Secure Web Appliance

Reverse Proxy

Table of Contents

List of Figures

1. Introduction

1.1. About CYAN Secure Web Appliance

The all-in-one appliance hardware solution developed by CYAN Networks is an optimal customized platform that makes the deployment of Secure Web very easy. The Appliance includes a complete pre-installed Secure Web, as well as a Web Admin Interface used for the configuration of the entire machine. The product can easily be integrated into the already existing infrastructures. The configuration and other operating tasks are done with your favorite web browser, thus no knowledge about the integrated operating system is required.

1.2. About Reverse Proxy

Reverse Proxy takes requests from the outside network, performs filtering and if the data passes all of the filtering rules, it resends the data on the inside network to predefined destination. The source from the outside network may be completely unaware of the fact that the communication goes through a Reverse Proxy.

1.3. About this Manual

This manual explains concept and configuration of the Reverse Proxy feature present in the CYAN Appliance solution. The reader is expected to have basic knowledge of the Secure Web platform, is able to access and work with the Web Admin Interface and has successful performed the initial setup steps of Secure Web, as outlined in the Getting Started Guides.

This manual is to be used with a CYAN Appliance with Secure Web version 2.1 and above.

For additional documentation, please see our document repository on http://www.cyan-networks.com/documentation

1.3.1. Document Conventions

Indicates a potentially risky situation, leaving the appliance in an unusable state.

Indicates a potentially risky situation, causing misfunction of the solutions.

Indicates information that is substantial for successfully configuring and using the product.

Provides helpful information for the process of configuring and using the product.

Provides additional information about typical scenarios and best practices.

2. Overview

Most of the Secure Web functionality can be described as a forward proxy. It means that Secure Web takes HTTP and other requests from different clients from the inside company network and then acts on behalf of the clients, performs filtering of these requests and then usually places the received data on the outside network.

Reverse Proxy works similarly but with a stream of data in the opposite direction. Reverse Proxy takes requests from the outside network, performs filtering and if the data passes all of the filtering rules, it resends the data on the inside network to predefined destination. The source from the outside network may be completely unaware of the fact that the communication goes through a Reverse Proxy.

The Reverse Proxy behavior may sound like a firewall. The difference is in the network layer where the filtering occurs. While firewall usually performs filtering based on IP addresses and ports, Reverse Proxy may filter requests according to the actual data content (and also anything else that a firewall could do).

3. Setting up Reverse Proxy

This section and the following subsections will cover how to configure Reverse Proxy on the CYAN Appliance.

First you have to login to the Web Admin Interface. It can be accessed by pointing your browser to the appliance IP address:

```
https://<appliance-ip>:9992/ (for example, https://192.168.1.1:9992/)
```

All of the Reverse Proxy settings can be found in menu *Services / Reverse Proxy*. The configuration starts in the sub menu *Configuration*. The position in the menu structure can be seen in the following figure:

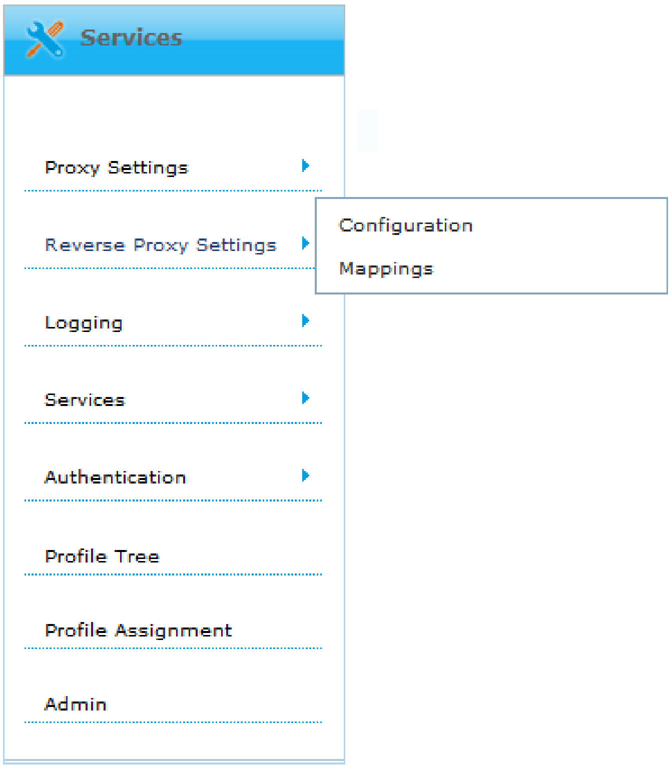
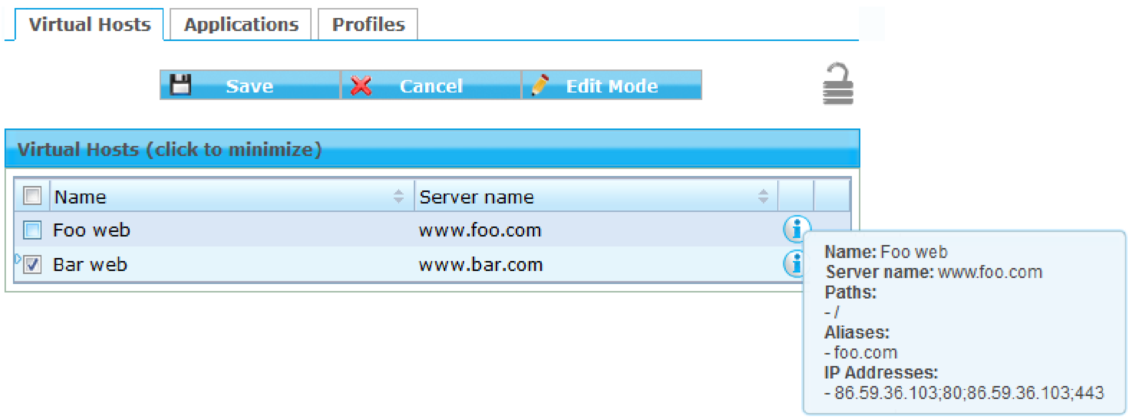


