<td>completed</td>
</tr>
</tbody>
</table>
```

7. (Optional) Select **Show errored sessions only** to view only the current errored proxied sessions.
8. Click **Show**. The Proxied Sessions table displays the ICAP-enabled sessions.

```
<table>
<thead>
<tr>
<th>Proxied Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client: 10.100.1.16:8088 Node: ads.yahoo.com:80</td>
</tr>
<tr>
<td>Duration: 1.7 min Bytes: 20.891 20.891</td>
</tr>
<tr>
<td>Server: US-2ch01:80</td>
</tr>
<tr>
<td>Client: 10.100.16:9049 Node: us-new2.yahoo.com:80</td>
</tr>
<tr>
<td>Duration: 1.9 min Bytes: 3,375 3,420</td>
</tr>
<tr>
<td>Server: YH-19707</td>
</tr>
<tr>
<td>Client: 10.100.16:80218 Node: streamap.kr:80</td>
</tr>
<tr>
<td>Duration: 1.8 min Bytes: 913 22,511</td>
</tr>
<tr>
<td>Server: YH-19707</td>
</tr>
<tr>
<td>Client: 10.100.16:80331 Node: streamap.kr:80</td>
</tr>
<tr>
<td>Duration: 1.6 min Bytes: 874 919</td>
</tr>
</tbody>
</table>
```

Of particular interest in the Proxied Sessions table is the ICAP (I) column. This column indicates the status of the ICAP-enabled session, with unique icons identifying the ICAP status. The table below describes each of the icons.
<table>
<thead>
<tr>
<th>ICAP Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(magnifying glass)</td>
<td>Scanning – ICAP requests are in the process of being scanned</td>
</tr>
<tr>
<td>(arrow)</td>
<td>Transferring – ICAP requests are being transferred to the ICAP server</td>
</tr>
<tr>
<td>(clock)</td>
<td>Deferred – ICAP scanning requests have been deferred until the full object has been received</td>
</tr>
<tr>
<td>(checkmark)</td>
<td>Completed – ICAP scanning requests completed successfully</td>
</tr>
<tr>
<td>(i)</td>
<td>Inactive – The ICAP feature is inactive for the session or connection</td>
</tr>
<tr>
<td>no icon</td>
<td>Unsupported – ICAP is not supported for the corresponding session or connection</td>
</tr>
</tbody>
</table>

**View Statistics on the Content Analysis Appliance**

Content Analysis has a number of malware processing reports that give you statistical details about the various processes on the system so that you can see the effectiveness of each process.

- "View Cache Hits" below
- "View the Sandboxing Report" on the next page
- "View the File Reputation Report" on page 59
- "View the Whitelist and Blacklist Reports" on page 61
- "View Number of Bytes Scanned" on page 62
- "View Number of Objects Scanned" on page 63

**View Cache Hits**

Historical statistics for cache hits are available in **Statistics > Cache Hits**.

The *Cache Hits* report shows how many files have been served to users without scanning, because those files were found to match a hash of an earlier successful scan. This report counts the files that were served from any of the Content Analysis caches (**Antivirus, File Reputation, Predictive Analysis, Sandboxing**). Information is shown for the past hour, day, or 30 days.
Use the **Email Day Report** button to send the details on this page to the administrator email accounts (defined in **Settings > Alerts > Email**).

**View the Sandboxing Report**

Sandboxing statistics are available in **Statistics > Sandboxing**.

The Sandboxing report includes data for all sandbox services configured on Content Analysis: on-box, cloud, and external sandbox appliances. Note that the report does not include any samples manually submitted via the Malware Analysis tab, although it does include files submitted via REST API clients.

The report contains the following charts:

- **Threats blocked by sandboxing** This statistic gets incremented every time a file is blocked because of a malicious sandboxing verdict. This includes serving from the cache or real-time sandboxing.

- **Files submitted to sandboxing** This statistic gets incremented when a file is sent to a sandboxing profile or vendor for further analysis. If there are multiple profiles or vendors configured (such as two MA profiles and FireEye), there will be multiple submitted counts per file (three, in this example). In addition, if a zip file contains files that should be sandboxed, the submitted statistic increments for each file inside the zip.

- **Threats discovered by sandboxing** This statistic gets incremented for every submitted file that is found to be malicious. (The discovered statistic won't ever be bigger than submitted.)

The report can display data for the last hour, day or 30 days. To clear the information displayed on this page, click **Reset Statistics**.
Use the **Email Day Report** button to send the details on this page to the administrator email accounts (defined in **Settings > Alerts > Email**).

## View the File Reputation Report

File Reputation statistics are available in **Statistics > File Reputation**.

The *File Reputation* report (previously known as the whitelisting report) displays the number of files scanned, and of those files, the number of files allowed based on their reputation score and the processing time savings by minute. Statistics reflect files submitted via ICAP and REST API clients. View File Reputation statistics for the last hour, day, or 30 days. To clear the data displayed on this page, click **Reset Statistics**.

---

59 of 111
Use the **Email Day Report** button to send the details on this page to the administrator email accounts (defined in **Settings > Alerts > Email**).

**View the Predictive Analysis Report**

Predictive Analysis scanning statistics are available in **Statistics > Predictive Analysis**.

The Predictive Analysis report displays the number of files scored by Predictive Analysis services (Symantec Advanced Machine Learning, Cylance), how many of these files were found to be safe, how many contained threats, and how many were sent to a sandboxing service for further analysis. There are individual graphs for each category: Scored, Safe, Threats, Sandbox. Statistics reflect files submitted via ICAP and REST API clients.
View Predictive Analysis scan results for the last hour, day, or 30 days. To clear the data displayed on this page, click **Reset Statistics**.

Use the **Email Day Report** button to send the details on this page to the administrator email accounts (defined in **Settings > Alerts > Email**).

**View the Whitelist and Blacklist Reports**

Reports for whitelist and blacklist activity statistics are available in **Statistics > Whitelist/Blacklist**.

The **Whitelist/Blacklist** statistics page reports on when Content Analysis recognizes file hashes in scanned data that are defined either whitelist or blacklist in **Services > Whitelist/Blacklist**. The green circle on the top of this page tracks the whitelisted files that have been allowed, and the red circle tracks the blacklisted files that have been blocked. Statistics reflect files submitted via ICAP and REST API clients.
Two graphs on this page track the history of blacklist and whitelist matches over the past hour, day, or month. Click the appropriate button under Show me the past Hour, Day, or 30 Days to change the interval view. Files that are detected and blocked are also reported on the Content Analysis home page.

To clear the data displayed on this page, click Reset Statistics.

Use the Email Day Report button to send the details on this page to the administrator email accounts (defined in Settings > Alerts > Email).

View Number of Bytes Scanned

Scanned traffic byte statistics are available in Statistics > Bytes.

The Bytes report allows you to monitor how many bytes Content Analysis has processed from files submitted via ICAP and REST API clients in the past hour, day, or 30 days. To clear the data displayed on this page, click Reset Statistics.
Use the **Email Day Report** button to send the details on this page to the administrator email accounts (defined in **Settings > Alerts > Email**).

**View Number of Objects Scanned**

The **Objects** graph is available in **Statistics > Objects**.

The **Objects** report shows how many objects (files) Content Analysis has scanned in the past hour, day, or 30 days. The objects can be files submitted via ICAP or REST API clients. To clear the data displayed on this page, click **Reset Statistics**.
Underneath the graphs, a Recent Threats report lists the specific threats that Content Analysis has found, with the most recent threats listed first. The report indicates which CA module (such as Antivirus or File Reputation) found the threat, the type of protocol used for file submission (ICAP or API), the source of the threat, the IP address of the client that requested the infected file, and the date and time of the incident.

### Recent Threats

<table>
<thead>
<tr>
<th>Module</th>
<th>Type</th>
<th>Source</th>
<th>Location</th>
<th>Date Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklist</td>
<td>ICAP</td>
<td><a href="http://localhost/putty.exe">http://localhost/putty.exe</a></td>
<td>127.0.0.1</td>
<td>2016-01-22 12:39:56 (PST)</td>
</tr>
<tr>
<td>Sandboxing</td>
<td>API</td>
<td>10.158.87</td>
<td>API-client-D</td>
<td>2018-01-22 12:08:18 (PST)</td>
</tr>
<tr>
<td>Sandboxing</td>
<td>API</td>
<td>10.158.87</td>
<td>API-plaint-D</td>
<td>2018-01-22 12:04:56 (PST)</td>
</tr>
<tr>
<td>Sandboxing</td>
<td>API</td>
<td>10.158.87</td>
<td>API-plaint-D</td>
<td>2018-01-22 12:03:35 (PST)</td>
</tr>
</tbody>
</table>

Use the Email Day Report button to send the details on this page to the administrator email accounts (defined in Settings > Alerts > Email).
