Secure Web Appliance

Getting Started

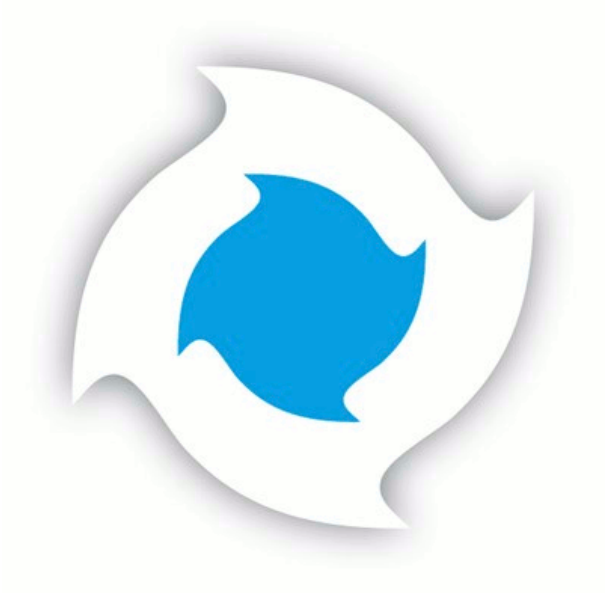

Table of Contents

List of Figures

List of Tables

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 this Manual

This manual explains basic concepts and the first steps for installing and configuring of the CYAN Appliance solution. The reader is expected to have basic computer network knowledge and be familiar with the usage of SSH (PuTTY) for troubleshooting. There is no knowledge of the Secure Web platform necessary prior reading this document.

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

1.2.1. 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. The Parts of the Appliance

The DS100 Appliance package contains the following parts:

- the desktop machine
- a power cord
- a power supply
- a 1 GB SD memory card

The RS 400, 6000, 8000 and 8000-X Appliance packages contain the following parts:

- the rack mountable machine
- a power cord
- an SD memory card

Figure 2.1. Appliance parts

3. The Appliance

The following pictures show the rear view of the Appliance models and the numbering of the ethernet ports:

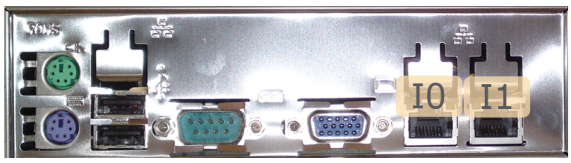

Figure 3.1. Rear view of the model DS100

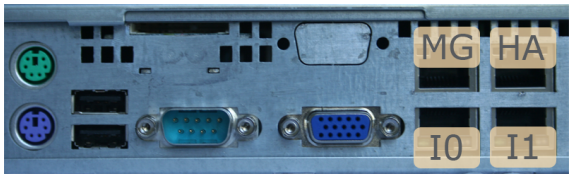

Figure 3.2. Rear view of the RS400 and RS6000 models

Figure 3.3. Rear view of the model DS1 (legacy model)

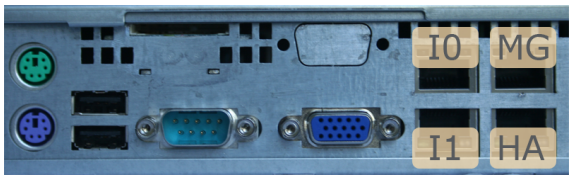

Figure 3.4. Rear view of the RS4 and RS6 models (legacy model)

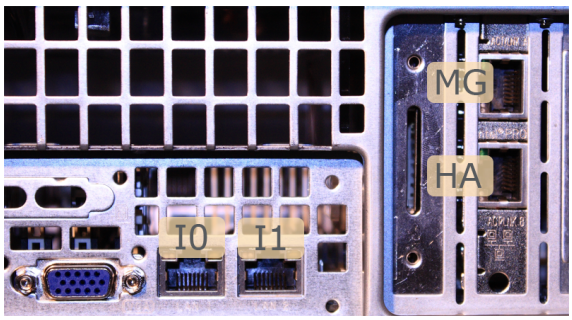

Figure 3.5. Rear view of the RS8 model (legacy model)

Each ethernet port has a specific usage:

- Port I0 is the proxy interface that takes up the client requests
- Port I1 is used for bridging and in dual-homed deployments for the outgoing proxy requests
- Port MG is defined as the management port

- Port HA is used to connect two CYAN Appliances for operating in high-availability mode

Ports MG and HA are not available on DS100 model, but MG port can be configured on it instead of one of the Ix ports.

The representation of the ethernet ports on the embedded Linux operating system is following: I0 = eth0, I1 = eth1, MG = eth2, HA = eth3

The following picture shows the front view of an Appliance in factory mode:

Figure 3.6. Front view of the Appliance

The front LCD of the Appliance shows the current network status of the machine.

The display switches between two screens and shows the following information:

- BR: the IP address assigned to the ethernet bridge (ports I0 and I1, not available on DS100 model)
- MG: the IP address assigned to the management port (MG, not available on DS100 model)
- HA: the current status of the machine in a high-availability environment. A machine that is not a member of a cluster will show “passive+worker”.
- SV: the IP address assigned as the Service IP.

In default configuration the Appliance tries to retrieve an IP address via DHCP on the bridged (BR) interface. If unsuccessful, <undefined> will be displayed in the BR line. The management interface MG is pre-configured with a static IP of 192.168.1.1 and a network mask of 255.255.255.0.

Immediately after connecting one of the bridged ports (ports 1 or 2) to the network, the bridge needs to learn about the network. It can take up to one minute until the DHCP request is issued and an IP address is assigned.

The four control buttons right next to the power button are deactivated in the current version of the appliance.

4. Appliance Deployment

There are numerous ways in which the Appliance can be deployed in the network, the basic concepts being: out-of-line, in-line and in the demilitarized zone (DMZ).

