clearswift

Clearswift SECURE ICAP Gateway integration with Barracuda NextGen Firewall

Technical Guide

Version 01

14/07/2016

Copyright

Version 1.0, July, 2016

Published by Clearswift Ltd.

Contents

1 Introduction

Clearswift technology provides the ability to completely decompose communication flows and inspect their content to identify critical information and perform the appropriate mitigation actions as defined in the information security policy. Thanks to the Clearswift SECURE ICAP Gateway this technology is made available to third parties that can make use of the ICAP interface to enforce the corporate security policy.

Barracuda Networks provides as part of their security portfolio the Barracuda NextGen Firewall to protect organization's networks. The product includes a proxy with the ability to perform HTTPS decryption and to forward traffic through ICAP to an external device for inspection.

By combining both solutions, clients can benefit from a consolidated and integrated platform that can protect organizations' network traffic, while ensuring the appropriate information security policy is applied on both incoming and outgoing web traffic.

This guide provides the list of tasks to deploy and configure an integrated architecture. It is advisable to follow the deployment and configuration guides from both Barracuda and Clearswift for their respective products to have a better understanding of the capabilities of the technology as well as to configure the platform to be able to fulfill the business and technical requirements.

2 Architecture Overview

Barracuda NextGen Firewall includes a proxy as part of its defenses. By enabling it different stacks are used for client and server connections. Before the traffic is forwarded from one stack to the other, the Barracuda system can send the content of the requests and responses for inspection to the configured remote scanner using ICAP.

In this architecture, users connect to the proxy to access content from external web servers:

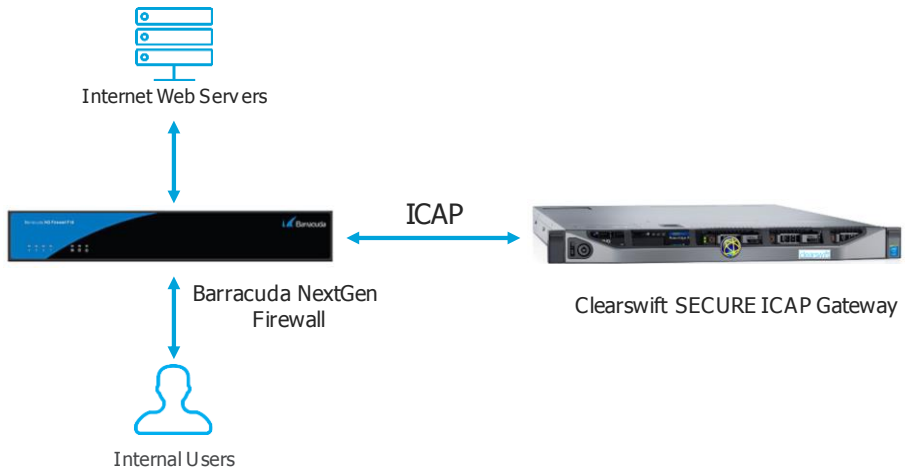


Figure 1: Barracuda NextGen Firewall and Clearswift SECURE ICAP Gateway integrated architecture

The Clearswift SECURE ICAP Gateway can then be used to enforce the appropriate information security policy for the traffic traversing the Barracuda NextGen Firewall.

This guide describes how to install and configure both the Clearswift ICAP Gateway and the Barracuda NextGen Firewall to integrate both products following the architecture described above.

3 Configuration and Setup

3.1 Overview

The configuration of the platform involves configuring the Clearswift SECURE ICAP Gateway to accept connections and configuring the Barracuda system to use an external Malware Protection in its proxy to forward requests and responses for adaptation.

It is important to note that requests are always considered to come from users and responses from servers. Different policies for requests and responses can be enforced by performing the appropriate configuration in the SECURE ICAP Gateway policy.