View Malware Reports in Symantec Management Center and Reporter

Symantec Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing results from Content Analysis and Malware Analysis (MA) appliances that are deployed as part of your Symantec security solution. You can then use Symantec Management Center to view malware reports from this database.

Earlier versions of Reporter collect data from multiple ProxySG appliances, and both Reporter and Management Center can generate malware reports from this database.

View Malware Reports in Management Center

Note: See "View a Reporter Report" in the Management Center WebGuide for more information.

1. Log in to Management Center.

2. Make sure you have added Reporter as a managed device. See the Management Center WebGuide for details.


4. Select a role and the Reporter database from the Database drop-down list. The database you select determines the list of available reports.

5. Select one of the following Security reports:

   Note: The reports listed below are available in Management Center 1.6-1.10; other versions of Management Center may have additional or different Security reports.

<table>
<thead>
<tr>
<th>Potentially Infected Clients - Unified</th>
<th>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporter 10.1.4 introduces the ability to create a database that includes malware scanning and sandboxing results from the Symantec Content Analysis (CA) and Malware Analysis (MA) appliances that are deployed as part of your SGOS proxy security solution. These reports are called Unified reports.</td>
<td></td>
</tr>
<tr>
<td>Displays an area, bar, column, or pie chart of the client IP addresses that might be infected by malicious content, as found by sandboxing, file reputation, predictive analysis score, antivirus, and WebPulse (GIN). By default, the report lists each IP address, sorted by the number of risky requests.</td>
<td></td>
</tr>
<tr>
<td><strong>Symantec Content Analysis 2.4</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Potential Malware Infected Clients</strong></td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a bar chart of the client IP addresses that might be infected by malicious content, as found by sandboxing, file reputation, antivirus, and WebPulse (GiN). By default, the report lists each IP address, sorted by the number of risky requests.</td>
</tr>
<tr>
<td><strong>Malware Detected Names</strong></td>
<td>Displays a bar chart of the names of the malware detected by Content Analysis. To view this report, you must add a Reporter appliance running 10.1.3.x or later.</td>
</tr>
<tr>
<td><strong>Blocked Users</strong></td>
<td>For each user, this report shows a bar chart of the number of requests that were blocked due to the URL being from one or more of the following categories: Spyware, Suspicious, Phishing, or Malicious. Note: This report will be blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td><strong>Blocked Request by User Agent</strong></td>
<td>For each user agent (browser + version), the report shows a bar chart of the number of blocked web requests to URLs from one of the following categories: Spyware, Suspicious, Phishing, or Malicious.</td>
</tr>
<tr>
<td><strong>Threat Sites Blocked</strong></td>
<td>Displays a bar chart of the websites that had blocked web requests to URLs from any of the following categories: Spyware, Suspicious, Phishing, or Malicious. The sites with the most blocked web requests appear at the top of the report.</td>
</tr>
<tr>
<td><strong>Trend of Risky Requests</strong></td>
<td>Displays a line graph that shows the number of risky web requests (for example, requests to URLs of malware categories) over the specified time period. The graph contains a shaded area that represents the normal requests range, which is a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of risky web requests during the last month.</td>
</tr>
<tr>
<td><strong>Trend of Risky Users</strong></td>
<td>Displays a line graph that shows the number of users making requests to URLs of risky categories (Spyware, Suspicious, Phishing, or Malicious) over the specified time period. The graph contains a shaded area that represents the normal count range, which is a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of users making risky web requests during the last month. Note: User drill-downs are blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td><strong>Trend of Blocked Requests</strong></td>
<td>Displays a line graph that shows the number of web requests that were blocked over the specified time period. The requests could be blocked for a variety of reasons, such as due to deny policies on the ProxySG appliance. The graph contains a shaded area that represents the normal requests range, which is a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of risky web requests blocked during the last month.</td>
</tr>
<tr>
<td><strong>Trend of Blocked Users</strong></td>
<td>Displays a line graph that shows the number of users who were blocked over the specified time period. The users could be blocked for a variety of reasons, such as due to deny policies on the ProxySG appliance. The graph contains a shaded area that represents the normal count range, a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of users blocked during the last month. Note: User drill-downs are blank if user name data isn’t available in the Reporter log file.</td>
</tr>
<tr>
<td>Trend of Th</td>
<td>Displays a line graph that shows the number of client IP addresses that accessed URLs in the following categories: Spyware, Suspicious, Phishing, or Malicious. The graph contains a shaded area that represents the <strong>normal count range</strong>, a range based on the organization's web traffic history over the last month. In addition, a dotted horizontal trend line indicates the average number of client IPs that were potentially infected during the last month.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Risky Clients</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a bar chart that provides details for the number of threats discovered by each detection method (sandboxing, file reputation, antivirus, WebPulse).</td>
</tr>
<tr>
<td>Threats</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database. Displays an area, bar, column, or pie chart that provides details for the number of threats discovered by each detection method—sandboxing, file reputation, predictive analysis score, antivirus, WebPulse (GIN).</td>
</tr>
<tr>
<td>Threats - Unified</td>
<td>To view this report, you must add a Reporter appliance running 10.1.3.x or later. Displays a column chart that shows the trend over time for each detection method–Sandboxing, File Reputation, Anti-virus, Web Pulse (GIN).</td>
</tr>
<tr>
<td>Trend of Threats</td>
<td>To view this report, you must add a Reporter appliance running 10.1.4.x or later and select a unified database. Displays an area, bar, column, or pie chart that shows the trend over time for each detection method–Sandboxing, File Reputation, Predictive Analysis score, Anti-virus, WebPulse (GIN).</td>
</tr>
<tr>
<td>Trend of Threats - Unified</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the number of threats by category (attack family or antivirus). Each colored section represents a threat type and corresponding number of incidents.</td>
</tr>
<tr>
<td>Threats - WAF</td>
<td>To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later. Displays an area, bar, column, or pie chart that shows the trend over time for antivirus and attack family threats.</td>
</tr>
</tbody>
</table>
Symantec Content Analysis 2.4

Attacks Per Family
To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later.
Displays an area, bar, column, or pie chart that shows the number of requests per attack type (for example, SQL injection). The data corresponds to that recorded for the x-bluecoat-waf-attack-family log field. Each slice represents an attack type. The chart displays only the top ten attack types.

Attacks Per Country
To view this report, you must add a WAF database from a Reporter appliance running 10.1.3.x or later.
Displays an area, bar, column, or pie chart that shows the total number of attacks per country. The bar is segmented; each color represents a different attack type. The chart displays only the top ten countries. The data is based on geolocation data and is only shown when either x-bluecoat-waf-attack-family or x-virus-id does not include "-".

Sandboxing Risk Score
To view this report, you must add a Reporter appliance running 10.1.3.x or later.
Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.

Trend of Sandboxing
To view this report, you must add a Reporter appliance running 10.1.4.x or later.
Displays an area, bar, column, or pie chart that shows the trend over time for each risk score.

Trend of Predictive Analysis
To view this report, you must add a Reporter appliance running 10.1.4.x or later.
Displays an area, bar, column, or pie chart that shows the trend over time for each predictive analysis score.

Trend of File Reputation
To view this report, you must add a Reporter appliance running 10.1.4.x or later.
Displays an area, bar, column, or pie chart that shows the trend over time for each file reputation score.

File Risk Score
To view this report, you must add a Reporter appliance running 10.1.3.x or later.
Displays a pie chart that shows the number of requests in each risk score. Each slice represents a risk score.

URL Threat
To view this report, you must add a Reporter appliance running 10.1.5.4 or later.
Displays a pie chart that shows the risk threat level (a rating between 1 and 10) of URLs. Malicious sites rank higher (for example, a 9 or 10) while a site that may be questionable, yet not malicious, may rank lower (for example, a 4 or 5). You can use the report to filter out specific risk levels. You can also see the users who visit the higher risk sites more frequently.

View Malware Reports in Reporter

Report 9.4 and higher have the following malware reports available.

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Requests Blocked by Site</td>
<td>Lists all URLs that were blocked because of suspected malware presence</td>
</tr>
<tr>
<td>Potential Malware Infected Clients</td>
<td>Lists all client IP addresses that might be infected by malicious content</td>
</tr>
<tr>
<td>Potential Threats</td>
<td>Lists malware names and URL categories for suspected threats</td>
</tr>
</tbody>
</table>
Fine-Tune the Configuration

This chapter describes techniques for improving the user experience during ICAP scanning (via patience pages or data trickling), ways to notify administrators about detected viruses, and several additional ICAP policies that you can implement.

