APPENDIX G

Third Party Integration

This appendix contains the following sections:

Overview

This appendix details the configuration settings for integrating with third party software and hardware. In some cases, Connector is required to provide user or group granularity. For further information about Connector, see the *Connector Administrator Guide*.

When you have configured your third-party system, you should ensure outbound traffic is allowed by connecting to the Cisco Cloud Web Security proxy address using telnet on port 8080.

Tip The easiest way to test that the service is working is to go to http://www.eicar.org/ and attempt to download an Anti-Malware Testfile. This should generate a block message.

BlackBerry Enterprise Server

You can configure your BlackBerry Enterprise Server (BES) to forward traffic to Cisco Cloud Web Security.

Note To connect to internal sites you must use Connector and create exceptions for those sites. In the following instructions the Connector URL should be used in place of the Cisco Cloud Web Security primary proxy URL.

Using the **BlackBerry Manager** create a new proxy mapping for the **BlackBerry MDS Connection Service** with the type **PROXY** and the URL and TCP/IP port of your Cisco Cloud Web Security primary proxy (found in your provisioning email).

Blue Coat

Blue Coat can be configured to enable user names, internal IPs, and domain groups to be sent to Cisco Cloud Web Security without needing to make end-user changes. This can be done either directly using the Blue Coat Authentication and Authorization Agent (BCAAA), or in ICAP mode using Connector.

Prerequisites

- If user granularity is required, for example user name or Active Directory security groups, then BCAAA must be installed on Active Directory.
- To send internal IP address to Cisco Cloud Web Security, Blue Coat must be configured, typically via the command line, to include x-forwarded-for headers.
- If Connector is used, a DNS Host (A) record must be created for the Blue Coat as part of the NTLM realm configuration.
- The Visual Policy Manager must contain a Web Access, Web Authentication, Web Content and Forwarding layer.

Proxying With BCAAA

To configure Blue Coat to proxy using BCAAA installed on the Active Directory:

Step 1 Create a Source Object and an Action Object for each user or group of users you want to forward to Cisco Cloud Web Security and an Action Object with a forwarding list of the Cisco Cloud Web Security proxies.

Step 2 Create an IWA realm with the primary server host and port on which BCAAA is operating with Basic and Kerberos credentials enabled.

Step 3 Add a rule to the Web Access Layer including the Source and Action objects. It must contain Control Request Header Objects with the name `X-Username` and the value `$(cs-user)`and `X-Groups` and `$(cs-auth-groups).`

Step 4 Add a rule to the Web Access Layer including the Source object and an Authentication object for the IWA realm, then install the policy.

If you require user or group granularity, you must ensure the Virtual URL is set to the DNS name of the Blue Coat device.

Tip You can create a Reflect IP Object for each subnet. By assigning a different IP to each subnet the Cisco Cloud Web Security proxy servers can redirect the subnet to a different account.

Proxying With ICAP

To configure Blue Coat to proxy with ICAP using Connector in Enterprise mode:

Step 1 Create a Forwarding Host for each Cisco Cloud Web Security proxy with HTTP and FTP enabled on ports 8080.

Step 2 Create a Forwarding Group containing the forwarding hosts and with load balancing switched off.

Step 3 Set the Action for HTTP and FTP services to Intercept.

Step 4 Create a policy for each of the Forwarding Hosts. Ensure the Source and Destination objects in the Forwarding Layer include the users you want to forward and the service element includes HTTP, HTTPS and FTP. Ensure the Action element in the Web Content Layer is set to Do Not Cache.

Step 5 Create a new ICAP service with the version set to 1.0. Ensure the Service URL is set to `icap://`*`<connector IP address>`*`:1344/connector`. Set the maximum connections to 1500, the connection timeout to 70. Ensure **Notify administrator** and **Virus found page** are not selected. Ensure **Client address** and **Authenticated user** are selected for **request modification**.

Step 6 Create a rule to use the ICAP service. The Web Content Layer must include a Destination object for the users you want to forward. The Action element must be set to Set ICAP Request Service.

Step 7 Configure the Web Authentication Layer to include the Source and Destination objects for the users you want to forward. Ensure the Action is Authenticate, that the correct realms are included and that the Mode is Auto.

Check Point

If you require granularity you must use Connector to connect directly to the Internet, bypassing Check Point. In this configuration Connector should be behind Check Point.

Check Point is not capable of transparently proxying HTTPS traffic. You must enable HTTPS traffic to access the Internet directly, bypassing Cisco Cloud Web Security.

If you are using FloodGate, you must create a rule to prioritize port 8080 traffic over all other services. SmartDefense should be switched off for traffic originating from the Connector IP address.

Note The configuration of the FloodGate and SmartDefense services may be reset if a Check Point firewall restarts.