The configuration tasks in the Barracuda system include enabling the HTTP proxy and configuring an external malware protection system. This configuration is shown as a reference and it is strongly recommended to follow Barracuda's documentation to perform such tasks.

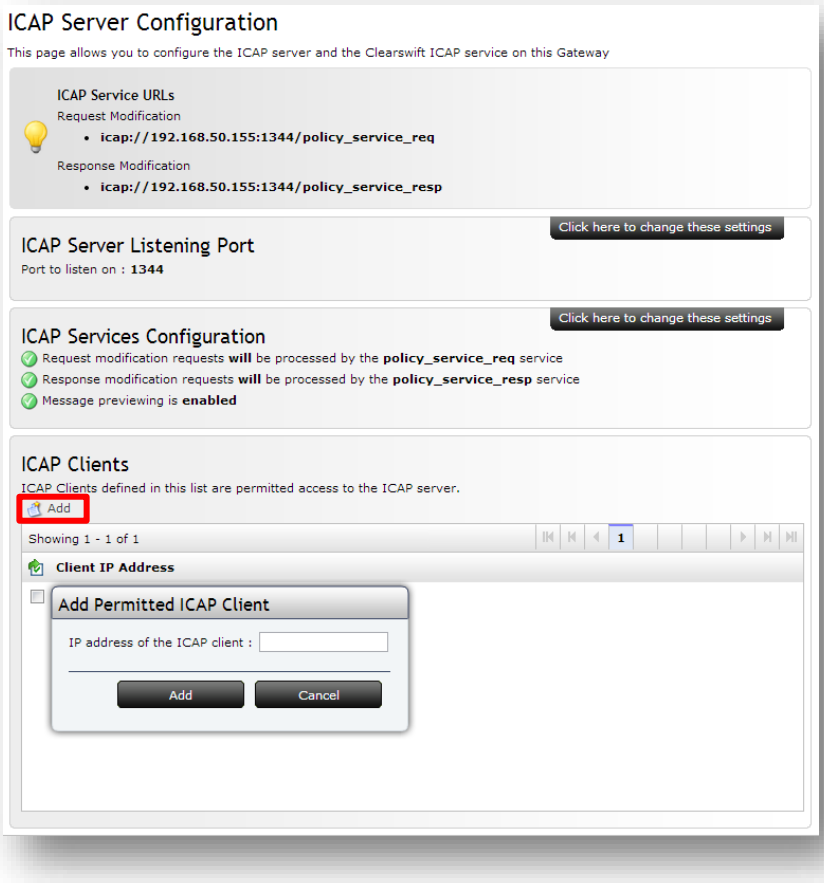
The following sections describe how to configure the integration of both products.

3.2 Clearswift SECURE ICAP Gateway configuration

The Barracuda NextGen Firewall acts as an ICAP client as it sends requests for content to be inspected. The Clearswift SECURE ICAP Gateway acts as an ICAP server, as it responds to requests made by the Barracuda device.

The ICAP Gateway controls that only requests from the configured ICAP clients are served. Thus, the IP address that the Barracuda NextGen Firewall uses to communicate with the Clearswift SECURE ICAP Gateway is required.

Configuration is done in the *ICAP Server Configuration* option under the *System* menu of the Clearswift SECURE ICAP Gateway administration UI.