Figure 3.1. Reverse Proxy settings in the menu structure

3.1. Virtual Hosts setup

The first step of Reverse Proxy configuration is setting up Virtual Hosts. It can be done in menu *Services / Reverse Proxy Settings / Configuration / Virtual Hosts*. You can see an example of this screen in the following figure:



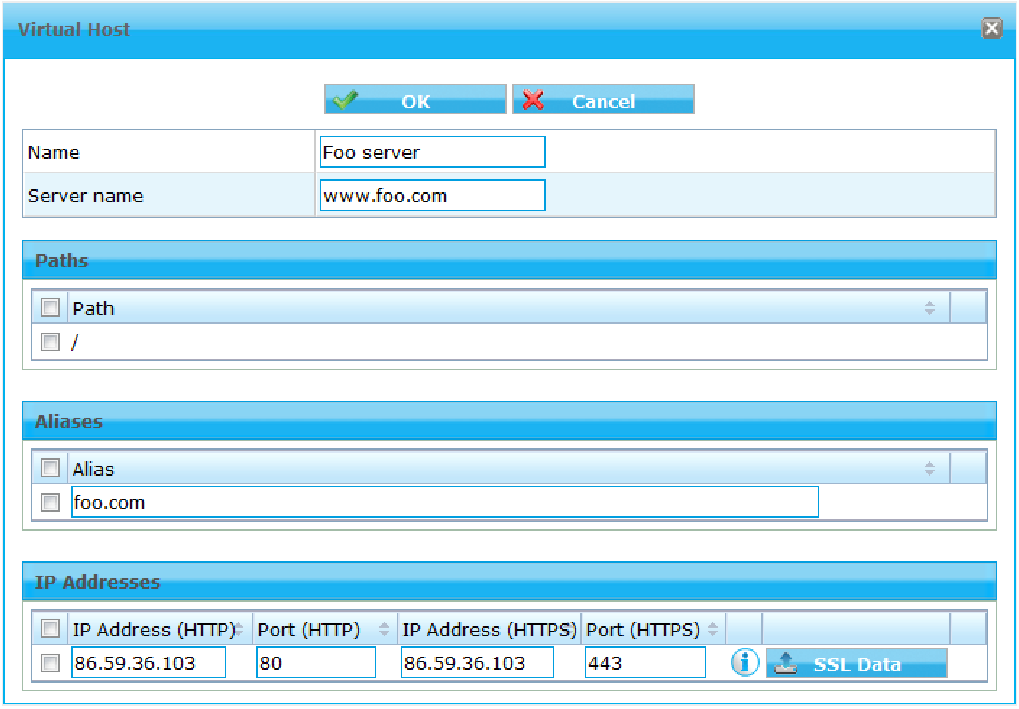
☐	Name	Server name
☐	Foo web	www.foo.com
☑	Bar web	www.bar.com

Name: Foo web
Server name: www.foo.com
Paths:
- /
Aliases:
- foo.com
IP Addresses:
- 86.59.36.103;80;86.59.36.103;443

Figure 3.2. Virtual Hosts tab example

In the screen, you can see two example Virtual Hosts already configured (each serves for a different fictitious web server). You can quickly see details of the configuration by moving mouse cursor on the blue round "i" icon. New Virtual Host records can be created from the context menu accessed by right clicking the list. Using this context menu can be the records also deleted. Editing a record can be done quickly by simply double clicking the desired record.

Let us have a look at the Virtual Host configuration in more detail. Creating or editing a record pops up a new window with all the Virtual Host options (see Figure 3.3, “Virtual Host configuration example”). The configuration may be familiar to you from configuration of virtual hosts in Apache web servers configuration and follows similar semantics.



Name	Foo server
Server name	www.foo.com

☐	Path
☐	/

☐	Alias
☐	foo.com

☐	IP Address (HTTP)	Port (HTTP)	IP Address (HTTPS)	Port (HTTPS)
☐	86.59.36.103	80	86.59.36.103	443

Figure 3.3. Virtual Host configuration example

Meaning of the options is following:

- **Name**: Identification of the Virtual Host. It can be any string.
- **Server name**: Primary URL that the Virtual Host should be serving.

- **Paths**: Limits the Virtual Host to some specific paths followed after the *Server name* or *Alias*. Default value for new records is "/".

  It is also possible to have two (or more) Virtual Hosts one domain. For example for *www.foo.com* one for *www.foo.com/* and second for *www.foo.com/private*. If more Virtual Hosts a present in the Virtual Hosts list for a common domain, the first one matched will be used. Therefore, the more specific should be in the list before the less specific ones (in this example *www.foo.com/private* before *www.foo.com/*).

- **Aliases**: Aliases (alternative server names) for this Virtual Host. Most common usage server name without *www* prefix. This alias is added automatically when you put in the *Server name* field URL with the *www* prefix.

- **IP Addresses**: List of expected destination IP addresses and ports of incoming HTTP(S) requests. Examples of what IP address put in this field will be shown later in Chapter 4, *Configuration examples*.

  It is also possible to join records in this list with an SSL certificate and a key. To do so, click the SSL Data and choose the appropriate option (see Figure 3.4, "SSL Data button"). To see whether there is any SSL Data assigned already or not move your mouse button on the "i" icon.