4.1. Out-of-line Deployment

The following diagram illustrates the out-of-line deployment:

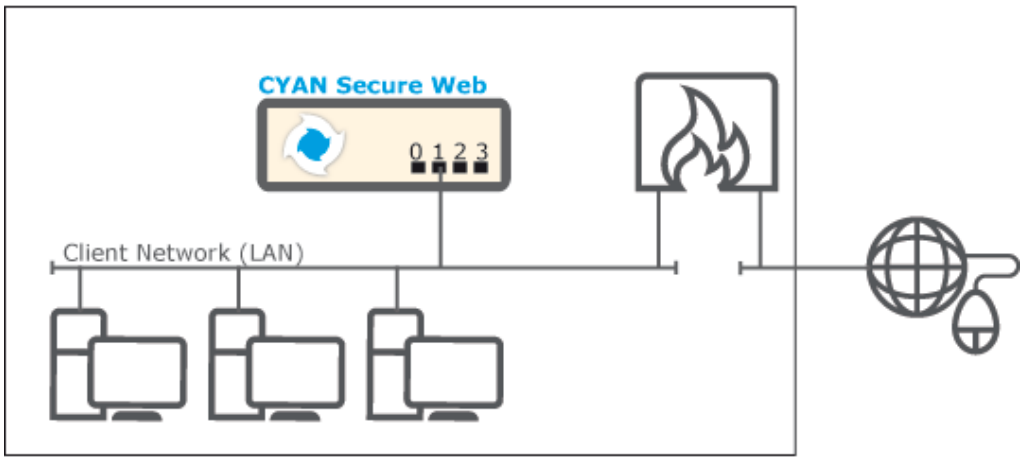

Figure 4.1. Out-of-line deployment

In the out-of-line deployment the Appliance resides on the same physical network as the clients. The clients must not necessarily use the Appliance for their Internet access. However, in order to ensure security the firewall must be configured to disallow all direct traffic from the client to the Internet. To utilize the Appliance either all clients are explicitly configured to use the Appliance, or a rule on the firewall utilizes the Appliance into transparent mode applying port forwarding rules.

To deploy the Appliance out-of-line, one of the ethernet ports I0 or I1 must be connected to the switch that builds your local network.

4.2. In-line Deployment

The following diagram illustrates the in-line deployment:

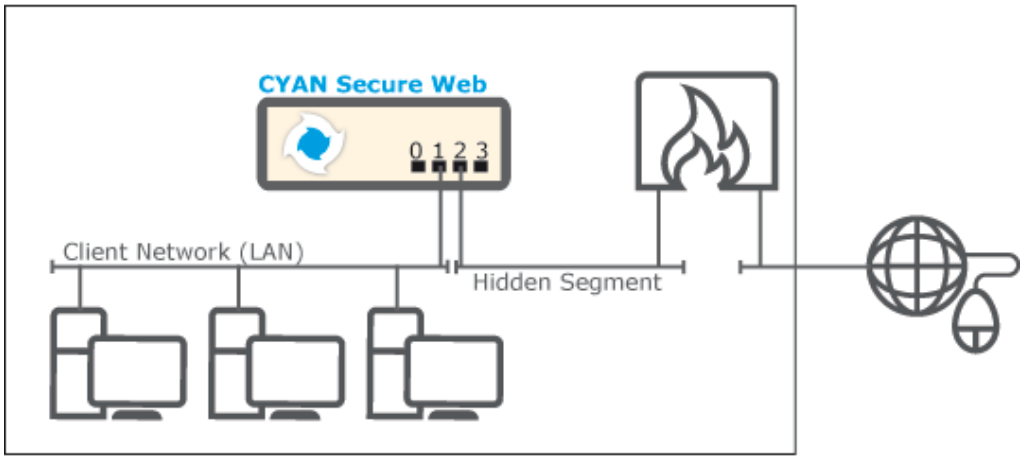

Figure 4.2. In-line deployment

In the in-line deployment the network will be physically split into two segments: the segment where all the clients reside and the segment that connects the Appliance with the firewall / gateway.

To deploy the Appliance in-line, connect the ethernet port I0 of the Appliance to the switch that builds your local network. Your firewall / gateway must be disconnected from this switch and directly connected with a cable to the ethernet port I1.

In case you connect the DS100 Appliance with a direct cable to your firewall / gateway, you need to use a cross-over network cable! The other models have 1 GB interfaces and they can swap the lines in the cable automatically.

4.3. DMZ Deployment

The following diagram illustrates the deployment in a DMZ:

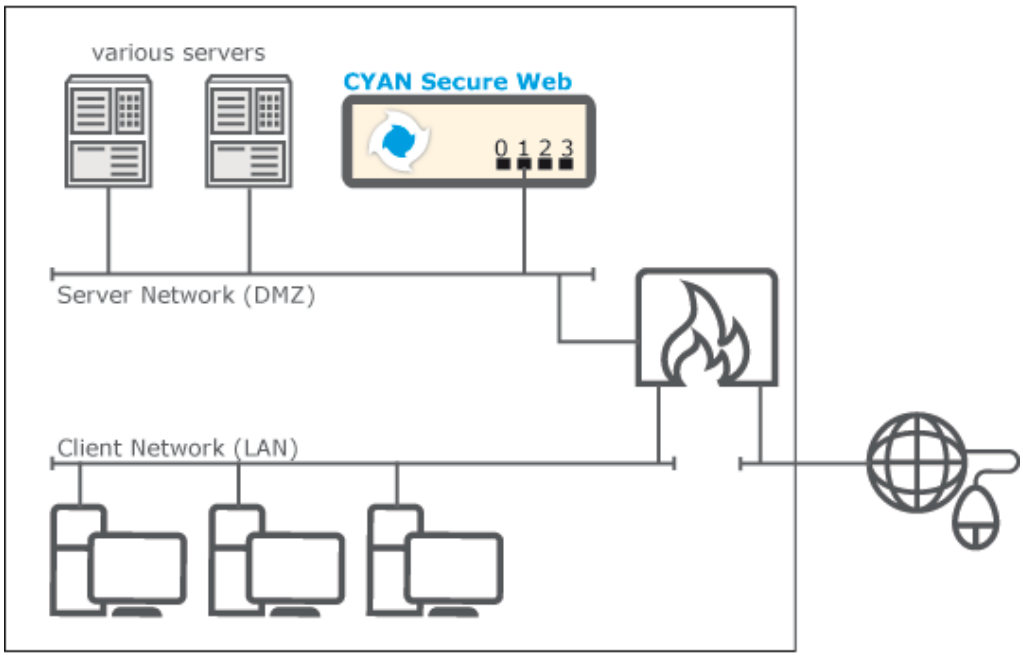

Figure 4.3. DMZ deployment

In the DMZ deployment, the Appliance resides in part of the network that is protected by the firewall from both the extranet and the intranet. In the case that a DMZ is established already, this is the preferred mode, especially if authentication shall be used and the authentication server is on this network.

To deploy the Appliance in the DMZ, one of the ethernet ports I0 or I1 must be connected to the switch that builds your demilitarized zone.

If your Appliance model is not DS100, in any of the main three basic modes, the management of the machine can be restricted to a separated management network. In order to secure the management access, connect the management port to the management network and follow the steps described in Section 6.7, “Restricting Administration to the Management Port”.

5. Proxy Modes

"Proxy Mode" refers to the way how clients “see” the Appliance. One can differentiate between two main modes: non-transparent and transparent mode.

Non-transparent (classic proxy) mode means that the client’s application (e.g. your web browser) must be aware of the existence of the Appliance, i.e. the client must be explicitly configured to use the Appliance in order to establish connections to the Internet.

On the other hand, in **transparent** mode, the client’s application does not know about the existence of the Appliance. Generally all traffic on TCP port 80 (HTTP) is redirected by a networks element (router, firewall, the CYAN Appliance) to the Appliance, i.e. the Appliance is “injected” transparently into the network traffic.