Improve the User Experience .......................................................... 70
Patience Pages ............................................................................. 70
Data Trickling ............................................................................. 70
Deciding Between Data Trickling and Patience Pages .................. 71
Deferred Scanning ..................................................................... 72
Configure ICAP Feedback ............................................................... 73
Enable Deferred Scanning ............................................................. 74
Configure Email Alerts ................................................................. 74
Configure E-Mail Settings ............................................................. 76
Customize the Malware Scanning Policy .......................................... 77
Example: Customize the Malware Scanning Policy ........................ 78
Create User-Based ICAP Policy ...................................................... 79
Enable Web Authentication ............................................................ 80
Create Authorization Rules ......................................................... 81
Implement a Request Modification ICAP Service .......................... 85
Create an ICAP Request Service .................................................. 85
Create an ICAP Request Policy - Forward Proxy/DLP .................. 86
Improve the User Experience

To avoid having users abort and reinitiate their web requests due to scanning delays, you may want to provide feedback to let users know that scanning is in progress. This feedback can take the form of a patience page, or you can use data trickling and deferred scanning to mitigate scanning delays. All three of these techniques are discussed in the following topics:

Patience Pages .......................................................................................................................... 70
Data Trickling ............................................................................................................................ 70
Deciding Between Data Trickling and Patience Pages .............................................................. 71
Deferred Scanning ..................................................................................................................... 72
Configure ICAP Feedback .......................................................................................................... 73
Enable Deferred Scanning .......................................................................................................... 74

Patience Pages

Patience pages are HTML pages displayed to the user if an ICAP content scan exceeds the specified duration. For example, the HTML page can display an informative message, such as:

The content of the page you requested is currently being scanned. Please be patient...

You can configure the content of these pages to include a custom message and a help link. Patience pages refresh every five seconds and disappear when object scanning is complete.

Patience pages are not compatible with infinite stream connections—or live content streamed over HTTP—such as a web-cam or video feed. ICAP scanning cannot begin until the object download completes. Because this never occurs with this type of content, the ProxySG continues downloading until the maximum ICAP file size limit is breached. At that point, the ProxySG either returns an error or attempts to serve the content to the client (depending on fail open/closed policy). However, even when configured to fail open and serve the content, the delay added to downloading this large amount of data is often enough to cause the user to give up before reaching that point. See "Conserve Scanning Resources" on page 99 for some alternate solutions.

Data Trickling

Patience pages provide a solution to appease users during relatively short delays in object scans. However, scanning large objects, scanning objects over a smaller bandwidth pipe, or placing high loads on servers might disrupt the user experience because connection timeouts occur. To prevent such timeouts, you can allow data trickling to occur. Depending on the trickling mode you enable, the ProxySG either trickles—or allows at a very slow rate—bytes to the client at the beginning of the scan or near the very end.
The ProxySG begins serving server content without waiting for the ICAP scan result. However, to maintain security, the full object is not delivered until the results of the content scan are complete (and the object is determined to not be infected).

**Note:** This feature is supported for HTTP/HTTPS connections only; data trickling for FTP connections is not supported.

### Trickling Data from the Start

In *trickle-from-start* mode, the ProxySG buffers a small amount of the beginning of the response body. As Content Analysis continues to scan the response, the ProxySG allows one byte per second to the client.

After Content Analysis completes its scan:

- If the object is deemed to be clean (no response modification is required), the ProxySG sends the rest of the object bytes to the client at the best speed allowed by the connection.
- If the object is deemed to be malicious, the ProxySG terminates the connection and the remainder of the response object bytes are not sent to the client.

Trickling-from-start mode is the more secure option because the client receives only a small amount of data pending the outcome of the virus scan. However, the drawback is that users might become impatient, especially if they notice the browser display of bytes received. They might assume the connection is poor or the server is busy, close the client, and restart a connection.

### Trickling Data at the End

In *trickle-at-end* mode, the ProxySG sends the response to the client at the best speed allowed by the connection, except for the last 16 KB of data. As Content Analysis performs the content scan, the ProxySG allows one byte per second to the client.

After Content Analysis completes its scan, the behavior is the same as described in "Trickling Data from the Start" above.

Symantec recommends this method for media content, such as Flash objects. This method is more user-friendly than trickle-from-start mode because users tend to be more patient when they notice that 99 percent of the object is downloaded. Therefore, they are less likely to perform a connection restart. However, network administrators might perceive this method as the less secure method, as a majority of the object is delivered before the results of the ICAP scan.

### Deciding Between Data Trickling and Patience Pages

Depending upon the type of traffic, the ProxySG configuration options plus policy allow you to provide different ICAP feedback actions:
Symantec Content Analysis 2.4

- For interactive traffic, that is a request involving a web browser, you can use either data trickling or a patience page.

- For non-interactive traffic, that is a request that originates from a non-browser based application, such as automatic software downloads or client updates, patience pages are incompatible; you can choose to use data trickling or to provide no feedback to the user.

- Trickling is not supported with native FTP traffic. However, when trickling is enabled globally in the ICAP service configuration, patience pages are supported with the proceeding policy:

  ```xml
  <Proxy>
  service.name=FTP response.icap_feedback.interactive(patience_page, 5)
  </Proxy>
  ```

Based on whether your enterprise places a higher value on security or availability, the ProxySG allows you to choose between patience pages and data trickling.

Deferred Scanning

The deferred scanning feature helps to avoid network outages due to infinite streaming.

Infinite streams are connections such as web-cams or Flash media—traffic over an HTTP connection—that conceivably have no end. Characteristics of infinite streams may include no content length, slow data rate, and long response time. Because the object cannot be fully downloaded, the ICAP content scan cannot start; however, the connection between the ProxySG and Content Analysis remains open, causing a wastage of finite connection resources.

With deferred scanning, ICAP requests that are unnecessarily holding up ICAP connections are detected and deferred until the full object has been received.

How Deferred Scanning Works

When the number of ICAP resources in use has reached a certain threshold, the ProxySG starts deferring scanning of the oldest outstanding ICAP requests. Once the defer threshold has been reached, for every new ICAP request, the ProxySG defers the oldest ICAP connection that has not yet received a full object.

The defer threshold is specified by the administrator as a percentage. For example, if the defer threshold is set to 70 percent and the maximum connections are set to 100, then up to 70 connections are allowed before the ProxySG begins to defer connections that have not finished downloading a complete object.

When an ICAP connection is deferred, the connection to Content Analysis is closed. The application response continues to be received; when the download is complete, the ICAP request is restarted. The new ICAP request may still be queued if there are no available ICAP connections. Once a request is deferred, the ProxySG waits to receive the full object before restarting the request. If there is a queue when a deferred action has received a complete object, that action is queued behind other deferred actions that have finished. However, it will be queued before other new requests.
Deferred Scanning and Setting the Feedback Options

Depending on how you configure the ICAP feedback option (patience page or data trickling) and the size of the object, deferred scanning may cause a delay in ICAP response because the entire response must be sent to the Content Analysis at once.

If a patience page is configured, the browser continues to receive a patience page until the object is fully received and the outstanding ICAP actions have completed.

If the data trickle options are configured, the object continues to trickle during deferred scanning. However, due to the trickle buffer requirement, there may be a delay, with or without deferred scanning, before the ProxySG starts sending a response.

Configure ICAP Feedback

Use the following steps to configure the global feedback settings. To define additional feedback policy that applies to specific user and conditional subsets, use the Return ICAP Feedback action object in the web access layer.

1. Log in to the ProxySG Management Console.

2. Specify the amount of time to wait before notifying a web-browser client that an ICAP scan is occurring.
   a. SGOS 6.5: Select Configuration > External Services > ICAP > ICAP Feedback.
   b. SGOS 6.6 or higher: Select Configuration > Content Analysis > ICAP > ICAP Feedback.
   c. Locate the ICAP Feedback for Interactive Traffic section.
   d. Enter a value in the Provide feedback after ___ seconds filed.

3. Select the feedback method for interactive (browser-based) traffic:
   - Return patience page (HTTP and FTP patience pages are available)
   - Trickle object data from start (more secure form of trickling)
   - Trickle object data at end (this form of trickling provides a better user experience)

4. For non-interactive traffic, specify the amount of time to wait before notifying a client that an ICAP scan is occurring.
   a. Locate the ICAP Feedback for Non-Interactive Traffic section.
   b. Enter a value in the Provide feedback after ___ seconds field.

5. Select the feedback for non-interactive traffic:
Symantec Content Analysis 2.4

- Trickle object data from start
- Trickle object data at end

6. Click Apply to save the settings.

To customize the text on HTTP and FTP patience pages:

SGOS 6.5: Select Configuration > External Services > ICAP > ICAP Patience Page.
SGOS 6.6 or higher: Select Configuration > Content Analysis > ICAP > ICAP Patience Page.

**Note:** For FTP transactions to be able to use a patience page, you must use the policy gesture response.icap_feedback.interactive(patience_page, 5).

Enable Deferred Scanning

To enable deferred scanning, you edit the ICAP service.

1. Log in to the ProxySG Management Console.
2. Edit the ICAP service.
   a. SGOS 6.5: Select Configuration > External Services > ICAP > ICAP Services.