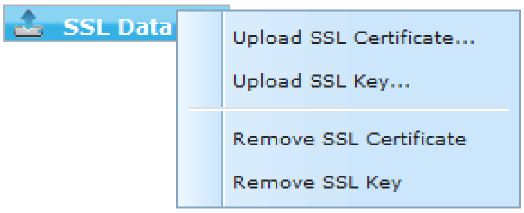
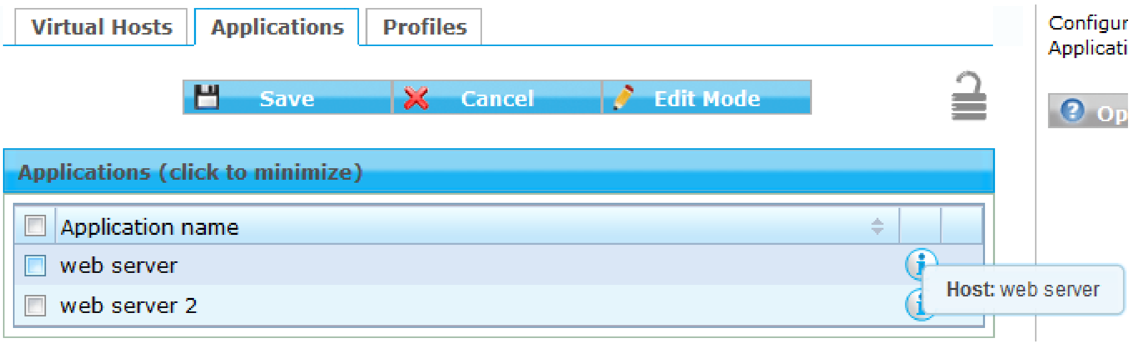


Figure 3.4. SSL Data button

Do not forget to save all changes done in the Virtual Hosts tab by the *Save* button before leaving from this tab. Any changes not previously saved will be otherwise discarded.

3.2. Applications setup

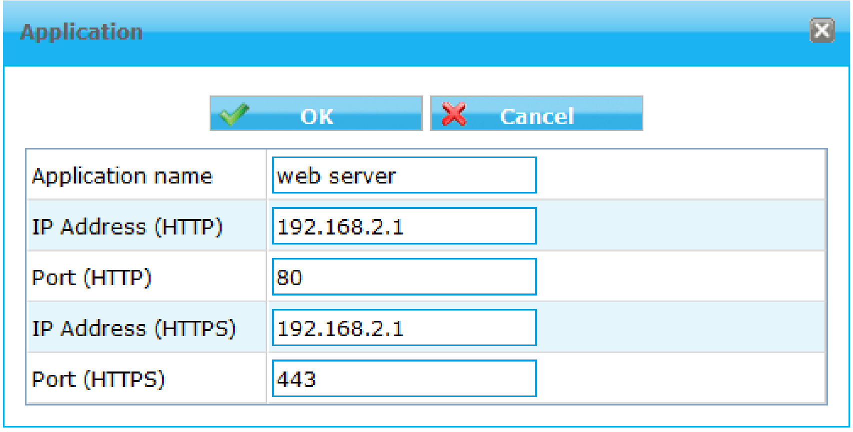
Applications setup can be done in menu *Services / Reverse Proxy Settings / Configuration / Applications*. You can see an example of this screen in the following figure:



□	Application name
□	web server
□	web server 2

Figure 3.5. Applications tab example

In the screen, you can see two example Applications already configured (each represents a different web server). All of the records can be manipulated the same way as shown in Section 3.1, “Virtual Hosts setup”. Creating or editing a record pops up a new window with all the Application options (see Figure 3.6, “Application configuration example”).



Application name	web server
IP Address (HTTP)	192.168.2.1
Port (HTTP)	80
IP Address (HTTPS)	192.168.2.1
Port (HTTPS)	443

Figure 3.6. Application configuration example

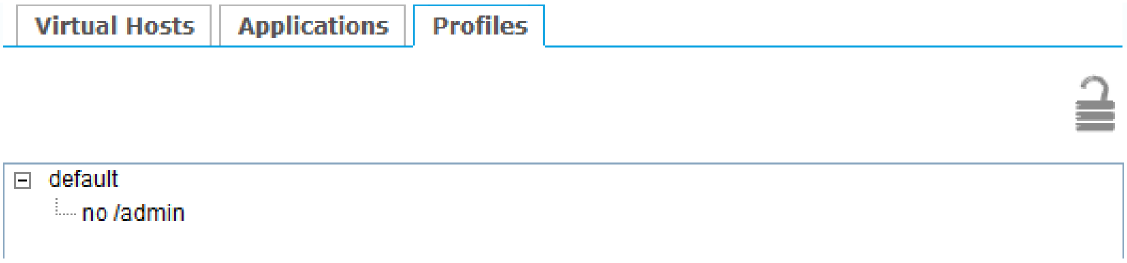
Meaning of the options is following:

- **Application name**: Identification of the Application. It can be any string.
- **IP Address**: IP address of the target where should be all the HTTP(S) requests sent.
- **Port**: TCP/UDP port of the target on which should be all the HTTP(S) requests sent.

⚠ Do not forget to save all changes done in the Applications tab by the *Save* button before leaving from this tab. Any changes not previously saved will be otherwise discarded.

3.3. Profiles setup

Profiles setup can be done in menu _Services / Reverse Proxy Settings / Configuration / Profiles. You can see an example of this screen in the following figure:

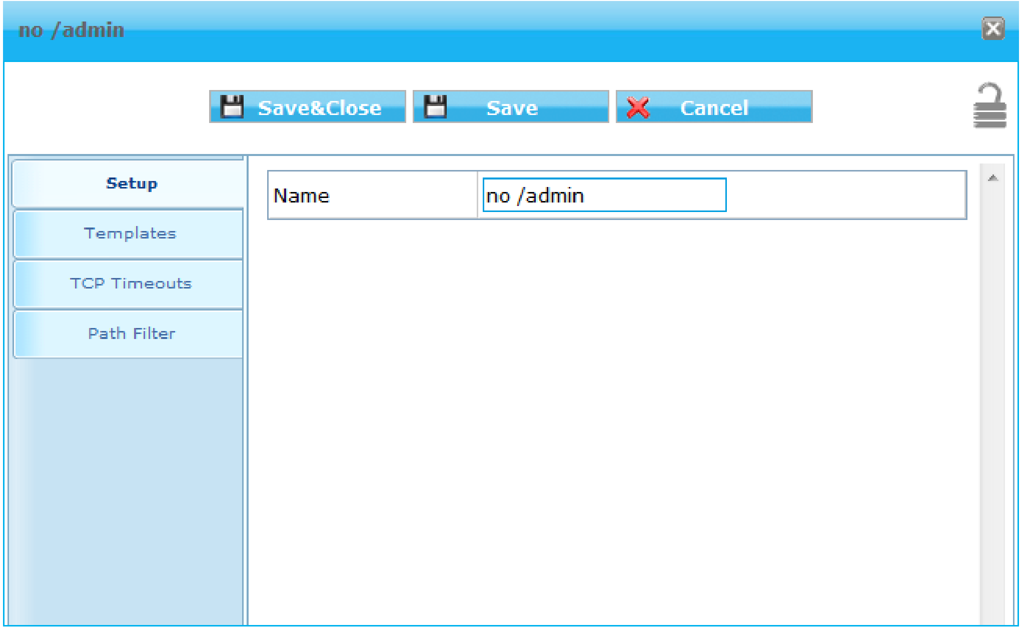


default
no /admin

Figure 3.7. Profiles tab example

In the screen, you can see two example Profiles already configured. All of the records can be manipulated in a similar way to the one shown in Section 3.1, “Virtual Hosts setup”. Additionally, records can be dragged and dropped on each other to change the parent/child hierarchy. Creating or editing a record pops up a new window with all the Profiles options (see Figure 3.8, “Profiles configuration example - Setup tab”).

In the *Setup* tab, you can change the Profile name under the option *Name*.

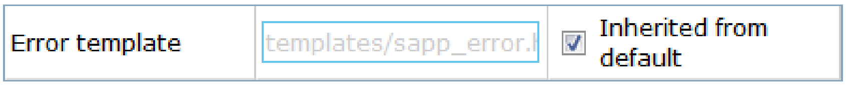


Name	no /admin

Figure 3.8. Profiles configuration example - Setup tab

In the Templates tab (see Figure 3.9, “Profiles configuration example - Templates tab”), it is possible to change the default error page displayed to user when a HTTP(S) request is denied by the Path Filter. The templates themselves are physically located in directory */opt/cyan/sweb/templates/* on the Appliance. This option allows to specify other location of a different template or letting be the template inherited from parent Profile.

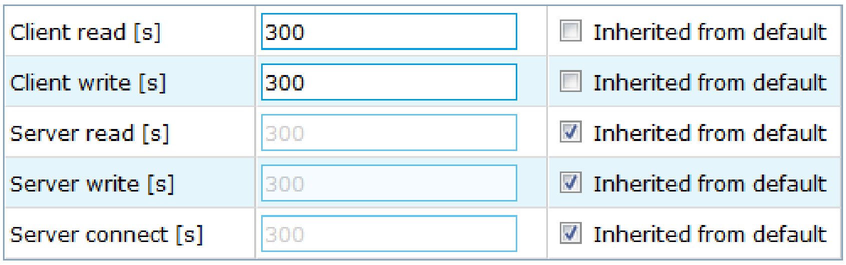
Path Filter option is explained later in this section.



Error template	templates/sapp_error.l	☑ Inherited from default

Figure 3.9. Profiles configuration example - Templates tab

In the TCP Timeouts tab, it is possible to change various TCP Timeout values (or let them be inherited from parent Profile). See the following example:



Client read [s]	300	□ Inherited from default
Client write [s]	300	□ Inherited from default
Server read [s]	300	☑ Inherited from default
Server write [s]	300	☑ Inherited from default
Server connect [s]	300	☑ Inherited from default

Figure 3.10. Profiles configuration example - TCP Timeouts tab

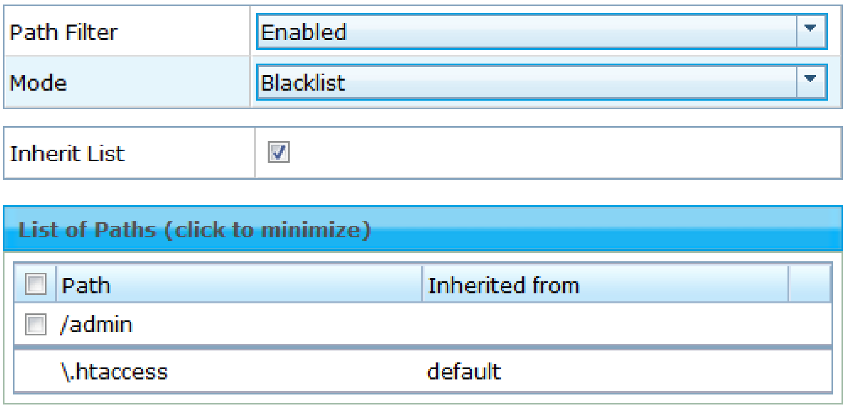
Probably most interesting part of the Profile settings is the Path Filter tab. It allows you to restrict access to certain web pages by examining the URL in HTTP(S) requests and applying black/white listing rules.

Meaning of the options is following:

- **Path Filter**: Set if the Path Filter should be Enabled, Disabled or the state should be inherited from the parent Profile.

- **Mode**:
  - **Blacklist**: Everything is allowed by default and *List of Paths* specifies what all should be denied.
  - **Whitelist**: Everything is denied by default and *List of Paths* specifies what all should be allowed.
  - **Inherited**: Type of the list should be inherited from the parent profile.
- **Inherit List**: If enabled, the *List of Paths* will contain all records from all parent profiles.
- **List of Paths**: List of paths that should be denied/allowed (depending on the *Mode* option). Path is a regular expression. New records can be added from the context menu.