Using each of these two modes has different consequences:

- **non-transparent mode**: as described above, each client’s application needs to be configured to use the Appliance which implies some additional administrative effort. Furthermore, in order to be able to enforce the use of this security and policy gateway, another network element (router, firewall) must ensure by blocking that no direct traffic from a client passes to the Internet. This is a typical configuration option suitable for most of the deployments.

- **transparent mode**: this mode requires the Appliance to be either deployed as an ethernet bridge or to configure port forwarding rules on your router or firewall device. Please refer to the documentation of your router or firewall to find out about the necessary configuration steps. You will most probably want to redirect all traffic that “goes to” the TCP destination port 80, which is the common port for HTTP servers. However, you may also want to redirect the ports 3126 and 8080, which are commonly used by proxy servers. This way you shall prevent the use of external (possibly anonymous) proxies. In this mode you can the user authentication be based just on IP addresses.

- **mix of both modes**: it is possible to combine both approaches. If a *transparent mode* is used it is still possible to use the *non-transparent mode* approach for some clients to, because the port of the Appliance has still assigned an IP address to which can be requests send.

In transparent mode, the Appliance cannot support authentication based on the user. It also cannot support protocols that are bypassing the proxy like native ICQ and equivalent.

Be careful when creating the redirect rule on your network device. Make sure that the traffic from the Appliance itself do not get redirected too, otherwise it will start to loop between the firewall and the Appliance, resulting in a failure of one or both devices.

The following diagram gives an overview of the proxy modes in the deployments and the consequences involved:

Deployment	Non-Transparent mode	Transparent mode	Notes
Out-of-line	ok	Firewall	Port forwarding by the firewall required. Non-trivial rules!
In-line	ok	ok	Single point of failure. Not supported: HA

Deployment	Non-Transparent mode	Transparent mode	Notes
DMZ	ok	Firewall	Port forwarding by the firewall required.

Table 5.1. Proxy mode implications

6. Installation of the Appliance

All administrative tasks can be carried out by using your favourite web browser. In order to get the access to the Web Admin Interface, an IP address of your local network which is accessible by your client PC must be assigned to the Appliance.

In case of the factory settings, the appliance will retrieve a dynamic IP address via DHCP. You can find the IP address on the front panel display (as seen in Figure 3.6, “Front view of the Appliance”).

In case you will not get any IP address assigned by DHCP, you may connect your client PC to the management interface where a dedicated IP address is assigned (more in Section 6.1.2, “Connecting to the Management Port”).

Once you have logged into the Web Admin Interface, you will find the *"Appliances"* menu in the left sidebar. This menu provides all the options and actions for Appliances. (more in Section 6.2, “Opening the Administration Interface”).

6.1. Connecting to the Network

The Appliance has four network ports. The first time you setup the Appliance, you will most probably choose to connect the proxy port I0 to your local network.

In case you have a separated management network, we recommend to use the management port MG.

Make sure that your company firewall allows the access to the Internet for the Appliance. The ports that need to be granted are:

Port	Protocol	Name
53	TCP, UDP	DNS
80	TCP	HTTP
443	TCP	HTTPS

6.1.1. Connecting to the Appliance Port

By default the Web Admin Interface is available on all Appliance ports (I0, I1) as well as on the management port (MG).

After connecting the port I0 to your local network, the Appliance will try to retrieve a dynamic IP address using DHCP. The ports I0 and I1 are bridged (BR). During the IP address retrieval, the LCD will show "BR: <undefined>". After the IP address has been successfully retrived, the display will change and the address will be shown accordingly.

If you do not have a DHCP server on your network, you may continue with Section 6.1.2, “Connecting to the Management Port” and configure the IP address for the proxy ports manually.

6.1.2. Connecting to the Management Port

On the management interface port of the Appliance (MG) a static IP address is assigned. The factory default is: `192.168.1.1` with a netmask of `255.255.255.0`. In order to connect to this IP address, you will have to setup your client PC with an IP address and network mask for this network range (for example `192.168.1.2/255.255.255.0`) and physically attach your client PC to this network port.

Users of the legacy Appliance model DS1 will have to apply a cross-over cable in case that the client PC is attached directly to the management network port, without any network switch in between.

6.2. Opening the Administration Interface

Point your browser to the address assigned via DHCP or the management IP (192.168.1.1), as the case may be.

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

The welcome screen allows you to either access the Web Admin Interface of the Secure Web or the Reporting System.

Figure 6.1. Welcome screen

Click on *"Login"* next to *"CYAN Secure Web"* to navigate to the Web Admin Interface.

When connecting for the first time to the Web Admin Interface, you will be prompted to set up the administrative account. In this case enter a Username and a Password of your choice.

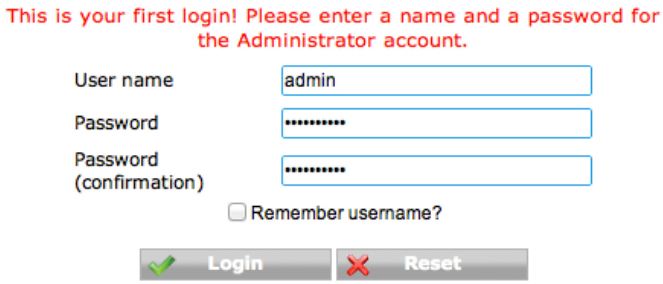

Figure 6.2. First login

This user account will be the first administrator account, put into the *Super Administrator* group and is the only account allowed to create other administrative accounts.

It is extremely important not to forget the *Super Administrator* password. While for *Administrator* accounts can be the password changed by the *Super Administrator* at any time, there is no quick and easy password recovery procedure for the *Super Administrator* account itself. If this password is lost, it is necessary to connect a CR-Rom drive over USB, boot up a Linux distribution, mount the file system and set a new password, or alternatively send the whole Appliance back to Cyan Networks for repair.

On Secure Web Appliances, an additional console account *csupport* will be enabled with the same password. The Appliance can be accessed via SSH protocol using this account (for example for maintenance purposes). For more information see Section A.1.1, “Access via SSH”.

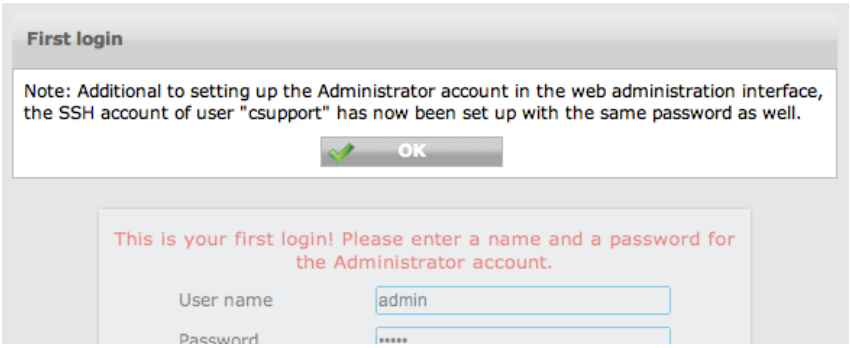

Figure 6.3. First login, csupport account

Please read and acknowledge the End User License Agreement (EULA) that is shown after the first login. Buttons to acknowledge the EULA are at the end of the document.