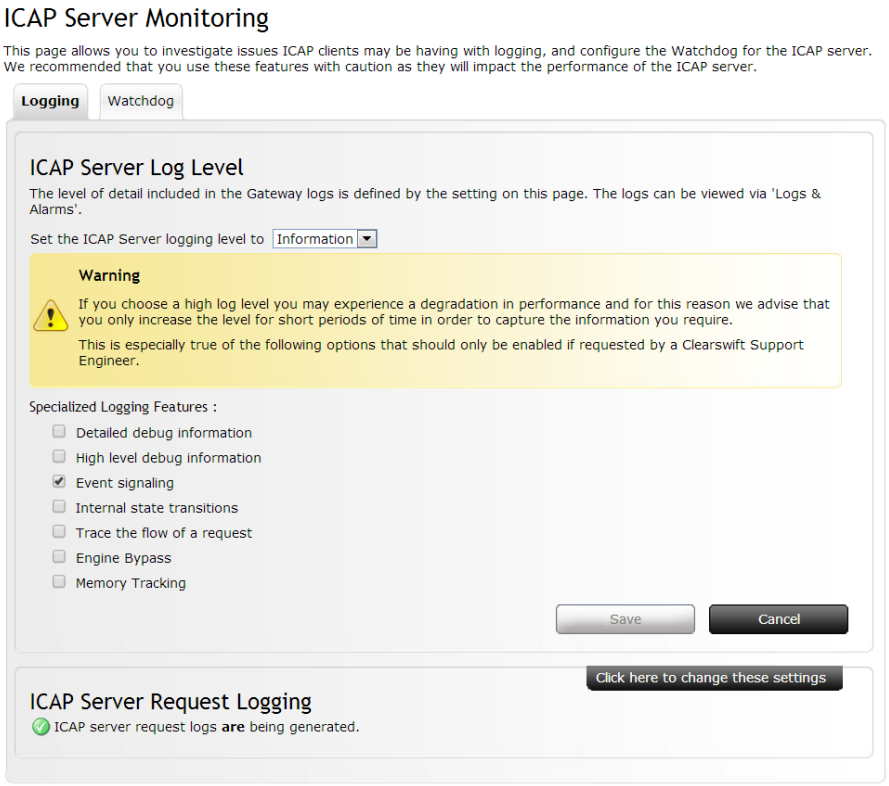


All of the Barracuda devices accessing the ICAP service must be configured in the ICAP Clients area with the IP address they are using to connect to the SECURE ICAP Gateway.

The Barracuda proxy will be receiving requests from users and receive content from servers. Both the requests and the responses can be sent for inspection to the ICAP Gateway. However, each of them is treated in a different manner. In order to identify them individually, different service URLs are provided. These can be configured in the "ICAP Services Configuration" box, including whether message previewing option will be accepted or not.

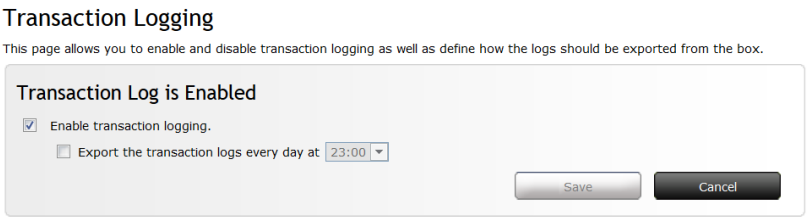
Also, by default the Clearswift ICAP Gateway is configured to listen on the port 1344. This can be modified if required through the configuration page.

Additionally, the Clearswift SECURE ICAP Gateway allows the configuration of the logging level in the "ICAP Server Monitoring" section of the configuration.



It must be noted that high levels of logging can have a negative performance impact on the platform.

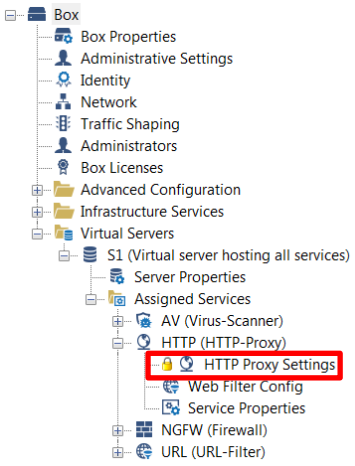
Also, it is important to highlight that these logs show the requests made by the Barracuda Firewall to the SECURE ICAP Gateway. There is also available a log on the transactions done by users under the *Transaction Logging* option of the *ICAP Settings* section under the *System* tab.