      SGOS 6.6 or higher: Select Configuration > Content Analysis > ICAP > ICAP Services.
   b. Select the ICAP service.
   c. Click Edit. The Edit ICAP Service window opens.
3. Enable scanning deferral.
   a. Select Defer scanning at threshold to enable the defer scanning feature.
   b. Enter a value (0-100) to set the threshold at which the ProxySG defers the oldest ICAP connection that has not yet received a full object. For example, if the maximum connections are set to 100 and you set the defer threshold to 65 percent, then up to 65 connections are allowed before the ProxySG begins to defer connections that have not finished downloading a complete object.
   c. Click OK to close the Edit ICAP Service window.
   d. Click Apply.

Configure Email Alerts

When significant events occur (such as when Content Analysis finds viruses and blocks files), Content Analysis can send alert messages to email addresses, local logs, syslog servers, and SNMP monitoring systems.
You can set Content Analysis to generate alerts for the following types of events:

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virus is found</strong></td>
<td>A virus was found in an ICAP session. If you have configured e-mail alerts, the URL of the web page where the virus was found is included in the e-mail. So that you do not accidentally launch the page, the URL is reformatted to make it unclickable. For example: <a href="http://virus.com">http://virus.com</a> is rewritten as hxxp://virus.com.</td>
</tr>
<tr>
<td><strong>File was passed through without being scanned</strong></td>
<td>A file was served to the user who requested it without any Content Analysis scanning. Based on the serve file policy setting in Services &gt; AV Scanning Behavior and Services &gt; AV File Types.</td>
</tr>
<tr>
<td><strong>File was blocked (exclude virus case)</strong></td>
<td>A file is blocked for any reason other than a virus infection. For example, the administrator decides to block password-protected compressed files.</td>
</tr>
<tr>
<td><strong>Anti-virus update failed</strong></td>
<td>The antivirus update failed due to an error in retrieving or installing the latest image.</td>
</tr>
<tr>
<td><strong>Anti-virus update succeeded</strong></td>
<td>A new version of an antivirus pattern file has been installed.</td>
</tr>
<tr>
<td><strong>Intelligent Connection Traffic Monitoring (ICTM)</strong></td>
<td>The maximum specified concurrent slow connection warning or critical thresholds has been reached.</td>
</tr>
<tr>
<td><strong>Reboot</strong></td>
<td>A system reboot has occurred on the appliance.</td>
</tr>
<tr>
<td><strong>Sandboxing Threat Admin Alert (Asynchronous)</strong></td>
<td>A newly discovered threat that the sandbox identified after it was delivered to the endpoint.</td>
</tr>
<tr>
<td><strong>Sandboxing Threat Alert</strong></td>
<td>The sandbox has identified a threat and blocked it using either real-time sandboxing or because it was found in the threat cache.</td>
</tr>
<tr>
<td><strong>File Reputation Threat Alert</strong></td>
<td>Whitelist scanning identified a threat within the configured Whitelisting threat threshold.</td>
</tr>
<tr>
<td><strong>Predictive Analysis Threat Alert:</strong></td>
<td>A predictive analysis service identified a file as potentially or absolutely infected with malware. Potentially infected files are sent to the configured sandbox server(s) (if configured) while absolutely infected files are blocked.</td>
</tr>
<tr>
<td><strong>File was blocked by user blacklist</strong></td>
<td>A file was blocked because its hash matched a hash on a custom blacklist.</td>
</tr>
</tbody>
</table>

Follow these steps to configure Content Analysis to send email alerts for significant events:
1. Log in to Content Analysis.

2. For each type of event you want to send an email alert:
   a. Select **Settings > Alert Locations**.
   b. For each type of event you want to send an email alert, select the check box in the E-mail column.
   c. Remove check boxes for any alert types you don’t want to use.
   d. Click **Save Changes**.

3. Configure the email server and settings. See "Configure E-Mail Settings" below.

### Configure E-Mail Settings

E-mail alert configuration is available in **Settings > Alerts > Email**.

When you enable email alerts for specific events, you must define an SMTP (Simple Mail Transfer Protocol) server and specify the e-mail addresses to which notifications will be sent.

![Screenshot of E-Mail Settings Configuration](image)

**E-mail Addresses**
- Sender e-mail address: `CAsystem33@domain.com`
- Recipient e-mail address(es): `sysadmin@domain.com`
- CC e-mail address(es): 

**Server Settings**
- Server address: `smtp.domain.com`
- Server port: `25`

**Authentication Settings**
- Username: `admin`
- Password: `************`
- Verify Password: `************`

Click **Save Changes**.
E-mail Addresses

- **Sender e-mail address** The sender's name will appear in the From line of any e-mail message that Content Analysis sends out. For example: `content_analysis@company.com`

- **Recipient e-mail address** The e-mail addresses to which alerts will be sent when alerts occur. Use a comma to separate addresses, for example: `user1@company.com,user2@company.com`.

**Warning**: At least one recipient address is required. If you don't set a recipient address, the appliance will not send alert e-mails.

Server settings

- **Server address** Your SMTP server hostname or IP address. This is the server that will send alert e-mail to your administrators.

- **Server port** The port used by your SMTP server. Typically, the port used for SMTP is 25.

Authentication settings

- If your SMTP server requires users to authenticate before sending mail, define your SMTP username and password.

- When you’re done entering your SMTP server settings, click **Save Changes**.

Customize the Malware Scanning Policy

When **malware scanning is enabled**, the threat protection policy is invoked. The rules implemented in the threat protection policy either use the defaults or the selections that you configured in the malware scanning options in **Configuration > Threat Protection > Malware Scanning** on the ProxySG appliance.

Unlike other policy files, the threat protection policy file is not displayed in the Policy Evaluation Order list in **Policy > Policy Options > Policy Options**, and the threat protection policy file cannot be edited or modified. However, you can create rules in the local policy file or in Visual Policy Manager (VPM) policy to supplement or override the configured defaults. The rules created in local or VPM policy supersede the configuration in the threat protection policy because of the evaluation order of policy files. By default on the ProxySG, policy files are evaluated in the following order: Threat protection, VPM, Local, Central, and Forward.

The threat protection policy is evaluated before the VPM, Local, Central, or Forward policy to provide you with the flexibility to adapt this policy to meet your business needs. For example, even if the malware scanning mode is configured at maximum protection through configuration, you can create rules in VPM to allow all traffic from internal hosts/subnets to be scanned using the high performance mode. Alternatively, if the default malware scanning mode is high performance, you can add rules in VPM to invoke maximum protection mode for sites that belong to select content filtering categories such as software downloads or spyware sources.
Example: Customize the Malware Scanning Policy

The following example demonstrates how to create rules in VPM to complement the malware scanning options that are set in configuration. In the example below, the configuration uses maximum protection for all malware scanning. In this example, you will create a VPM rule to allow internal traffic on a specific subnet to be scanned using the high performance setting; all other traffic will be scanned with maximum protection.

1. Log in to the ProxySG Management Console.

2. Verify that malware scanning is enabled and is set to Maximum protection.
   
   a. Select Configuration > Threat protection > Malware Scanning.
   
   b. Verify:
      
      SGOS 6.5: Enable malware scanning check box is selected.
      
      SGOS 6.6 or higher: Use external content analysis services option is selected.
      
      c. Verify that the Protection level is set to Maximum protection. This setting is global for all ICAP scanning between the ProxySG and Content Analysis.

3. Launch the VPM.
   
   
   b. Click Launch. The Visual Policy Manager opens in a new window.

4. Create policy to scan all traffic from an internal host using the high performance mode. This example uses the 10.0.0.0/8 subnet.
   
   
   b. In the Action field, right-click and select Set > New > Set Malware Scanning. The Add Malware Scanning Object dialog opens.
   
   c. Select Perform high performance malware scan.
Fine-Tune the Configuration

**Add Malware Scanning Object**

**Select Malware scanning level:**

- Use protection level set in configuration
- Perform maximum protection malware scan
- Perform high performance malware scan

**OK**  **Cancel**  **Help**

---

d. Click **OK** to save your changes and exit all open dialogs.

e. In the Destination field, right click and select **Set > New > Destination IP Address/Subnet**. The Set Destination IP/Subnet Object dialog opens.
f. Enter the IP address and subnet for the internal host (10.0.0.0 and 8), click **Add**, and then click **Close**.
g. Click **OK** to save your changes and exit all open dialogs.
h. Install the policy.
   
   a. Click **Install Policy**.
   
   b. Click **OK**.
   
   c. Close the VPM window.

After this policy is installed, all traffic from the internal subnet 10.0.0.0/8 will be scanned using the high performance mode. The completed rule is shown below.

---

### Create User-Based ICAP Policy

Your ICAP policy (created previously) on the ProxySG sends traffic to Content Analysis for scanning. You can make additions to your ProxySG policy to block/allow files based on the user’s or group’s name. For example, you may want to allow administrators to download certain file types (such as EXE files) that are blocked for other users.