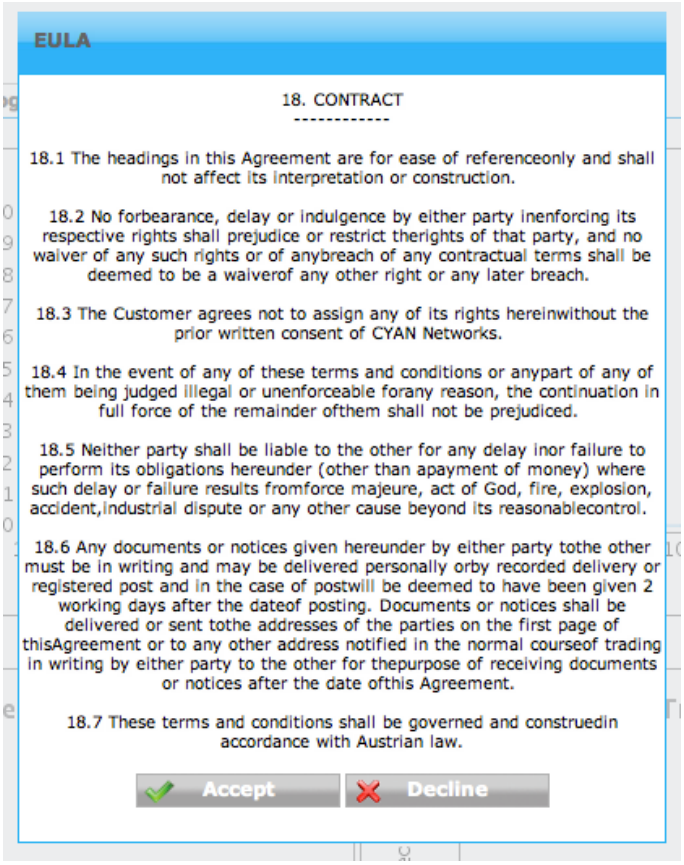

Figure 6.4. EULA

6.3. Secure Web License

Secure Web requires a valid license to operate. In case you have not received your license information and would like to evaluate Secure Web, please browse to the location

`http://www.cyan-networks.com/registration`

and follow the instructions on the screen. After a successful completion of the registration, a key file that includes the evaluation license will be sent to your email address.

In order to activate Secure Web with a valid license, got to menu *Services/Admin/License* and upload the key file that is attached to the email you received, after clicking the *"Secure Web"* button.

In case you received a ZIP archive with your license, **do not** uncompress it. The archive contains your Secure Web license and any additional license that you may have purchased and must be uploaded to Secure Web without uncompressing it on your own.

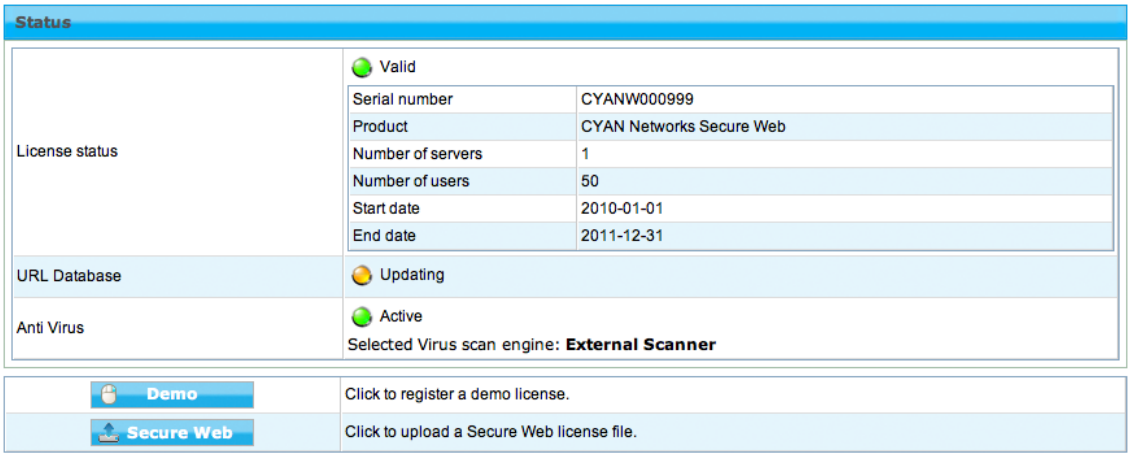

Figure 6.5. Secure Web License

Immediately after uploading the Secure Web license, the Appliance will start updating the URL database. The amount of downloaded data is about 100 MB so this can take several minutes, depending on the speed of your Internet connection.

6.4. User Support

The Appliance machines come with a pre-configured user named *csupport*. The primary purpose of this user is to provide access to the machine for the CYAN Networks support team. The support user, however, can also be used by yourself to get access to the machine for troubleshooting.

For the support user we installed the public key of the CYAN Networks support team. It is therefore not necessary to provide us with the password of the machine. The authentication is instead done by using public/private-key authentication.

The support user is enabled by default and set to the password of the first administrative user account that has been created on the first login. To disable the user, got to menu *Appliances/ Maintenance/Appliance Accounts*.

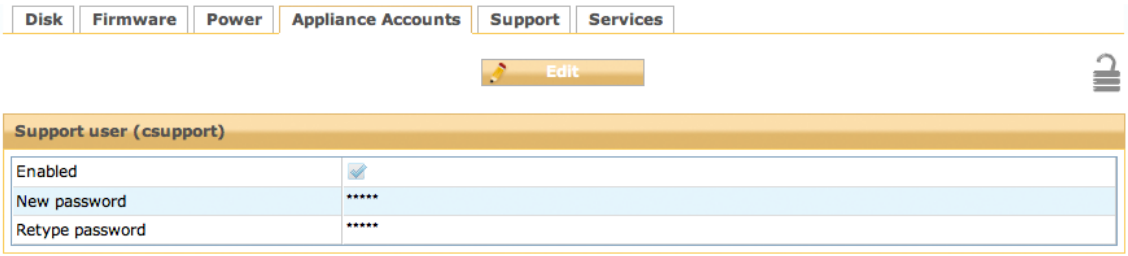

Figure 6.6. Disabling the support user

In a typical customer environment, the proxy machine is located somewhere within the network or in the DMZ, in any case behind a firewall. In case you would like to provide the CYAN Networks support team with access to your machine, please take care of a proper mapping of the connection for SSH from the public Internet to the Appliance machine.