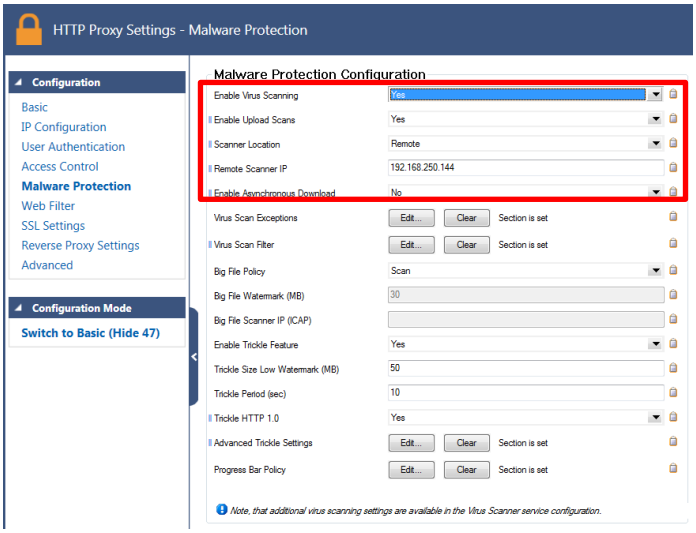
For more information, please refer to the online help of the product, accessible on the left pane of the management UI.

3.3 Barracuda NextGen Firewall configuration

The configuration consists on configuring an external malware inspection device for the on-box HTTP Proxy. The configuration of that service can be found by selecting *Configuration* from the Management UI and then *Configuration Tree*:



Once opened, under the *HTTP (HTTP-Proxy)* node, the *HTTP Proxy Settings* needs to be opened by double-clicking on it. On the left pane, under *Configuration Mode*, select *Switch to Advanced View*. Then, under the *Configuration* option of the left pane, select *Malware protection*:



The settings to set are highlighted in the previous image and are the following ones:

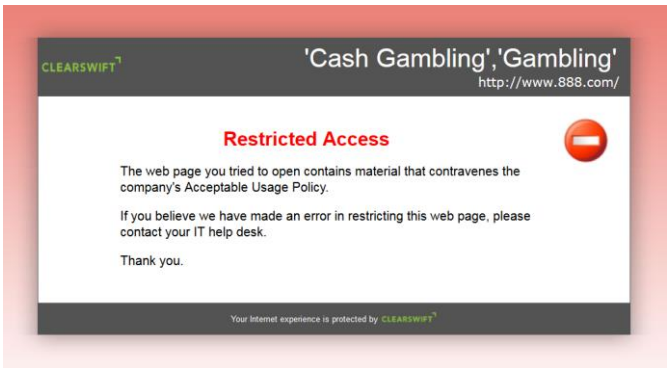
- *Enable Virus Scanning*: Must be set to *Yes*.
- *Enable Upload Scans*: Allows scanning content being uploaded. The recommendation is to enable it by selecting *Yes*.
- *Scanner Location*: Must be set to *Remote*, as otherwise the local antimalware engine is run.
- *Remote Scanner IP*: The IP address of the SECURE ICAP Gateway must be configured for the content to be forwarded to it.
- *Enable Asynchronous Download*: Must be set to No.

To change these settings, please remember to *Lock* access to the UI, and then *Send Changes* and *Activate* them. After following these steps, any request sent by users or response received from the servers will be forwarded to the SECURE ICAP Gateway for inspection.

If HTTPS inspection is enabled in the Barracuda NextGen Firewall, which requires the HTTP Proxy to be configured in Forward explicit mode, the HTTPS content will also be inspected by the SECURE ICAP Gateway.

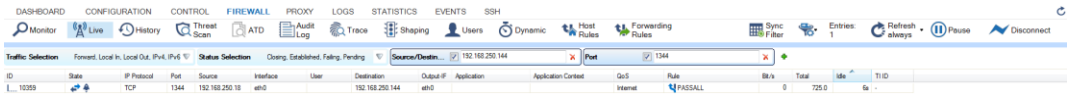
3.4 Testing the configuration

The simplest test to confirm that everything has been configured correctly is to browse to use the proxy of the Barracuda NextGen Firewall.