Symantec Content Analysis 2.4

To set up user-based ICAP policies, you must complete the following tasks:

1. Create a web authentication layer that prompts for user credentials when a web browser is opened. See "Enable Web Authentication" below.

2. Create a web access layer with authorization rules that allow certain users access to blocked files and deny access to other users. See "Create Authorization Rules" on the facing page.

**Note:** These steps assume you have already configured Content Analysis and ProxySG appliances to work together. (See "Configure Symantec Appliances to Communicate" on page 22.) In addition, you need to have configured users and groups for authentication (using RADIUS, LDAP, Microsoft Active Directory, or other authentication servers) and created a realm on the ProxySG to connect to these servers; refer to the SGOS Administration Guide for more information.

Enable Web Authentication

To have users prompted for user name and password when they open a web browser, you need to create a web authentication layer in your policy.

1. Open the ProxySG Visual Policy Manager.
   a. Log in to the ProxySG Management Console.
   b. Select Configuration > Policy > Visual Policy Manager.
   c. Click Launch. The Visual Policy Manager opens in a new window.

2. Create a web authentication layer.
   b. Accept the proposed name or assign a descriptive name to the layer.
   c. Click OK.

3. Configure an authentication action.
   a. Right-click the Action field and select Set > New.

4. Specify the realm name for authentication.
   a. In the Name field, accept the proposed name or type a descriptive name for the object.
   b. In the Realm drop-down list, select the name of the previously-configured realm.
Create Authorization Rules

Create a rule that designates which users/groups are allowed access to blocked file types and which users/groups are denied access.

1. The Visual Policy Manager should still be open.

2. Create a web access layer.
   a. Select **Policy > Add Web Access Layer**.
   b. Accept the proposed name or assign a descriptive name to the layer.
   c. Click **OK**.

3. Create a user object for the user who you want to allow access to blocked file type.

   **Note**: If you have created user groups and want to create rules based on groups instead of individual users, you can create a group object instead of a user object. Follow the steps to the right, except specify group information.

   a. Right-click the Source field and select **Set > New**.
   b. Select **User**. The Add User Object dialog opens.
c. In the User field, type the user's name.

**Note:** Case is significant for local realms.

d. In the Authentication Realm drop-down list, select the name of the previously-configured realm.

e. Click OK; click OK again to add the object.

4. The destination policy object, Apparent Data Type, can be used to identify the types of files contained within an archive, after scanning that data for malware. Based on the rest of the policy, this can be used to control the types of files the users and groups you configured in step 3 can download, even if those files are contained within an archive, (such as zip, gz or rar archive types).

a. Right-click the Destination field and select Set > New.

b. Select Apparent Data Type. The Add Apparent Data Type Object dialog opens.

c. Choose the file types you wish to permit for this user.

d. Select Enable ICAP Scanning at the bottom of the dialog.

e. In the Name field, change the name to Restricted file types.

f. Click OK; click OK again to add the object.

5. Indicate that this user should be allowed access to blocked file types.

a. Right-click the Action field; select Allow. The rule should look similar to the following:
6. In the same web access layer, create a rule for another user/group. This rule will deny access to the user/group.
   a. Click **Add rule**. A new rule row is shown.
   b. Right-click the Source field, click **Set > New**. Select **User** or **Group** and enter or browse for the user or group that will not be permitted to download the restricted file types identified in step 5. Click OK to save this user or group as the source for the rule.
   c. Right-click the Destination field; select **Set**. The Set Service Object dialog opens.
   d. From the existing destination objects, select **Restricted file types**.
   e. Click **OK** to add the object. The rule should look similar to the following:

   ![Rule Configuration](image)

   Note that the default action is **Deny**, so it is already correctly set.

7. To define other users/groups to whom you want to allow or deny access, follow the above steps to create appropriate rules in the web access layer.

8. Install the policy (all layers).
   a. Click **Install Policy**.
   b. Click **OK**.
   c. Close the VPM window.

9. Test the policy.
   a. Users who have an Allow rule will be able to access URLs that point to blocked file types or have archive files containing a blocked file type (for instance, a ZIP file that contains an EXE file).
   b. Users who have a Deny rule will see a screen similar to the following when attempting to access a
Symantec Content Analysis 2.4

blocked file type:

Access Denied (policy_denied)

Your system policy has denied access to the requested URL.

For assistance, contact your network support team.
Implement a Request Modification ICAP Service

ICAP response modifications for incoming traffic are used for virus protection; ICAP request modifications for outgoing traffic are used for data leak protection (DLP) in Forward Proxy deployments and for malware scanning in Reverse Proxy deployments.

1. Create an ICAP service on the ProxySG for request modification.
2. Create a policy for the ICAP Request service for data leak protection on outbound traffic.
3. Test the policy.

**Note:** The same client request can have request modification applied before it is forwarded to the origin-content server and response modification applied as the object data returns.

Create an ICAP Request Service

Follow these general steps for creating an ICAP request modification service.

1. Log in to the ProxySG appliance Management Console.
2. Add a new ICAP service.
   a. SGOS 6.5: Select **Configuration > External Services > ICAP**.
      SGOS 6.6 or higher: Select **Configuration > Content Analysis > ICAP**.
   b. Click **New**. The Management Console displays the Add list Item dialog.
c. Enter a name for the Content Analysis service and click OK

d. Click Apply.

3. Select the new entry in the list and click Edit. The Edit ICAP Service dialog opens.

a. Enter the Service URL, which is the Content Analysis ICAP address. The format is as follows: icap://IP_address/ICAP_service, where IP_address is the Content Analysis IP address or hostname and ICAP_service is the name of the CAS appliance (CAS by default).

Note: Starting in SGOS 6.6, the Service URL does not require the ICAP_service when the ICAP server is Content Analysis or ProxyAV. You can enter icap://IP_address/.

b. Select request modification for the ICAP method.

c. Change other settings as required.

d. Click OK to close the dialog.

4. Click Apply.

Create an ICAP Request Policy - Forward Proxy/DLP

Configure the policy for ICAP requests. The ICAP request mode is used to scan an outgoing request for Forward Proxies where internal user requests can be subjected to URL filtering, antivirus scanning, or data leak prevention. In the following example, the ICAP request will scan all outbound HTTP, HTTPS, and FTP connections and will prevent you from uploading a virus to a public FTP server.
1. Open the ProxySG Visual Policy Manager.
   a. Log in to the ProxySG Management Console.
   b. Select **Configuration > Policy > Visual Policy Manager**.
   c. Click **Launch**. The Visual Policy Manager opens in a new window.

2. Create a web access layer.
   a. Select **Policy > Add Web Access Layer**.
   b. Accept the proposed name or assign a descriptive name to the layer.
   c. Click **OK**.

3. Create an HTTP/HTTPS service object for the request policy.
   a. Right-click the Service field; select **Set > New**.
   c. Name the protocol method *HTTP* and select **HTTP/HTTPS** from the **Protocol** list.
   d. In the *Common methods* section, select the **POST** and **PUT** check boxes, and click **OK**.

   ![Diagram](image)

4. Create an FTP service object.
   a. In the Set Action Object dialog, click **New**.
   c. Name the protocol method *FTP* and select **FTP** from the **Protocol** list.
Symantec Content Analysis 2.4

d. In the Commands that modify data section, select the STOR check box, and click OK.

5. Create a combined (HTTP and FTP) service object.
   a. In the Set Service Object dialog, click New > Combined Service Object.
   b. Select the HTTP object and click Add.
   c. Select the FTP object and click Add.
   d. Click OK.
   e. Click OK again to set the Combined Service object as the Web Access Layer service.

6. Set the action for the Request policy.
   a. Right-click the Action field and select Set > New.
   b. SGOS 6.5: Select Set ICAP Request Service. The Add ICAP Request Service Object dialog opens.
      SGOS 6.6 or higher: Select Perform Request Analysis. The Add Request Analysis Service Object dialog opens.
   c. Select the request service you previously created and click Add.
   d. Click OK, OK.

7. Install the policy.
   a. Click Install Policy.
   b. Click OK.
c. Close the VPM window.
Load Balance Multiple Content Analysis Appliances

This chapter describes how to set up load balancing of scanning requests when your deployment includes multiple Content Analysis appliances.

About ICAP Service Groups

A ProxySG ICAP service is a named entity that identifies the Content Analysis appliance, the ICAP method, and the supported number of connections. A service group is a named set of ICAP services. You will need to create service groups when you are using multiple Content Analysis appliances to process a large volume of scanning requests (load balancing).

ICAP service group of three Content Analysis ICAP servers

Your deployment can have multiple ProxySG appliances, each using an identical ICAP service group of multiple Content Analysis appliances.