Due to security reasons, the support user is disabled in the factory defaults but enabled during the first login.

We recommend that you leave the support user enabled prior to changing any network settings, leaving you with a possibility to recover an access to the machine without having to reset it to the factory defaults.

6.5. Changing the IP Address(es)

In order to change the IP address of your Appliance, navigate to the menu *Appliance/Network/Interfaces*.

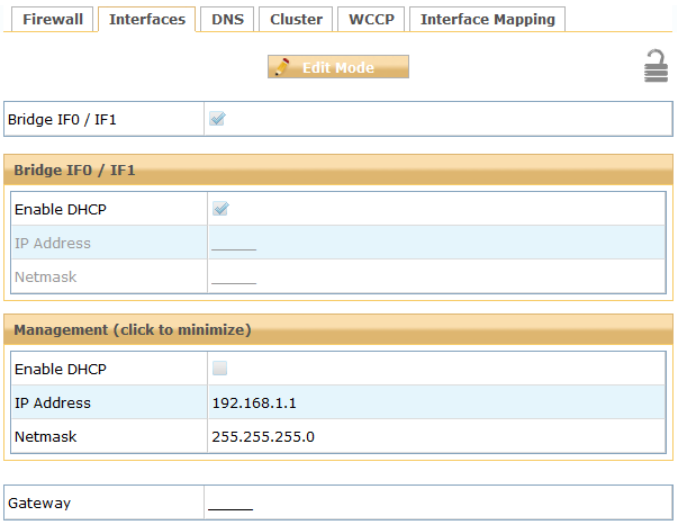

Figure 6.7. Network interfaces

After saving the changes, the appliance will immediately reconfigure itself and apply the new IP configuration. It takes the BR interface approximately 30 secondsto learn the network layout. Then you will have to reconnect to the Web Admin Interface on the new IP address.

In case you setup a static IP address, do not forget to adjust the DNS settings accordingly (see Section 6.6, “Setting up the DNS”).

After changing the IP address the machine might be inaccessible by your client PC. If you have made a mistake, please refer to Section A.2, “Recover from an invalid IP address” in order to manually reset the IP configuration.

6.6. Setting up the DNS

For static network configurations, you may specify up to three domain name servers in the menu *Appliances/Network/DNS*. In DHCP environments, DNS servers are usually set up automatically.

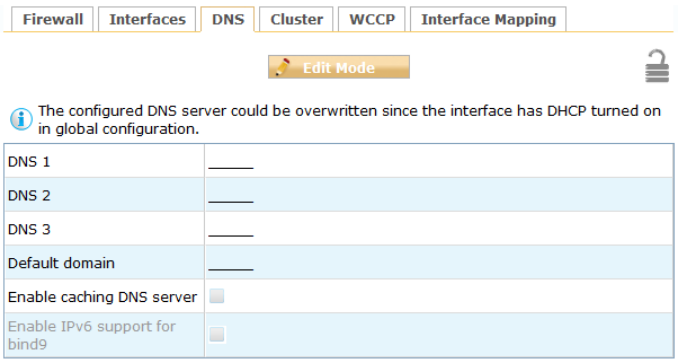

Figure 6.8. DNS Setup

6.7. Restricting Administration to the Management Port

The factory default allows the access to the Web Admin Interface on the bridge ports as well as on the management port. In order to restrict the access only to the management port

1. Open the menu *Appliances/Network/Firewall*
2. Disable the flag *"Allow management from IF0/IF1"*. This will deny any access to the Web Admin Interface that arrives on one of the bridged ports.

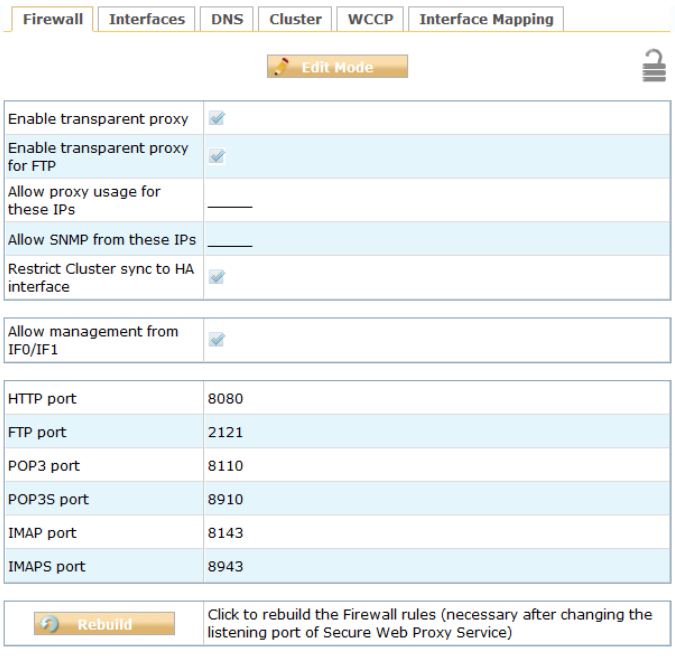

Figure 6.9. Bind management on management interface

The management interface does not support a gateway setting. Access is enabled solely from the management network segment.

Make sure that you are connected via the management port of the Appliance. After disabling management on the proxy ports (I0 and I1) you will no longer have access to the Web Admin Interface via this ports!

7. Configuring the Proxy Service

CYAN Secure Web consists of a number of services that build the proxy, web filtering and web security product (Secure Web Proxy). All services and corresponding components can be configured via the *Services* menu found on the left:

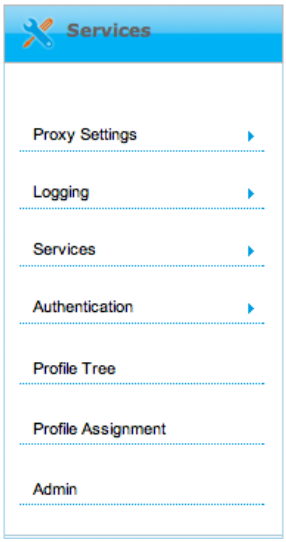

Figure 7.1. Services menu

7.1. Service Proxy

In most situations the Secure Web Proxy has no direct access to the Internet. At least a company firewall is located between the proxy system and Internet access. Sometimes an additional upstream proxy needs to be used for an access.

From the Secure Web Proxy, access to the following resources is required for operational purposes. Please make sure that access to these resources is allowed on any upstream firewall or proxy system.