An example of Path Filter configuration can be seen in the following figure:



Path Filter	Enabled
Mode	Blacklist
Inherit List	☑

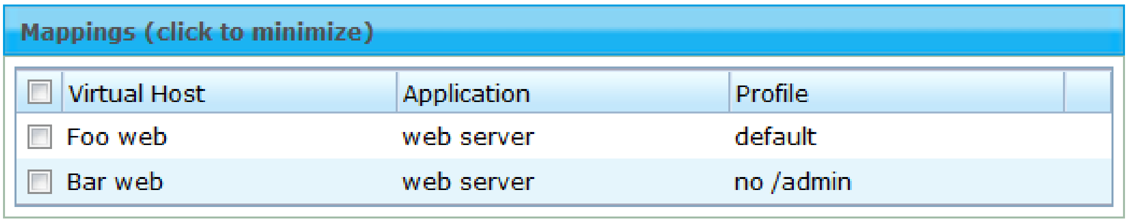
List of Paths (click to minimize)

□	Path	Inherited from
□	/admin	
	\.htaccess	default

Figure 3.11. Profiles configuration example - Path Filter tab

3.4. Mappings configuration

Mappings tie all the configuration of Virtual Hosts, Application and Profiles discussed in previous sections together. Mappings can be configured in menu *Services / Reverse Proxy Settings / Mappings*. You can see an example of the Mappings list in the following figure:



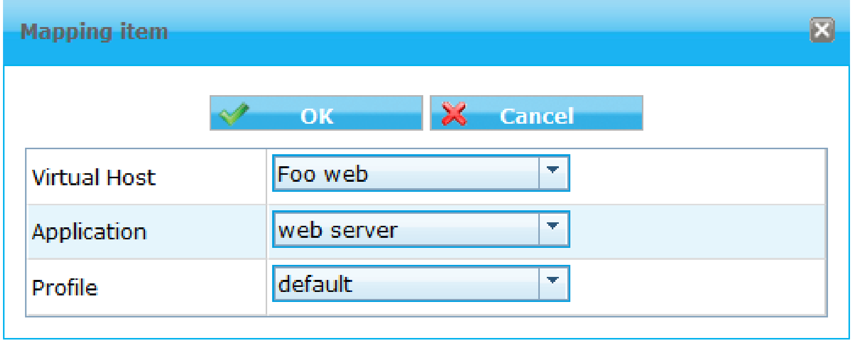
Mappings (click to minimize)

□	Virtual Host	Application	Profile
□	Foo web	web server	default
□	Bar web	web server	no /admin

Figure 3.12. Mappings list example

Any Mapping item determines what requests the Reverse Proxy accepts (Virtual Host), with what machine/server it communicates (Application) and how the communication should be restricted (Profile).

New Mapping item can be created from the context menu accessed by right clicking the list. Using this context menu can be the records also moved, edited or deleted. Incidentally, editing of a record can be done quickly by simply double clicking the desired record and any record can be also easily rearranged by dragging and dropping. The following figure shows details of one Mapping item:



Virtual Host	Foo web
Application	web server
Profile	default

Figure 3.13. Mapping item example

It is possible to create just one Mapping item per Virtual Host.

4. Configuration examples

In this section will be covered some simple configuration examples using the Reverse Proxy feature. These configurations do not have to reflect any real configuration but they should help you to better understand how or why to use the Reverse Proxy. Please read all the examples because each of them contains some helpful tips for the configuration that is not present in the others.

4.1. Existing web server in a public network

Let us start with the simplest configuration possible. A web server connected directly to the internet with a public IP address. This server probably already has some kind of firewall by itself. See the following figure:

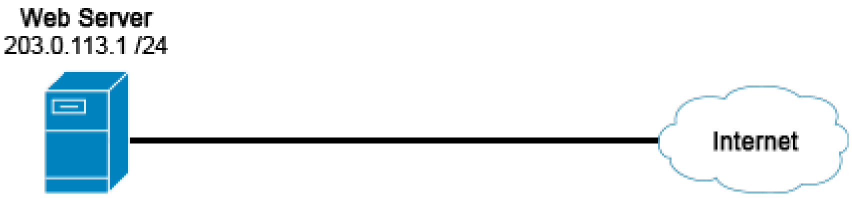


Figure 4.1. Simple example without the Appliance

Now we would like to use the Appliances Reverse Proxy to filter the requests coming on the server from the Internet. We can simply put the server inside a private network and put the Appliance between the server and the Internet. See the following figure:

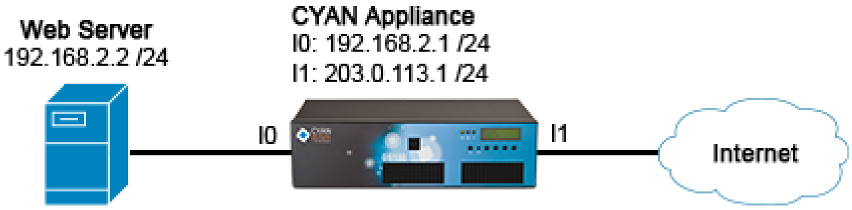


Figure 4.2. Simple example with the Appliance

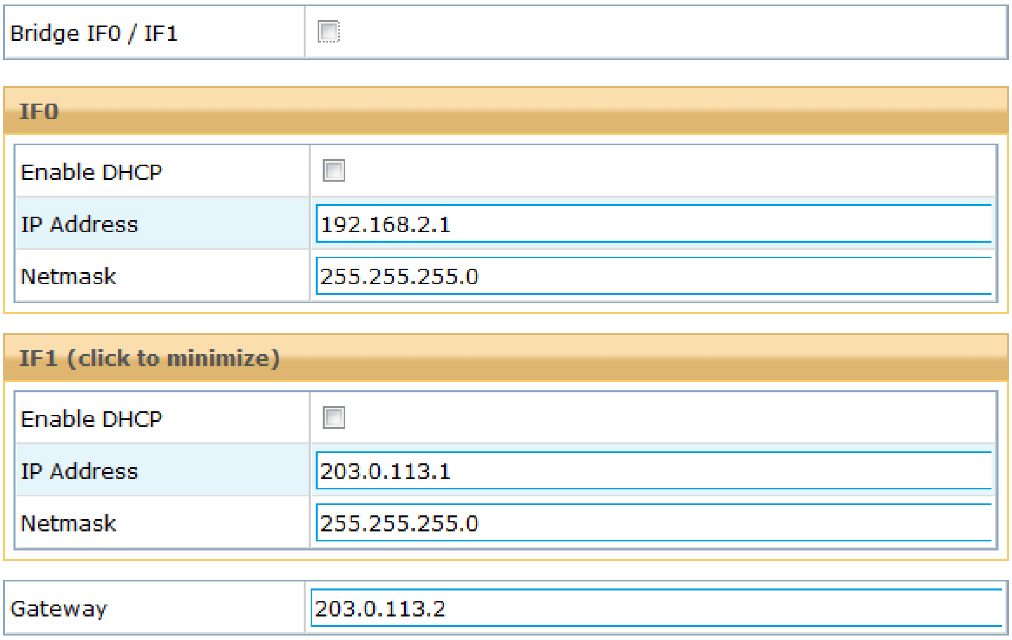
Now we have to change the IP addresses. The Appliance has two interfaces:

- **I1:** - This one should be connected to the "public" network (in this example to the Internet). For this port being accessible from the Internet, it needs to have the server's public IP address assigned.