Transparent HTTP proxying does not require any changes to a user’s browser, providing that the user’s gateway of last resort is the Check Point firewall.

To configure Check Point to transparently proxy HTTP:

Step 1 Create a service with the type Other named http_proxy using Protocol 6.

Step 2 Edit the Advanced Other Service Properties and set the Match to `SRV_REDIRECT(`*`<incoming destination port>`*`,`*`<IP to forward to>`*`,`*`<new destination port>`*. The IP to forward to is the Cisco Cloud Web Security primary proxy (found in your provisioning email).#

Step 3 Ensure Accept Replies, Match for 'Any,' Aggressive Aging, and Synchronize connections on Cluster are enabled.

Note There must be at least one Network Address Translation (NAT) rule in the rule base for this to work. However, the NAT rule does not necessarily have to apply to this connection.

Firebox

When setting up a local area network with a WatchGuard Firebox as a single gateway firewall device, Cisco recommends using Connector and allowing port 8080 traffic to pass through Firebox. In this configuration, both HTTP and HTTPS traffic is sent to Cisco Cloud Web Security, avoiding potential issues with HTTP(S) sites failing due to inconsistencies in source IP addresses. When Firebox is used as a transparent proxy without Connector:

- Cisco Cloud Web Security only processes traffic coming from the external IP address. You will not be able to see detailed report information on user activity or set up detailed user access policies based on Active Directory groups and user names or internal IP addresses.
- You will not be able to use both primary and secondary Cisco Cloud Web Security proxies for failover purposes.

To configure Firebox to allow HTTP(S) traffic:

Step 1 Create a policy for TCP with the Client Port set to ignore and the Port set to 8080.

Step 2 Set the Incoming connections policy to Disabled. It is possible to set the policy to Enabled and Denied but this may cause conflicts if any other inbound port 8080 rules have been configured.

Step 3 Set the Outgoing connection to Enabled and Allowed.

Step 4 In the From box, add the IP range or internal hosts that will be accessing the service. If this applies to your whole trusted network then the predefined trusted group can be used.

Step 5 In the To box, add the IP addresses of your primary and secondary Cisco Cloud Web Security proxies (from your provisioning email). Cisco does not recommend using the default setting of **any**.

It is possible to lock down user's proxy settings when using an Active Directory domain. However, if another domain is being used then it is advisable to lock all other outbound HTTP(S) traffic to prevent users bypassing Cisco Cloud Web Security.

It is likely that HTTP(S) services already exist within your policy that allow direct Internet access. If so, Cisco recommends that these should be changed to Enable and Deny outbound traffic. Making this change will ensure that any traffic that tries to leave the client network on port 80 or 443 will appear in the logs and provides you with information about any user attempting to connect directly to the Internet. There will also be less chance of conflict because all Web traffic will be going via the Cisco Cloud Web Security rule.

Although Firebox does not support transparent proxying, there is an option to set an upstream proxy server for HTTP traffic. To enable transparent proxying:

Step 1 Create a new HTTP service and select Use Caching Proxy Server.

Step 2 Enter the IP address of the Cisco Cloud Web Security primary proxy (from your provisioning email) and set the port to 8080.

Firebox will forward all HTTP traffic to the Cisco Cloud Web Security primary proxy. However, it will not failover to the secondary proxy and HTTPS traffic will not be forwarded. If you require failover support you should use Connector instead. As a work around for HTTPS, a rule can be configured to go out direct.

It is advisable to turn off all of the other features of the HTTP proxy rule in the other tabs. It is possible to create another HTTP rule which can bypass the proxy forward.

ISA Server/Forefront TMG

Cisco recommends using ISA Server/Forefront TMG in ICAP mode with Connector. For a full description of how to configure ISA Server/Forefront TMG, refer to the *Connector Administrator Guide*.

NetCache

Connector can be integrated with NetCache to provide user and group granularity. NetCache must be configured for NTLM authentication against an Active Directory domain before proceeding.

To configure NetCache to proxy with ICAP using Connector in Enterprise mode:

Step 1 Create a New Parent hierarchy using the Cisco Cloud Web Security primary proxy (from your provisioning email) as the Host Name. HTTP and HTTPS must be set to 8080. There must be no entry for RTSP, MMS, or ICP. Object caching must be switched off. The monitor status for TCP must be set to Pass through the client user name and password.

Step 2 Enable ICAP 1.0 and switch off Generate the X-Client-IP ICAP Header from the X-Forwaded-For-HTTP Header.

Step 3 Create a New Service Farm for Connector. In the Vectoring Point, set the REQMOD_PRECACHE Order to 1.