- service.cyan-networks.com - TCP port 80 (HTTP), TCP port 443 (HTTPS)
- appliance.cyan-networks.com - TCP port 80 (HTTP)
- deb.cyan-networks.com - TCP port 80 (HTTP)

In some situations the Secure Web Proxy has no direct access to the Internet and an upstream proxy is needed for requests to CYAN update services. In that case, the parameters found in the menu *Services/Admin/Service Proxy* need to be configured accordingly.

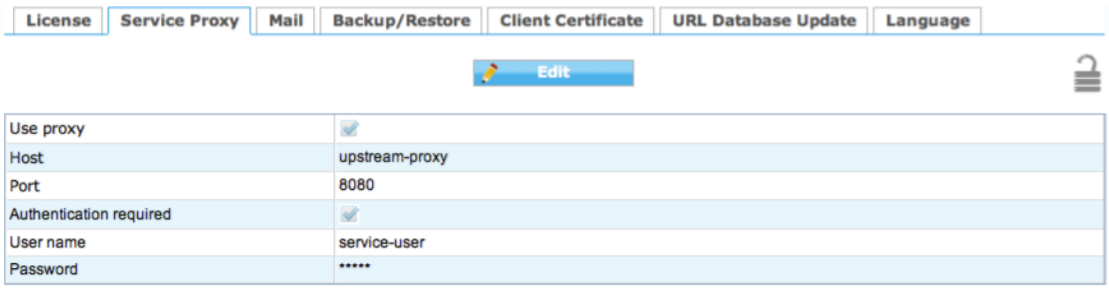

Figure 7.2. Service Proxy

Enable the use of an upstream proxy and specify the host and the port information in the dialog above. If the upstream proxy requires an authenticated users in order to be allowed to access the Internet, this credentials have to be added here too.

Only *Basic Authentication* is supported for upstream proxy access. If unsure, please ask your upstream proxy administrator for details on how to authenticate on the system.

7.2. Activating the Anti-Virus Engine

The Appliance comes pre-installed with the Clam AV engine. To enable virus scanning, navigate to the menu *Services/Proxy Settings/Anti Virus* and enable the scan engine. Please make sure that the selected Virus engine is set to *External Scanner* as shown in the screenshot below.

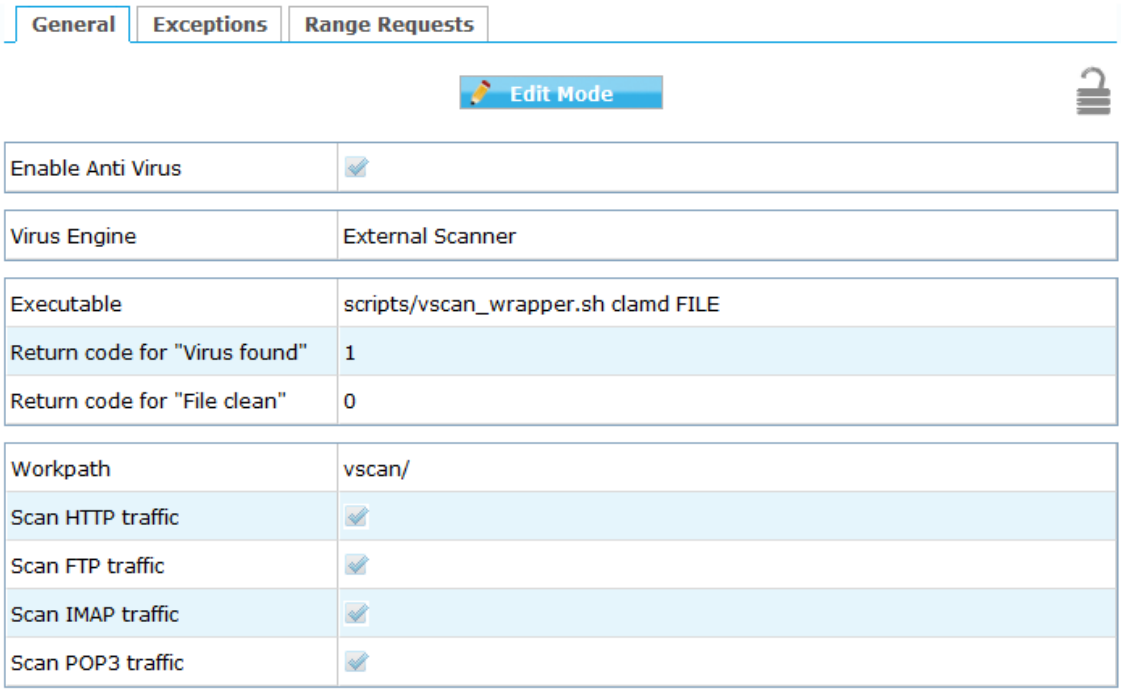

Figure 7.3. Anti Virus Engine

In order for you to evaluate the ESET anti virus engine, please send an e-mail to sales@cyan-networks.com for a trial license.

7.3. Testing your Installation

After you have finished configuring the Appliance, don't forget to press the *Apply* button on top of the Web Admin Interface. Without this action, the configuration changes are not applied to the Secure Web components.

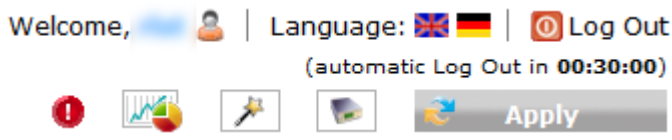

Figure 7.4. Apply button

To test your installation, all you need to do is to point your Internet browser to your newly setup Appliance. A short guide about how to configure some of the most used browsers follows:

7.3.1. Setting up browser

7.3.1.1. Internet Explorer

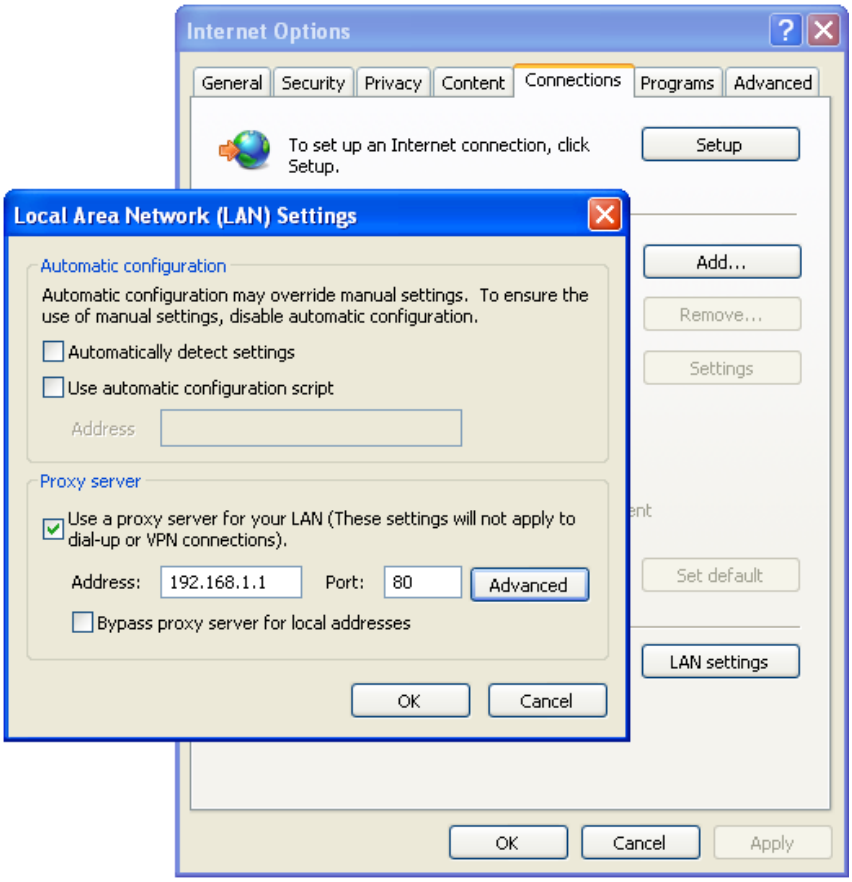

Figure 7.5. Proxy setup - Internet Explorer

To configure an Internet Explorer browser to use the newly setup Appliance as a proxy server, go to menu *Tools / Internet Options*, then navigate to tab *Connections* and click on the button *LAN settings*. In the dialog that appears check the *"Use proxy server for your LAN..."* checkbox, fill the IP address of the Appliance and port.

Figure 7.5, “Proxy setup - Internet Explorer” only contains a sample IP address. The IP address of your Appliance may differ. Please fill in the IP in the "Manual proxy configuration" field accordingly.

7.3.1.2. Mozilla Firefox

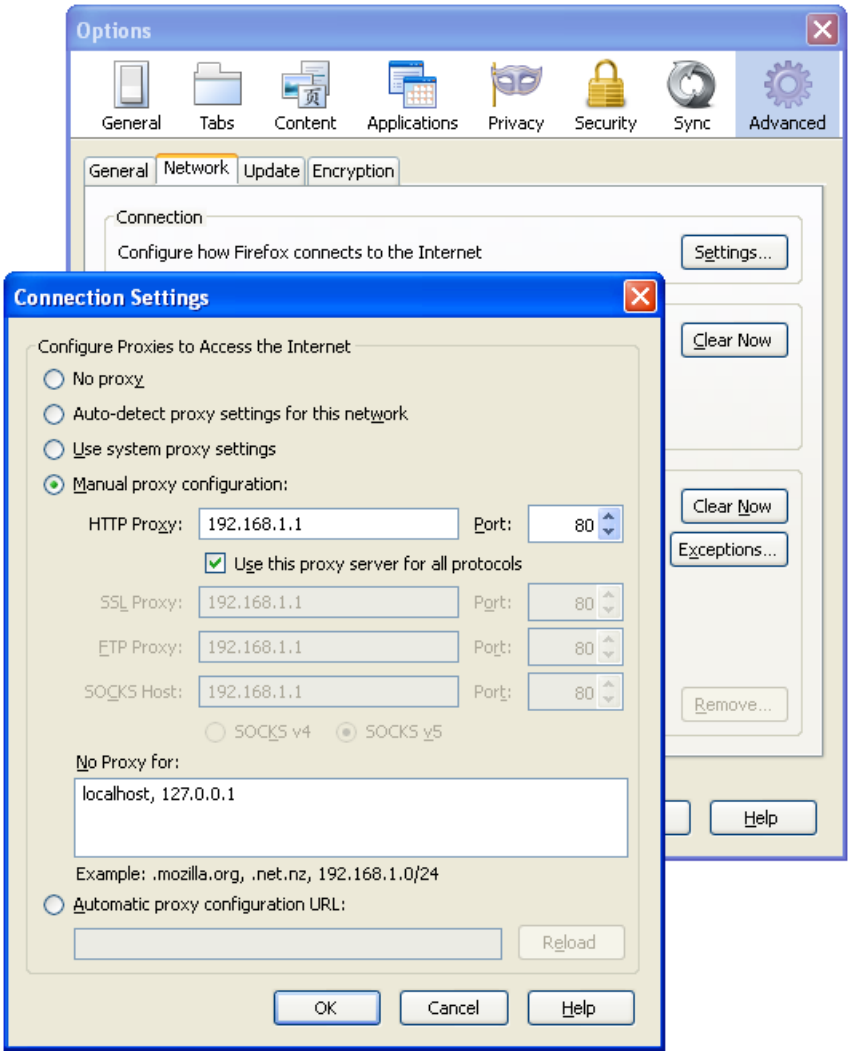

Figure 7.6. Proxy setup - Mozilla Firefox

To configure a Mozilla Firefox browser to use the newly setup Appliance as a proxy server, go to menu *Tools / Options*, then navigate to tab *Advanced*, sub tab *Network* and in *Connection* box click on the button *Settings…* In the dialog that appears select *Manual proxy configuration*, fill the IP address of the Appliance, port and check the *"Use proxy for all protocols"* checkbox.