- **I0: -** This one should be connected to the "private" network (in this example to the server). We can create a simple private network 192.168.2.0/24 and assign one address from this address range to the port I0 and another to the server.

For configuration of the IP address on the server please refer to a documentation for the operating system running on this server. It is also necessary to set the IP address of the I0 interface as a default gateway on the server.

IP addresses on the Appliances ports should be configured manually in menu *Appliances / Network / Interfaces*. It is important to turn off the *Bridge IF0 / IF1* option and disable DHCP on both interfaces. See an example in the following figure:



Bridge IF0 / IF1	□

IF0

Enable DHCP	□
IP Address	192.168.2.1
Netmask	255.255.255.0

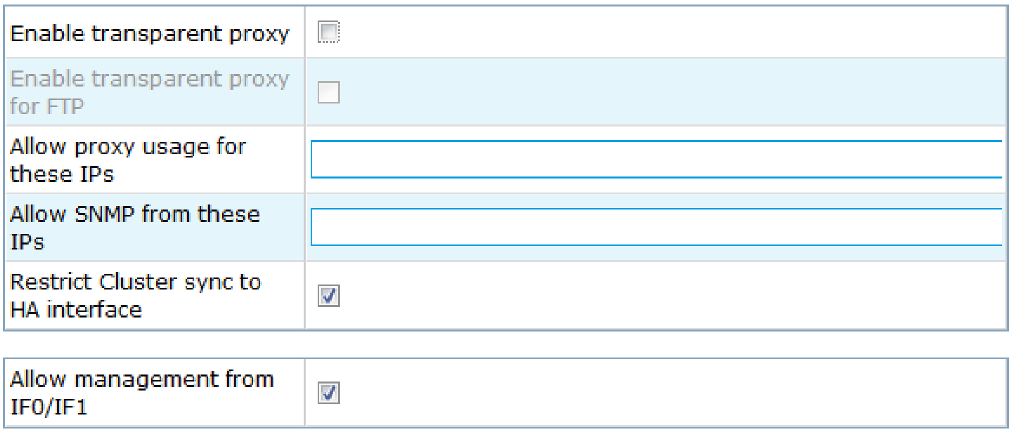
IF1 (click to minimize)

Enable DHCP	□
IP Address	203.0.113.1
Netmask	255.255.255.0

Gateway	203.0.113.2

Figure 4.3. Example of interfaces configuration

It is also necessary to change the Firewall settings of the Appliance in menu *Appliances / Network / Firewall* and uncheck the *Enable transparent proxy* option. Not doing so will cause dysfunction of the Reverse Proxy feature. See the following example:



Enable transparent proxy	□
Enable transparent proxy for FTP	□
Allow proxy usage for these IPs	
Allow SNMP from these IPs	
Restrict Cluster sync to HA interface	☑

Allow management from IF0/IF1	☑

Figure 4.4. Example of Firewall configuration

In the Firewall settings in menu *Appliances / Network / Firewall* is also a good idea to uncheck the *Allow management from IF0/IF1* option. When this option is checked the appliance management is accessible in this configuration to anyone from the Internet. It is better to use for the configuration a special management interface (if your Appliance has one) or direct HW access to the Appliance.

Before disabling this option please make sure you have other way of accessing the Appliance than just on ports I0 or I1.

Now that we have done the configuration from the "hardware" point of view, let us move to the Reverse Proxy setup itself. The details of the configuration of Virtual Hosts, Applications, Profiles and Mappings were explained previously in Chapter 3, *Setting up Reverse Proxy* and its subsections.

Virtual Hosts (Section 3.1, “Virtual Hosts setup”) - add one virtual host with the following values:

- **Name:** any identifier, for example *example.com*.
- **Server name:** The domain of the web server. Let us assume that this server provides web pages for the domain www.example.com. So we put *www.example.com*.
- **Paths:** We can leave the default */*.
- **Aliases:** At this point *example.com* should have been already added automatically. It is ok to leave it that way.
- **IP Addresses:** *203.0.113.1* / *80* / *203.0.113.1* / *443* (HTTP IP / HTTP port / HTTPS IP / HTTPS port). We can also add the SSL data if needed.

Applications (Section 3.2, “Applications setup”) - add one application with the following values:

- **Application name:** any identifier, for example *web server*.
- **IP Address (HTTP):** *192.168.2.2*
- **Port (HTTP):** *80*
- **IP Address (HTTPS):** *192.168.2.2*
- **Port (HTTPS):** *80*

Profiles (Section 3.3, “Profiles setup”) - we can use the default one or add a new one with the following values:

- **Name:** any identifier, for example *no restrictions*.
- **Path filter:** *Disabled*
- For the rest we can leave the default values.

Mappings (Section 3.4, “Mappings configuration”) - we have to add one mapping with the following values:

- **Virtual Host:** *example.com*
- **Application:** *web server*
- **Profile:** *no restrictions*

That is all. Now if have done everything correctly and applied the configuration with the *Apply* button, the Reverse Proxy should be running.