To help distribute and balance the load of scanning requests when the ProxySG is forwarding requests to multiple services within a service group, the ProxySG uses an intelligent load balancing algorithm. When deciding which service in the service group to send a scanning request, this algorithm takes into consideration the following factors:

- Number of requests that are in a “waiting” state on each service (a request is in this state when it has been sent to the service but the response hasn’t been received)
- Number of unused connections available on each service (calculated by subtracting the number of active
Symantec Content Analysis 2.4

transactions from the connection maximum on the server)

- The user-assigned weight given to each server (see "Weighting" below)

Weighting

Weighting determines what proportion of the load one Content Analysis bears relative to the others. If all Content Analysis servers have either the default weight (1) or the same weight, each share an equal proportion of the load. If one server has weight 25 and all other servers have weight 50, the 25-weight server processes half as much as any other server.

Before configuring weights, consider the capacity of each server. Factors that could affect assigned weight of a Content Analysis appliance include the following:

- The processing capacity of one Content Analysis in relationship to other Content Analysis appliances (for example, the number and performance of CPUs or the number of network interface cards).
- The maximum number of connections configured for the service. The maximum connections setting pertains to how many simultaneous scans can be performed on the server, while weighting applies to throughput in the integration. While these settings are not directly related, consider both when configuring weighted load balancing.

Note: External services (ICAP, WebPulse, BCAA) have a reserved connection for health checks. This means that as the load goes up and the number of connections to the external service reaches the maximum, with additional requests being queued up and waiting, the maximum simultaneous connections is actually one less than the limit.

Having appropriate weights assigned to your services is critical when all Content Analysis servers in a service group become overloaded. As servers reach their capacity, proper weighting is important because requests are queued according to weight.

One technique for determining weight assignments is to start out by setting equal weights to each service in a group; then, after several thousand requests, make note of how many requests were handled by each service. For example, suppose there are two services in a group: Service A handled 1212 requests, Service B handled 2323. These numbers imply that the second service is twice as powerful as the first. So, the weights would be 1 for Service A and 2 for Service B.

Setting the weight value to 0 (zero) disables weighted load balancing for the ICAP service. Therefore, if one Content Analysis of a two-server group has a weight value of 1 and the second a weight value of 0, should the first Content Analysis go down, a communication error results because the second Content Analysis cannot process the request.

Load Balancing

When load balancing between services, how does the ProxySG decide which ICAP service to send a scanning request to? For each service, it calculates an index by dividing the number of waiting transactions by the server weight
Load Balance Multiple Content Analysis Appliances

(think of this as wait/weight). The ICAP service with the lowest index value will handle the new ICAP action, assuming that the service has an available connection to use. If it does not, it will send the request to the service with the next lowest index value that has a free connection.

Load will be distributed among services proportionally according to their configured weights until the maximum connection limit is reached on all services.

**Example 1**

Service A and B are in the same service group.

- Service A can handle up to 50 connections, is assigned a weight of 1, has 17 active transactions, with 5 transactions in the waiting state. The index is calculated by dividing the wait by the weight: $5/1 = 5$.
- Service B can handle up to 100 connections, is assigned a weight of 2, has 17 active connections, with 15 waiting transactions. The index is $15/2 = 7.5$.

Which service will the ProxySG assign the next ICAP action? Service A because it has a lower index.

**Example 2**

Service C and D are in the same service group.

- Service C can handle up to 5 connections, is assigned a weight of 1, has 5 active transactions, with 1 transaction in the waiting state. The index is $1/1=1$.
- Service D can handle up to 10 connections, is assigned a weight of 1, has 7 active transactions, with 5 waiting transactions. The index is $5/1=5$.

To which service will the ProxySG assign the next ICAP action? Although Service C has a lower index than Service D, it does not have any available connections; therefore, the ProxySG will assign the next ICAP action to Service D which has several free connections.

**Specify Weight within an ICAP Service Group**

An ICAP service group is automatically created when you add one or more Content Analysis appliances to the ProxySG. For example, the proxyav service group includes all response modification services configured on the ProxySG.

To load balance, each service in the service group must be assigned a weight. This weight value specified determines the number of requests that will be directed to each Content Analysis in the service group.

To assign weights to an ICAP service group:

1. Log in to the ProxySG Management Console.
2. Edit the service group to assign a weight to each service in the group.
Symantec Content Analysis 2.4

a. SGOS 6.5: Select Configuration > External Services > Service Groups.

SGOS 6.6 or higher: Select Configuration > Content Analysis > Service Groups.

b. Select the service group and click **Edit**; the Edit Service Group dialog opens.

c. Select a service and click **Edit**; the Edit Service Group Member dialog open.

d. In the **Entry Weight** field, assign a weight value. The valid range is 0-255.

e. Click **OK** to close the dialog.

f. Repeat steps c -e for each service in the group.

g. Click **OK** again to close the Edit Service Group Entry dialog.

h. Click **Apply**.

Create Load Balancing Policy

An ICAP response load balancing policy is essentially the same as a standard ICAP response policy; the only difference is that you specify the service group as the response service object instead of the service.

Using the ICAP load balancing policy, the ProxySG sends ICAP response modification requests to Content Analysis appliances in the service group. The load carried by each Content Analysis appliance in the group is determined by the weight values that you assigned in the previous task.

1. Open the ProxySG Visual Policy Manager.

   a. Log in to the ProxySG Management Console.

   b. Select **Configuration > Policy > Visual Policy Manager**.

   c. Click **Launch**. The Visual Policy Manager opens in a new window.

2. Create a web content layer.

   a. Select **Policy > Add Web Content Layer**.

   b. Assign a descriptive name to the layer (for example, CAcluster).

   c. Click **OK**.

3. Create an action for the rule.

   a. Right-click the Action field; select **Set**. The Set Action Object dialog opens.

   b. Click **New**.

   c. SGOS 6.5: Select **Set ICAP Response Service**. The Add ICAP Response Service Object dialog
opens.

SGOS 6.6 or higher: Select **Perform Response Analysis**. The Add Response Analysis Service Object dialog opens.

4. Configure the response service group object.
   a. In the **Available services** list, select the response service group and click **Add**.
   b. Select **If available use secure ICAP connections** for the secure ICAP mode.
   c. In the **Error Handling** section, select **Deny the client request**.
   d. Click **OK**; click **OK** again to add the object.

5. Install the policy.
   a. Click **Install Policy**.
   b. Click **OK**.
   c. Close the VPM window.
Configure Content Analysis Failover

Failover is the ability to switch over automatically to a redundant or secondary appliance when the primary appliance fails. To ensure that your network is always protected from malware threats, you can deploy two Content Analysis appliances on the same subnet and configure ICAP processing to fail over to the second appliance if the primary Content Analysis goes down.

When creating an ICAP policy, you specify a list of ICAP services to use, in order of preference. If the first service in the list does not pass the health checks, the ProxySG uses the next healthy service on the list to perform the scanning. This alternate Content Analysis appliance is called the *standby server*.

The primary Content Analysis appliance resumes ICAP processing when the next health check is successful; the standby Content Analysis appliance does not retain the primary responsibility.

*Notes*

- Failover is configured as part of the ICAP policy definition.
- You cannot configure failover policy until ICAP services are configured on the ProxySG.
- To avoid errors, ICAP service names cannot be named fail_open or fail_closed (the CLI commands prevent these names from being created).

Create Content Analysis Failover Policy

A Content Analysis failover policy is similar to a standard ICAP response policy, except that you add two services to the policy (one for each Content Analysis appliance). The order in which you select the services determines which Content Analysis is considered the primary server and which is considered the standby server: the primary should be selected first. The ICAP failover policy tells the ProxySG to use the primary Content Analysis appliance for all ICAP scanning. If the primary server fails, the ProxySG will use the standby Content Analysis appliance for scanning until the primary server is healthy again.

The following procedure assumes that you have already created an ICAP service for each Content Analysis appliance. (See “Automatically Configure an ICAP Service on the ProxySG” on page 30 or “Manually Configure an ICAP Service on the ProxySG” on page 36.) Note that the services must be of the same type (for instance, response modification).

1. Open the ProxySG Visual Policy Manager.
   a. Log in to the ProxySG Management Console.
   b. Select **Configuration > Policy > Visual Policy Manager**.
   c. Click **Launch**. The Visual Policy Manager opens in a new window.

2. Create a web content layer.
Note: If you already have a web content layer with a scanning policy, you should either delete it and create the rule described below, or modify the existing rule to match the settings below.


b. Assign a descriptive name to the layer (for example, CAfailover).

c. Click OK.

3. Create an action for the rule.

a. Right-click the Action field; select Set. The Set Action Object dialog opens.

b. Click New.

c. SGOS 6.5: Select Set ICAP Response Service. The Add ICAP Response Service Object dialog opens.