In case there is a problem with the ICAP server, there will be delays accessing the page.

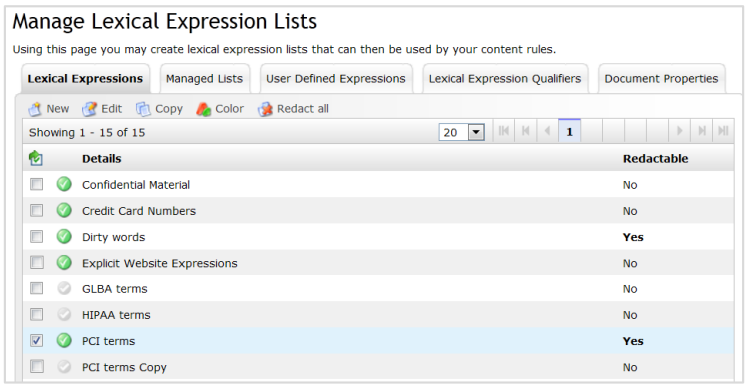
Additionally, the Barracuda NextGen Firewall logs the firewall activity, so by opening the *FIREWALL* tab, a filter can be created with Source/Destination the IP address of the SECURE ICAP Gateway and port 1344:



In order to validate that adaptation is done correctly, it is recommended to configure a test policy in the SECURE ICAP Gateway and check it is applied correctly. The following steps show how to test a redaction policy for PCI related information.

From the SECURE ICAP Gateway Web UI:

1. Navigate to Policy -> Policy References -> Lexical Expressions
2. Select the checkbox for the *PCI Terms* expression list and click on the *Redact All* button, checking that the *Redactable* column now shows *Yes* for the selected expression list



The next step is to create a redaction content rule. From the Clearswift SECURE ICAP Gateway UI:

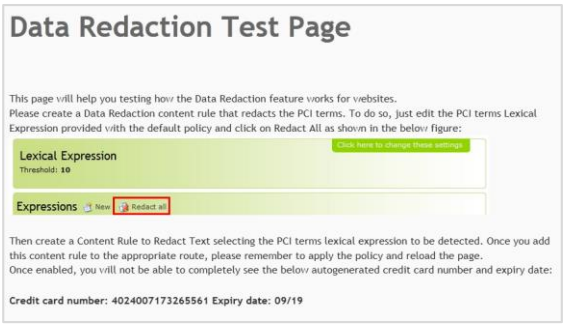
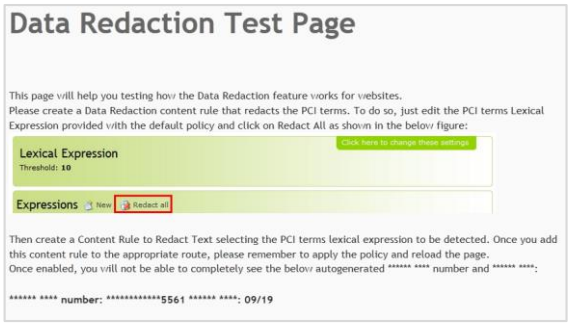
1. Navigate to Policy -> Manage Policy Definition -> Content Rules
2. Click on *New* and select a *Redact Text* type.
3. Set an appropriate name to the content rule in the *Overview* area, e.g. *Redact PCI Terms*
4. Edit the *Lexical Expression* area and select *PCI Terms* from the *Expression list* drop-down, and click on *Save*
5. Modify the Media Types, Size Restriction and Direction To Apply areas if required
6. In the *What To Do?* area modify the settings for the *On Unsuccessful Redaction* and set as primary action to *Block the communication using* and select *Block page for 'Confidential Material'* as the block page. Please save afterwards

The last step is to assign the just created content rule to a policy route. To do so:

1. Navigate to Policy -> Manage Policy Definition -> Web Policy Routes
2. Select the route to edit (e.g. *traffic that does not match another route*) and click on *Edit*
3. In the Unless One Of These Content Rules Triggers area, click on New
4. Select the just created content rule from the pop-up window and click on *Close*
5. Select the content rule from the list and move it up to the appropriate position in the list with the up and down arrows

After doing these changes, the policy needs to be applied for it to take effect.