4.2. Existing web server in a private network

In this example, we have our web server already in a private network, maybe behind some kind of router with a firewall (see Figure 4.5, “Example of a private network behind a router”) or in a demilitarized zone (DMZ, see Figure 4.6, “Example of a demilitarized zone”) and we would like to use the Reverse Proxy.

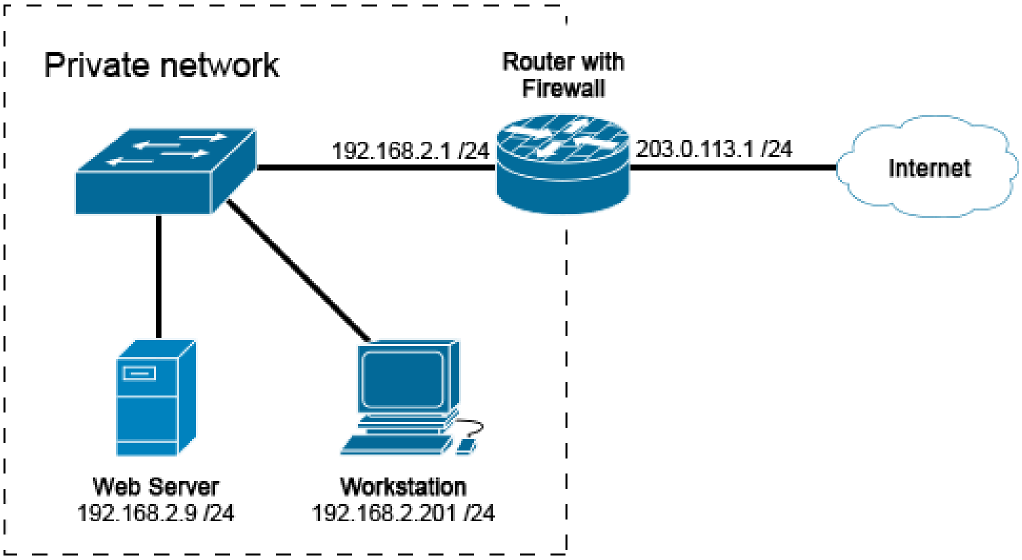


Figure 4.5. Example of a private network behind a router

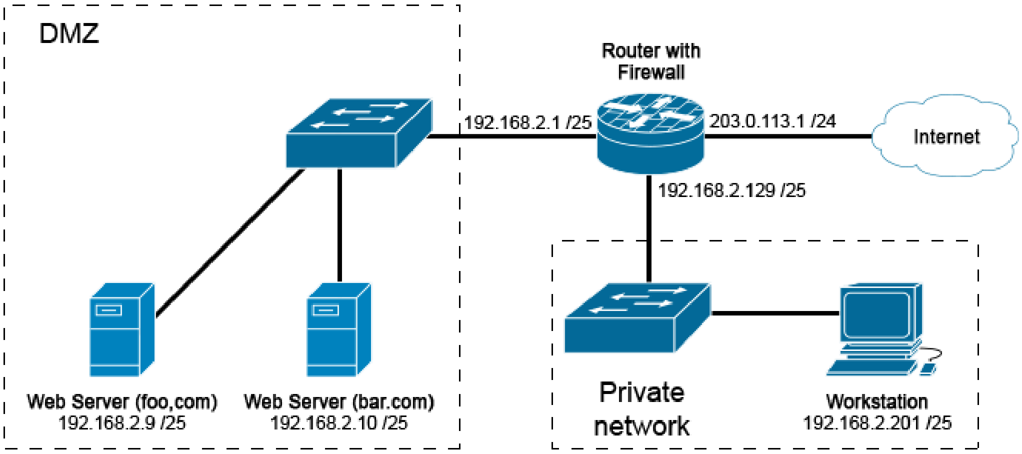


Figure 4.6. Example of a demilitarized zone

In the first example, if we have just one server we could use similar approach as we have used previously in Section 4.1, “Existing web server in a public network”, and just put the Appliance between the server and the switch. Or maybe we could attach the Appliance directly to the router and then a another switch or the server directly to the Appliance. There is many possibilities and the choice will depend on your needs and possibilities.

In the second example, we already have a DMZ setup. Now in here the DMZ has a private IP address scheme (because the router maybe performs NAT). But all the devices may as well have public IP addresses. Now we can again put the Appliance right behind the router (see Figure 4.7, “Example of a demilitarized zone with the Appliance connected In-line”) and make the In-line connection.

However, this will not be practical if we will have other devices in the DMZ that do not need to use the reverse proxy (for example an FTP server). However, we can also do the Out-of-line connection (see Figure 4.8, “Example of a demilitarized zone with the Appliance connected Out-of-line”). Now the servers do not need any reconfiguration at all. You can simply point your DNS records to the IP address of the Appliances port I1 or reroute the traffic to the Appliance instead of servers.