Step 4 Enable the Service Farm and set Round Robin Based Load Balancing with Bypass on Failure. Select Weak Consistency and ensure Ibw is switched off. Configure the Services to be `icap://`*`<IP to forward to>`*`:1344/connector` where the IP to forward to is the Cisco Cloud Web Security primary proxy.

Step 5 To enable granularity, set the Access Control Lists for HTTP(S) to `icap (`*`<service farm name>`*`) any`.

You can add exceptions to the service by creating a new Forwarding Rule for HTTP(S) where the Phrase Equals the IP address you wish to bypass Cisco Cloud Web Security and the Distribution Method is set to Direct.

When you enable your first Forwarding Rule, the default rules will be switched off. It is not possible to enable them again so a Forwarding Rule must be created for HTTP(S) to send normal traffic to Cisco Cloud Web Security. The rule must not include any conditions and the Distribution Method must be Parent Cluster.

Note The Connector ISTag response to an ICAP server is fixed by default, but with NetCache you may need to set it to randomized by adding `icap.generate.random.istag=true` to Connector's agent.properties file.

NetScreen

Juniper Networks NetScreen can be configured to enable user names, internal IPs, and domain groups to be sent to Cisco Cloud Web Security. In addition to configuring the firewall, you must also change the Domain/LAN proxy settings. Global or local browser settings must include the proxy server IP/Domain name supplied and the HTTP port 8080. Policy amendments are based on port 8080 being set explicitly in the user's browser.

To configure NetScreen to forward to Cisco Cloud Web Security:

Step 1 Create a custom service for TCP on port 8080. Set the Source Port range to 0 to 65535.

Step 2 If Internet users will be on the trust interface, create a firewall policy from the trust/private interface to the untrust/public interface. Alternatively, substitute any other outbound facing interface. This policy should be as high in the list as possible. The rule must be tied down from the LAN object or range that will access the Internet through the Cisco Cloud Web Security proxy to the IP address/domain name of the remote proxy. The rule must be one way and will be set to 'allow'.

Step 3 Add the Cisco Cloud Web Security proxy IP addresses (from your provisioning email). The netmask must be 255.255.255.255 and the Zone must be the untrust zone. The configuration of NAT is dependent on policy. If policy-based NAT is in use then source NAT must be selected in the specific rule. This is not required if general NAT is in use.

Step 4 Create a policy for outbound access on port 8080 from the trust zone to the untrust zone. The Source Address must be Address Book Entry Inter-Lan and the Destination Address should be Address Book Entry (Multiple). Enter the addresses for which you want to enable outbound access. Set Service to (Multiple) and enter the addresses again. Set the Application to None, the Action to Permit, VPN to None, L2TP to None and enable logging.

Note NetScreen firewalls have an HTTP proxy rule with antivirus scanning and Web filtering. If Internet users are using the Cisco Cloud Web Security proxies exclusively, then it is recommended that this function is switched off.

When you have configured your internal Internet users to send traffic to Cisco Cloud Web Security, it is advisable to lock down HTTP(S) traffic being sent directly to the Internet so that users cannot bypass the newly configured service.

To do this, remove HTTP(S) access from the previously existing rule. You should then have a rule base where Any to Any access is switched off, the previously existing rule is applied to DNS traffic and HTTP(S) and FTP traffic goes to Cisco Cloud Web Security.

Any other rules allowing outbound HTTP(S) must be switched off or set to deny, or HTTP(S) removed from the specific rule. It is also advisable to create a policy from the trusted to the untrust zone that denies all HTTP traffic on port 80. The source will be the restricted LAN object or range, the destination will be Any. The action will be drop/deny.

It is useful to have Logging switched on. This will allow you to audit the rule to make sure that all users are going through the Scanning proxy rule and not hitting the drop rule which should be at the bottom of the rule base.

Juniper ScreenOS 5.4 or later supports transparent proxying, or “NAT destination.” Transparent proxying enables traffic to be forwarded to Cisco Cloud Web Security with any client configuration. Because SSL has built in defense against ‘man-in-the-middle’ attacks, traffic redirection is not supported for HTTPS.

Cisco Cloud Web Security use the public IP address as one means of authenticating traffic. If you have dynamically assigned public IP addresses (for example, most DSL and broadband connections), it is possible to leverage NetScreen support for DDNS registration to authenticate new IP addresses.

To configure NetScreen to enable transparent proxying:

Step 1 Create an authentication key in ScanCenter. See [REF].

Step 2 Create a new policy for traffic from the trust zone to the untrust zone. Set the Source and Destination addresses to Address Book Entry (ANY). Set the Service and Application to HTTP. Ensure the WEB Filtering options are switched off. Set the Antivirus Profile, Tunnel VPN and L2TP to None. In the advanced policy settings, switch off Source Translation and enable Destination Translation. Select Translate to IP and enter the address of the Cisco Cloud Web Security primary proxy (from your provisioning email). Set the Map to Port to 8080 and switch off Authentication.