Browsing to one of the virtual servers where PCI content is published should show the content redacted:

Before	After
	

The above sample page and some additional examples can be found at http://www.clearswift.com/threattests

4 Troubleshooting

4.1 Slow response

There is a continuous communication between the Barracuda NextGen Firewall and the SECURE ICAP Gateway. This connection is very sensitive to delays or network problems. In case of having a slow response, please make sure the connectivity between both devices is flawless, that both are in the same network and that the latency in the communication between both servers is negligible.

4.2 Standard procedure

In order to troubleshoot the communication between both devices, it is recommended to use the Barracuda NextGen Firewall Management UI. The firewall real time view shows how connections are dealt and if there is any policy blocking them. It is a very common mistake to have a rule that blocks the traffic between both components.

To troubleshoot Clearswift SECURE ICAP Gateway it is advisable to allow additional logging in the system to be able to track the activity. This can be done by following the below steps:

1. Navigate to *System -> ICAP Settings -> ICAP Server Monitoring*
2. Enable the *ICAP Server Request Logging* and save
3. Apply policy

In this section, additional detailed logging can be enabled. Please note that enabling a high logging level can impact the performance of the system and is only advisable to do so for short periods of time while troubleshooting is taking place.

The generated logs can be accessed navigating to *System -> Logs & Alarms*. The *ICAP Server Requests* shows a trace of the received requests and responses and the outcome of them.

In the previous example, where the index.html file contained text to be redacted and the virtual server was configured listening at 192.168.50.221, the following log lines were generated:

```
May 11 11:17:54 200:Allowed 2 REQMOD ?
http://192.168.50.221/ar/dr/index.html
May 11 11:17:54 adapt:Modified 6 RESPMOD 200
http://192.168.50.221/ar/dr/index.html
May 11 11:17:54 200:Allowed 1 REQMOD ?
http://192.168.50.221/ar/dr/style.css
May 11 11:17:54 200:Allowed 6 RESPMOD 200
http://192.168.50.221/ar/dr/style.css
```

```
May 11 11:17:54 200:Allowed 1 REQMOD ?
http://192.168.50.221/ar/dr/RedactAll.jpg
May 11 11:17:55 200:Allowed 89 RESPMOD 200
http://192.168.50.221/ar/dr/RedactAll.jpg
```

As it can be seen, the response from the server for index.html was modified, which was caused by the redaction rule in place.

It must be noted that the system watchdog generates periodic requests to http://icap.clearswift.net/test/, so these lines are not related to the traffic generated from the Barracuda system.

5 FAQ – Frequently Asked Questions

Q: Can adaptation be applied only in one direction of the traffic?

A: Yes. The Barracuda NextGen Firewall will always inspect incoming traffic. But it also allows the configuration of inspection on content being uploaded. Unfortunately, it is not possible to do the inspection only on uploaded content.

Q: Can a pool of SECURE ICAP Gateways be used by different Barracuda systems?

A: Yes. The pool of ICAP servers can be defined in different instances of the Barracuda NextGen Firewalls and configured to send the requests or responses for adaptation to the SECURE ICAP Gateways pool. However, the configuration on the Barracuda Malware inspection, only allows the definition of an IP address to connect to. That means that a load balancer should be placed in order to do make requests from one Barracuda NextGen Firewall to several Clearswift SECURE ICAP Gateways.