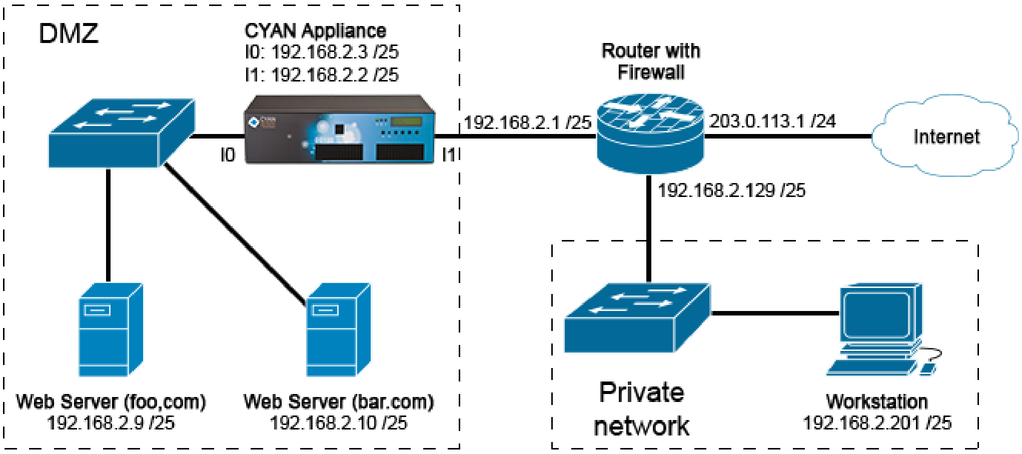


Figure 4.7. Example of a demilitarized zone with the Appliance connected In-line

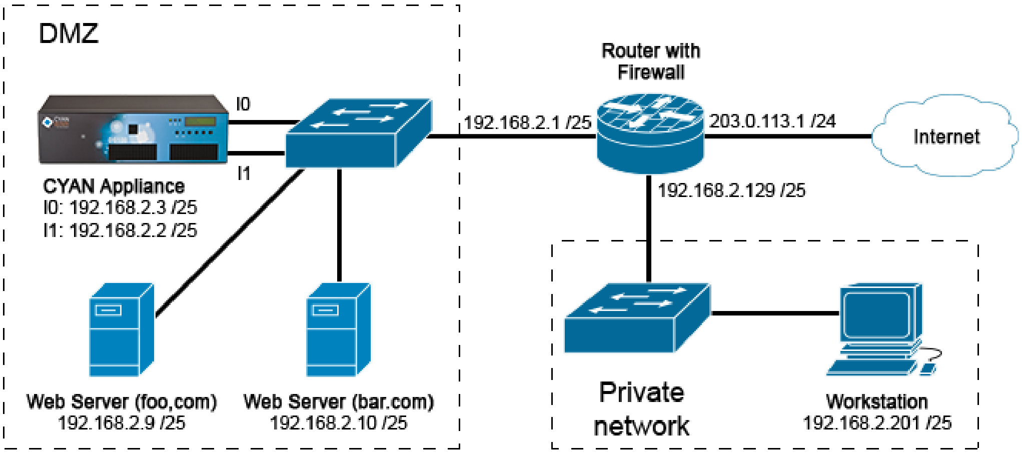


Figure 4.8. Example of a demilitarized zone with the Appliance connected Out-of-line

Appendix A. Contact data

A.1. How to contact our sales department

Tel.:	+43 (1) 33933-0
Email:	sales@cyan-networks.com

A.2. How to contact our support department

Tel.:	+43 (1) 33933-333
Email:	support@cyan-networks.com

A.2.1. Getting Support

In case you should have any technical problems, or questions and would like to get support from our team, we kindly ask you to provide us with the following information:

- Description of your question or problem
- The version information of the product:
  - The version information of Secure Web can be found after logging into the Web Admin Interface in the top part of the screen:

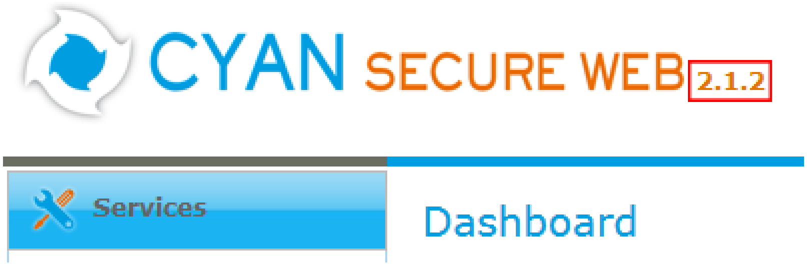


Figure A.1. Version information of the Secure Web

  - The version information of the Reporting System can be found after login in the top part of the screen of the Web Admin Interface:

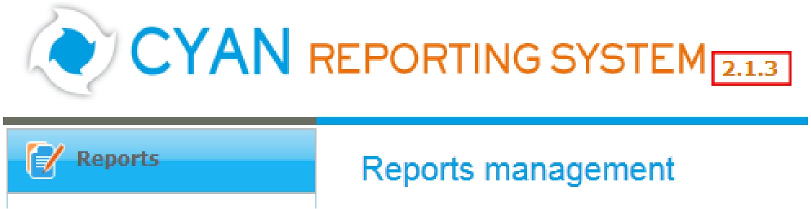


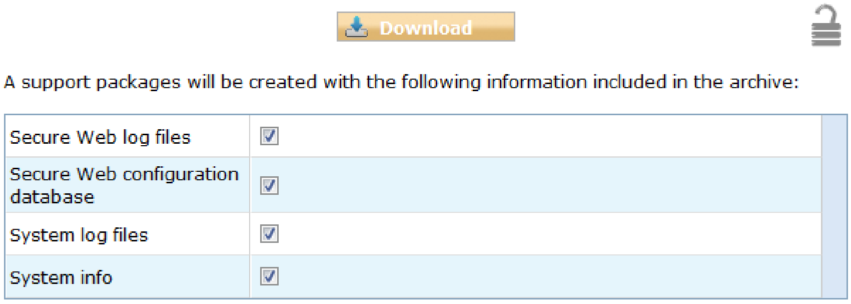
Figure A.2. Version information of the Reporting System

  - All the information contained in the screen found in menu *Services / Services / Overview*
- In the case authentication is activated, provide us with the method in place (via Windows Agent, via Linux Agent, etc.)
- The deployment method of the Appliance (Out-of-line, In-Line, DMZ)
- The operation mode of the Appliance (dedicated mode, transparent mode)

- Information about the environment (proxy cascades that are used, firewalls and gateways involved in the infrastructure that are of relevance to the Appliance)

The appliance interface provides the possibility to create a support package that includes the configuration and log files of the system. This package can help us to track down the issue easier and faster. Please attach this package to your e-mail.

In order to create a support pack, navigate to menu *Appliances / Maintenance / Support* and click on the *Download* button. You may select the files you want to provide to our support team and then download a package, which we kindly ask you to send to our support email address.



A support packages will be created with the following information included in the archive:

Secure Web log files	☑
Secure Web configuration database	☑
System log files	☑
System info	☑

Figure A.3. Support Package

Further documentation about the product as well as technical white papers that describe certain use cases can be found in our documentation repository on our homepage:

http://www.cyan-networks.com/documentation