   SGOS 6.6 or higher: Select Perform Response Analysis. The Add Response Analysis Service Object dialog opens.

4. Configure the response service group object.

a. SGOS 6.5: Select Use ICAP response service.

   SGOS 6.6 or higher: Select Use the following external response analysis service.

b. In the Available services list, select the primary Content Analysis service and click Add.

c. In the Available services list, select the secondary (standby) Content Analysis service and click Add.

d. Select Deny the client request.

e. Click OK; click OK again to add the object.

5. Install the policy.
a. Click Install Policy.

b. Click OK.

c. Close the VPM window.
Configuration Best Practices

This chapter describes strategies for improving scanning performance as well as best practice guidelines for configuring antivirus and sandbox settings.

Conserve Scanning Resources .......................................................................................................................... 99
  Scan-and-Serve Policy Using Mirroring ............................................................................................................. 99
Avoid Processing of Canceled Connections ........................................................................................................ 102
Antivirus Scanning Best Practices ..................................................................................................................... 102
  Vendor-Specific Settings .................................................................................................................................. 103
Sandboxing Best Practices .................................................................................................................................. 103
Conserve Scanning Resources

HTTP web objects range from very small to very large in size, and for each scanned object, a scanning resource (connection) is used on Content Analysis. Some objects, referred to as infinite streams or slow downloads, do not have finite object ends. For example, a stock ticker is an infinite data stream that is transmitted over HTTP using a web browser.

Since Content Analysis has a finite number of ICAP connections available at any given time, attempting to scan this type of data can potentially consume significant time and Content Analysis resources (potentially slowing other scans)—until an error is returned. If allowed to continue, these transfers fail with one of the following ICAP error codes:

- Maximum file size exceeded
- Scan timeout

The default configuration of Content Analysis triggers such errors after the file size exceeds 100MB or after 800 seconds of scanning. While these settings are appropriate for other types of web objects, they don’t work for infinite streams such as web-cams and stock tickers. To address this issue, you can:

- Enable deferred scanning (See "Deferred Scanning" on page 72 and "Enable Deferred Scanning" on page 74.)
- Implement a mirroring policy (See "Scan-and-Serve Policy Using Mirroring " below.)
- Use Symantec’s customizable policy templates to help you configure CPL policy that bypasses content scanning for low-risk/high-volume content. See Secure Web Gateway - Content Analysis Policy Best Practice for details on downloading, customizing, and installing the policy template.

Scan-and-Serve Policy Using Mirroring

This example uses the ICAP mirroring policy action, introduced in SGOS 6.5. This policy action allows you to serve content for known, difficult-to-handle data types (such as stock tickers or media streams without end, also known as infinite streams) directly to users, without needing to have them wait for Content Analysis to scan portion or the complete stream before it is served to their browser. When invoked, this policy action opens two connections - one to serve the file to the requesting user and another to one to the ICAP server to be scanned.

The target for this solution is ProxySG/Content Analysis deployments that require all data to be scanned for company or governmental regulations. All data will be scanned, but with no delay for the user. If a threat is detected during scanning while the user is still accessing the data, the user’s connection will be terminated.

The Scan-and-Serve policy ensures that all data is sent to the ICAP server.
Install a Scan-and-Serve Policy for Slow Downloads

1. Download the CPL text file attached to this PDF. Alternatively, you can copy and paste the text:
   a. Copy the policy text after this procedure to your clipboard.
   b. Paste it into a text document and save it to your desktop or other convenient location.
   c. Modify the policy to meet your requirements.
2. Log in to the ProxySG Management Console.
3. Install the policy file.
   a. Select Configuration > Policy > Policy Files.
   b. From the Install Local File from drop-down list, select Text Editor.
   c. Click Install. A browser window displays the Edit and Install the Local Policy File page.
   d. Open your CPL file and copy the text.
   e. Return to the Edit and Install the Local Policy File page, and paste the contents of the file at the end of the local policy file on your ProxySG.
   f. Click Install. A dialog opens, informing you whether the installation was successful. If necessary, correct any errors in the file and reinstall it.

CPL Code for Scan-and-Serve Policy

Note: This policy requires SGOS version 6.5.7.7, 6.6.3.2, or higher and expects that you have an existing ICAP rule elsewhere in policy.

;------------------START ICAP Best Practices Scan and Serve CPL as of December 17, 2015
;ICAP Best Practices - Scan and Serve Policy is designed to be placed in local policy
;which, by default, is evaluated after other policy files (such as VPM).
;This policy requires that the ProxySG appliance is running SGOS 6.5.7.7, 6.6.3.2, or higher.
;Modify the policy with known infinite stream URLs under the “Bad_response_for.ICAP” section.

<CACHE>
delete_on_abandonment(yes)

<PROXY>
condition=http_https_scheme response.icap_mirror(yes) condition=ICAP_Mirror

   define condition http_https_scheme
   url.scheme=http
url.scheme=https
end condition http_https_scheme

define condition ICAP_Mirror
; Negate ICAP service only if the OCS response is undesirable
    condition=Bad_response_for_ICAP condition=Not_ICAP_service
end condition ICAP_Mirror

define condition Bad_response_for_ICAP
    condition=NO_or_LARGE_CONTENT_LENGTH
    condition=MEDIA_MIME_TYPES
    condition=HTTPv0.9_UserAgents
    ; Yahoo stock ticker problem -15sep06
    url.domain=//streamerapi.finance.yahoo.com
    url.domain=//stream.aol.com
    url.domain=//finance.google.com
    ; Other streaming media exceptions
    url.domain=//youtube.com
    url.domain=//pandora.com
end condition Bad_response_for_ICAP

define condition NO_or_LARGE_CONTENT_LENGTH
; note- the following line is correct- do NOT add .* between quotes
    response.header.Content-Length=!"" ; true if Content-Length header is not present
    response.header.Content-Length=!"^[0-9]{1,8}$" ; >9,999,999
end condition NO_or_LARGE_CONTENT_LENGTH

define condition MEDIA_MIME_TYPES
    response.header.Content-Type="video/"
    response.header.Content-Type="application/streamingmedia"
    response.header.Content-Type="application/x-streamingmedia"
    response.header.Content-Type="application/vnd.rn"
    response.header.Content-Type="application/ogg"
    response.header.Content-Type="application/x-ogg"
    response.header.Content-Type="audio/"
    response.header.Content-Type="multipart/x-mixed-replace"
end condition MEDIA_MIME_TYPES

define condition HTTPv0.9_UserAgents
    http.response.version=0.9 condition=MisBehaving_Old_UserAgents
end condition HTTPv0.9_UserAgents

define condition MisBehaving_Old_UserAgents
    request.header.User-Agent="Winamp"
    request.header.User-Agent="NSPlayer"
    request.header.User-Agent="RMA"
    request.header.User-Agent="ultravox"
    request.header.User-Agent="itunes"

Avoid Processing of Canceled Connections

When an HTTP request appears cacheable, the ProxySG completes the download, even if the requesting client has abandoned the connection. This allows the ProxySG to store a cached version of the object for future requests. However, for slow downloads, this behavior can result in each client request queuing a separate instance for scanning.

To avoid the continued processing of a request after the client application has disconnected, you can enable the CPL property delete_on_abandonment for certain client applications.

Delete_on_abandonment does not work when patience pages are enabled; it can be used only with data trickling or with no ICAP feedback.

The following example policy prevents queuing of duplicate requests for a known aggressive client:

```
<cache>
request.header.User-Agent="Winamp" delete_on_abandonment(yes)
</cache>
```

Alternatively, you can enable delete_on_abandonment for all clients, using the following code:

```
<cache>
delete_on_abandonment(yes)
</cache>
```

Antivirus Scanning Best Practices

Content Analysis scanning behavior options allow you to set the parameters for optimal malware scanning. These options are in the Services > AV Scanning Behavior screen.

The default values for antivirus scanning behavior policies are defined with security best practices in mind. Under typical operation, the default values should not require modification.

- **Cached responses**—Enabling this setting allows Content Analysis to return cached responses to the ProxySG appliance when applicable. If the hash of the data matches a file that Content Analysis has already determined to be clean or contain a virus, it returns the cached response. It is faster and more efficient to check a file's status in the cache rather than to rescan a file whose status is already known.
- **File size/count limitations**—The maximum individual file size that can be scanned. Because larger file sizes require longer to scan, be sure to increase the connection timeout value on the ProxySG’s ICAP service if you increase the maximum file size on Content Analysis. For example, if you leave the default maximum file size at 100 MB, the default connection timeout value (70 seconds) would be sufficient. But if you allow 2 GB files, a timeout value of 70 would be too low.

- **Policies for antivirus exceptions**—**Block** (the default) is the recommended policy for each situation. In other words, Content Analysis will drop the file (rather than serve it unscanned) when timeouts and file sizes are exceeded and when errors are encountered.