Note The rule to redirect HTTP traffic to Cisco Cloud Web Security must occur before a rule that allows it to go directly to the Internet.

Step 3 If internal subnets or intranet addresses are on the WAN side (un trust zone), then you must create a new policy to allow traffic to those networks to bypass filtering (go direct). The rule to allow local intranet traffic must occur before the rule that redirects traffic to Cisco Cloud Web Security.

Step 4 Create a DDNS entry for dynamic IP registration. Set the Server Type to dyndns, the Server Name to ddns.scansafe.net. Set the Refresh Interval and Minimum Update Interval to 1. Alternatively, if the IP address of the WAN interface is the public address supplied by your ISP, use the default settings. Enable Clear Text. Enter a User Name and set the Password to the authentication key you generated earlier. Set Bind to Interface to None. Alternatively, if the IP address of the WAN interface is the public address supplied by your ISP, select ethernet0/0. Set the Host Name to the domain name registered for your service, for example yourcompany.com. Enable the DDNS Client. Registration may take a minute or so, The Last-response column in the DDNS Entries Table will be ‘good’ if registration was successful.

The advantage of this configuration is that you do not need to change any proxy settings within the user’s browser. Providing the user’s gateway of last resort is the SonicWALL firewall, it will be able to transparently proxy HTTP connections to Cisco Cloud Web Security.

SonicWALL

If you require granularity you must use Connector to connect directly to the Internet, bypassing SonicWALL. In this configuration Connector should be behind SonicWALL

To configure SonicWALL without using Connector:

Step 1 In the **Web Proxy** page, enter the name or IP address of the Cisco Cloud Web Security primary proxy (found in your provisioning email) in the **Proxy Web Server** box.

Step 2 Enter `8080` in the **Proxy Web Server Port** box.

Step 3 Select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.

Step 4 If you have clients configured on the perimeter network, select the **Forward Client Requests to Proxy Server** check box and apply your changes.

The advantage of this configuration is that you do not need to change any proxy settings within the user's browser. Providing the user's gateway of last resort is the SonicWALL firewall, it will be able to transparently proxy HTTP connections to Cisco Cloud Web Security.

Note You must enable direct access to the Internet for HTTPS traffic without sending it to Cisco Cloud Web Security. SonicWALL is not capable of transparent proxying HTTPS traffic.

Squid

You can forward web requests to Cisco Cloud Web Security using the open source Squid firewall. The official Squid website (http://www.squid-cache.org/) recommends building Squid from the source. However, a prebuilt package is available in the standard Red Hat Enterprise Linux and CentOS repositories. Alternatively, Cisco provides a prebuilt RPM package for use with WCCP. A prebuilt Windows binary is available from Acme Consulting (http://squid.acmeconsulting.it/download/dl-squid.html) which sponsors the Windows port.

Prerequisites

Before installing the RPM provided by Cisco you must install the perl-URI package (1.30-4 or later):

```
yum install -y perl-URI
```

Add the following lines to the /etc/security/limits.conf file:

```
*   hard   nofile  32768
*   soft   nofile  32768
```

Edit the maximum number of connections in the /etc/sysctl.conf file then the settings with the sysctil -p command:

```
net.ipv4.netfileter.ip_conntrack_max = 65536
```

Enter the following commands to apply the required firewall rules:

```
/sbin/iptables -t nat -F /sbin/iptables -F /sbin/iptables -I INPUT 1 -p tcp --dport 80
-j ACCEPT
/sbin/iptables -I INPUT 1 -p tcp --dport 3128 -j ACCEPT
/sbin/iptables -t nat -A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT --to-ports
3128
/etc/rc.d/init.d/iptables save
```

Configuration

There are a number of lines in the squid.conf file which are customer-specific. The items you must modify are identified in bold in the examples below.

Modify the following lines to match the proxies defined in your provisioning email (where xxx.xxx.xxx.111 and xxx.xxx.xxx.222 are the primary and secondary Cisco Cloud Web Security proxy respectively):

```
cache_peer xxx.xxx.xxx.111 parent 8080 0 no-query no- digest proxy only weight=10
login=*:password default cache_peer xxx.xxx.xxx.222 parent 8080 0 no-query no- digest
proxy only weight=1 login=*:password default
```

Modify the following line to match your internal network range:

```
acl local_netowrk src 192.168.10.0/24
```

Comment out the lines starting wccp2 in the WCCP Configuration section.

To force Squid to use only the Cisco Cloud Web Security proxies enter the following line:

```
never_direct allow all
```