**Vendor-Specific Settings**

Kaspersky scanning behavior can be improved by enabling the **antivirus engine heuristic** and **enhanced scanning**. These options allow for threats other than those defined in the current pattern database to be identified.

**Sandboxing Best Practices**

By default, users are permitted to download a file when Content Analysis sends it to be analyzed by a configured sandbox. If a threat is detected, that detection is added to the system cache, and subsequent requests for the same file are denied. For added security, Content Analysis supports optional real-time sandbox analysis, preventing users from being infected during sandbox analysis.

Because the time it takes to analyze files in sandboxes can vary from a few seconds to a few minutes, enabling real-time sandbox scanning can result in an increase in the number of open ICAP connections between the ProxySG appliance and Content Analysis. After the maximum number of ICAP connections are used, ICAP requests are queued on the ProxySG appliance.

To avoid queuing issues, Symantec recommends you limit real-time scanning to specific file types. To designate which file types you want to scan real-time, select **Services > Sandboxing** and view the **Files Types and Extensions** panel. To enable real-time scanning for a file type, select **Wait for Result** (Note that **Sandbox** will also be selected.). If neither option is checked for a file type, Content Analysis will not send the file to Malware Analysis.
## File Types and Extensions

<table>
<thead>
<tr>
<th>Sandbox</th>
<th>Wait For Result</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td></td>
<td>Windows Installer (.msi)</td>
</tr>
<tr>
<td>✔</td>
<td>✔</td>
<td>Application (.exe)</td>
</tr>
<tr>
<td>✔</td>
<td></td>
<td>Application Extension (.dll)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS CAB archive file (.cab)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>True Type Font file (.ttf)</td>
</tr>
<tr>
<td>✔</td>
<td></td>
<td>MS Word Document (.doc)</td>
</tr>
<tr>
<td>✔</td>
<td></td>
<td>MS Excel Worksheet (.xls)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS PowerPoint Presentation (.ppt)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MS Visio Document (.vsd)</td>
</tr>
<tr>
<td>✔</td>
<td>✔</td>
<td>Adobe Portable Document Format (.pdf)</td>
</tr>
</tbody>
</table>
## Troubleshoot ProxySG+Content Analysis Integration Problems

This chapter provides solutions to problems you may have when integrating the ProxySG and Content Analysis appliances.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Analysis is not scanning web traffic</td>
<td>106</td>
</tr>
<tr>
<td>Users cannot access any websites</td>
<td>106</td>
</tr>
<tr>
<td>ProxySG runs out of memory during heavy traffic load</td>
<td>110</td>
</tr>
<tr>
<td>Scans are taking too long</td>
<td>110</td>
</tr>
<tr>
<td>Content Analysis is not getting virus updates</td>
<td>110</td>
</tr>
<tr>
<td>Firefox bypasses Content Analysis processing</td>
<td>111</td>
</tr>
</tbody>
</table>
Symantec Content Analysis 2.4

Content Analysis is not scanning web traffic

**Symptoms:** The ICAP Objects report on Content Analysis does not show any files being scanned for the last hour (or other recent time period). The ProxySG’s Statistics > ICAP (SGOS 6.5) or Statistics > Content Analysis (SGOS 6.6) page does not display any requests, connections, or bytes for the last hour (or other recent time period).

**Solutions:** If Content Analysis is not scanning web traffic, there is likely a configuration error that is preventing the ProxySG from sending traffic to Content Analysis. Here are a few things to double-check:

- Did you create an ICAP service on the ProxySG? See "Automatically Configure an ICAP Service on the ProxySG" on page 30 or "Manually Configure an ICAP Service on the ProxySG" on page 36.

- Does the ICAP service have the correct URL of the Content Analysis appliance? Does the URL include the same antivirus service name specified on Content Analysis? If you changed the antivirus service name from its default (proxyav1), you must make sure to include this same name as part of the Service URL for the ICAP service on the ProxySG. The Service URL should look something like this: ica://203.0.113.17/proxyav1

  **Note:** Starting in SGOS 6.6, the service name is not required when specifying a Service URL for Content Analysis or ProxyAV.

- Did you create a policy for the ICAP service? See "Automatically Configure an ICAP Service on the ProxySG" on page 30 or "Configure ICAP Policy" on page 39.

Users cannot access any websites

**Symptoms:** All users get a denied message in their web browsers when trying to go to any website.

**Solution 1:** If Content Analysis is down and your ICAP policy is set to Deny the client request if an error occurs during ICAP processing, users will not be able to browse the Internet — all requests will be denied. Thus, if you have created your ICAP policy on the ProxySG before setting up Content Analysis, users will not have web access. Therefore, it’s important to have Content Analysis up and running before you install the ICAP policy.
To avoid the inevitable support calls that result from lack of web access when Content Analysis is down, you may want to consider changing the ICAP policy to **Continue without malware scanning** (SGOS 6.6) or **Continue without further ICAP response processing** (SGOS 6.5). With this setting, users will be able to browse the Internet when Content Analysis is down. However, this opens up the network to potential viruses being downloaded during Content Analysis downtime. (Although desktop virus scanners might provide some protection from malware.)

Another way to avoid this problem is to have a standby Content Analysis appliance that will take over processing when the primary ICAP server is down. See "Configure Content Analysis Failover" on page 95.

**Solution 2:** This problem can also be caused by inconsistent secure ICAP settings for the ICAP service, Content Analysis, and ICAP policy. If you want to use secure ICAP for HTTPS, you need to enable it in all three places. The following series of screenshots show the proper settings that should be in place to allow users to browse secure websites (scanned with secure ICAP) and non-secure websites (scanned with plain ICAP).
Symantec Content Analysis 2.4

Secure ICAP enabled on the ICAP service (configured on the ProxySG)
Secure ICAP enabled in the policy for the ICAP response service (configured in the VPM)

**Solution 3:** This problem can be caused by incorrect SSL configuration for secure ICAP. See "Enable Secure ICAP Connections" on page 23.

**Solution 4:** The antivirus license could be invalid or expired. To check the status of the antivirus license on Content Analysis, select **System > Licensing.**
Symantec Content Analysis 2.4

**ProxySG runs out of memory during heavy traffic load**

**Symptoms:** The ProxySG becomes unresponsive and needs to be restarted.

**Solution:** The most common cause of this problem is setting too high of a value for the Maximum number of connections for the ICAP service. With too high of a value, ICAP connections start queuing up, and eventually the ProxySG will run out of memory and need to be restarted. Refer to the following table to make sure you set the appropriate maximum value.

<table>
<thead>
<tr>
<th>Model</th>
<th>Recommended ICAP Connections</th>
<th>Maximum ICAP Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS-S200-A1</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CAS-S400-A1</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>CAS-S400-A2</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>CAS-S400-A3</td>
<td>200</td>
<td>300</td>
</tr>
<tr>
<td>CAS-S400-A4</td>
<td>300</td>
<td>400</td>
</tr>
<tr>
<td>CAS-S500-A1</td>
<td>400</td>
<td>500</td>
</tr>
<tr>
<td>(600 when using Symantec AV)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAS-V100 (CAS-VA)</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

If you have two ProxySG appliances sending ICAP requests to a single Content Analysis, you also need to be careful about not setting too high of a value for Maximum number of connections. If more than one ProxySG appliance communicates with your Content Analysis appliance, divide the maximum number of connections among them.

**Scans are taking too long**

**Symptoms:** Users complain about delays in web browsing.

**Solution:** Slow scanning is most likely caused by Content Analysis attempting to virus scan infinite streams. To avoid this problem, Symantec recommends that customers enable deferred scanning or implement a mirroring policy.

**Content Analysis is not getting virus updates**

**Symptoms:** The network administrator gets an e-mail notification that the antivirus update failed.

**Solution 1:** It is possible that the DNS server was temporarily down or some other network problem interfered with the virus update. Try forcing the update by selecting Services> AV Patterns and clicking Force Update All Now.

**Solution 2:** Each antivirus vendor provides pattern file updates that necessarily contain portions (or descriptions) of viruses. Generally, these virus segments are encoded and are too small to be mistaken as a true virus by other AV vendors. But occasional false positives occur. These can be prevented by exempting virus pattern update locations...
from scanning, as the following example policy illustrates (place this policy after all other ICAP policies on the ProxySG):

```xml
<cache>
  url.host=download.bluecoat.com response.icap_service(no)
  url.host=av-download.bluecoat.com response.icap_service(no)
</cache>
```

**Firefox bypasses Content Analysis processing**

**Symptoms:** Websites viewed in a Firefox browser are not being scanned.

**Solution:** Add the following CPL to your policy:

```xml
<proxy>
  category=Suspicious action.strip_range(yes); or url, domain, request headers, other categories.
  define action strip_range
  delete( request.header.Range )
end
```