7.3.1.3. Google Chrome

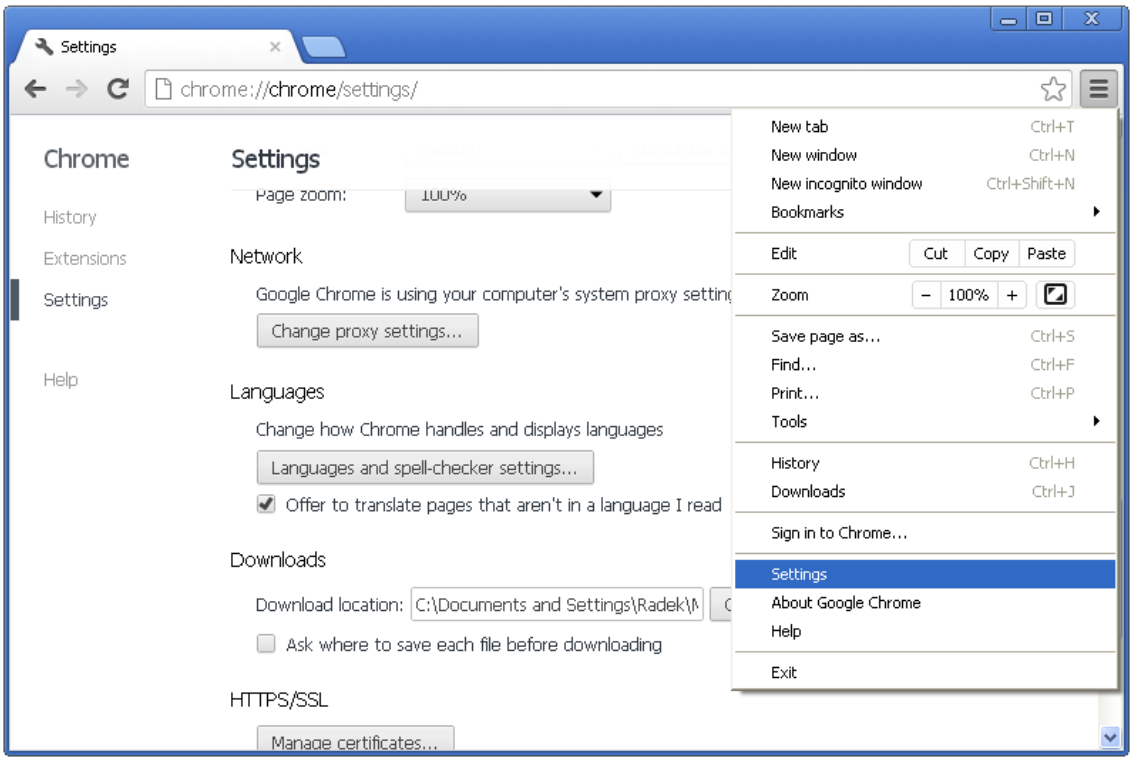

Figure 7.7. Proxy setup - Google Chrome

To configure a Google Chrome browser to use the newly setup Appliance as a proxy server, go to menu *Settings*, at the bottom of the page click on *"Show advanced settings"*, scroll down to *Network* heading and click on the *Change proxy settings...* button. The rest of the configuration is the same as for Internet Explorer browser.

7.3.1.4. Opera

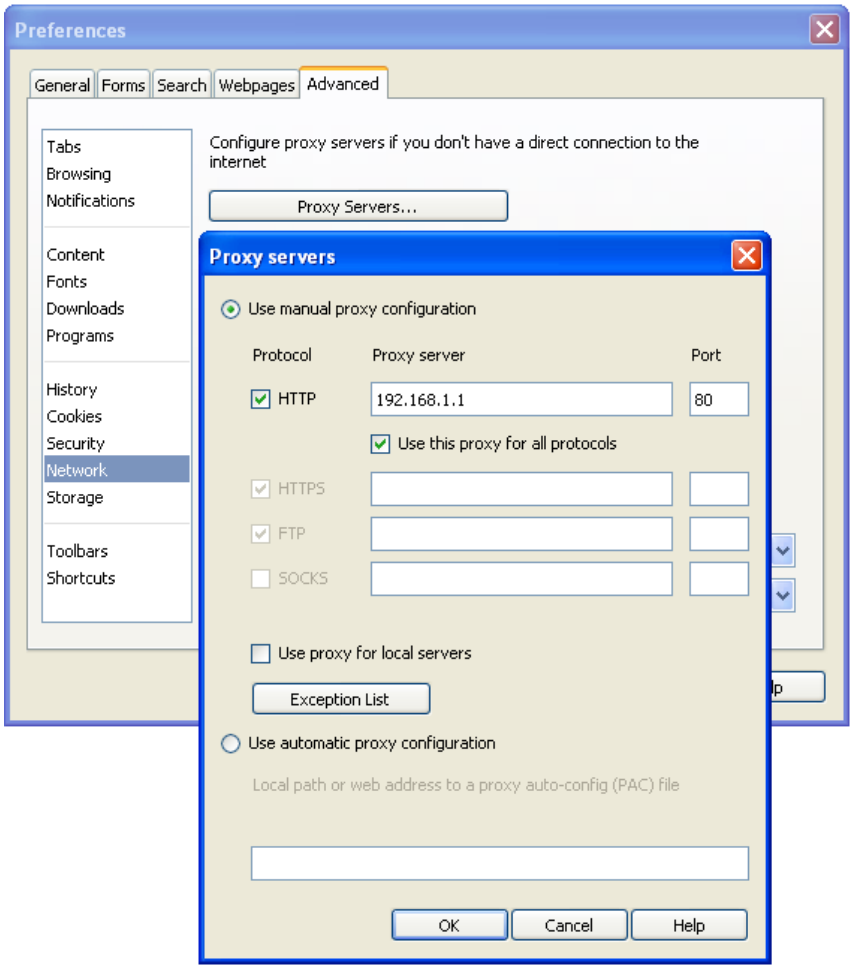

Figure 7.8. Proxy setup - Opera

To configure an Opera browser to use the newly setup Appliance as a proxy server, go to menu *Settings / Preferences…*, then navigate to tab *Advanced*, select *Network* in the list click on the *Proxy Servers…* button. In the dialog that appears check *HTTP*, *"Use this proxy for all connections"* and fill the IP address of the Appliance and port.

7.3.1.5. Windows Domain

If you have several computer connected to a Windows Domain and you are using Internet Explorer or Google Chrome browsers, the configuration of these browsers can be done also on the Domain Controller. Let us assume the following example Windows Domain:

- One domain called *ict.local*.
- One Organizational Unit (OU) within the domain called *company*.
- One Security Group *Computers* that is part of the OU *company*.
- Any number of computers, that are placed in the Security Group *Computers* and on which should be the proxy settings be changed.

To successfully set the proxy settings on all the computers within the *company/Computers* group, the following steps are necessary:

First, open the **Group Policy Management Console**. Click *Start*, click *Run…*, type "gpmc.msc" and press *OK*.

If the Group Policy Management Console fails to start, especially in the Microsoft Windows 2003 Server, you need to install it first. For the Microsoft Windows 2003 Server it can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=21895

In the Group Policy Management Console, add a new Group Policy Object (GPO). Navigate to *Group Policy Objects*, right click in the *Contents* tab and select *New*, as showed in the following figure:

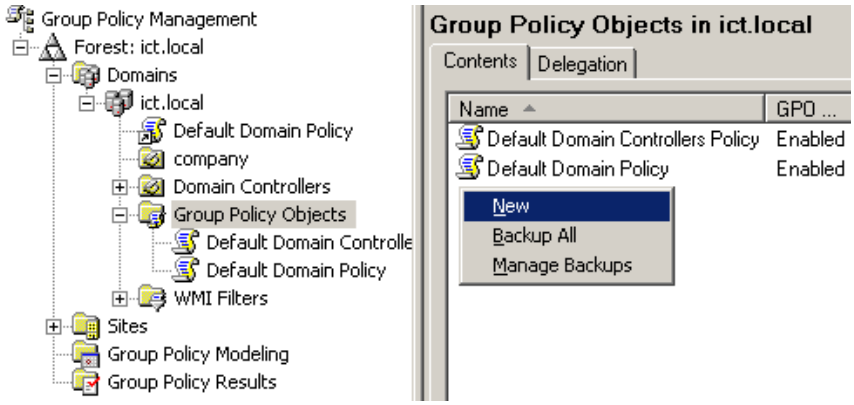

Figure 7.9. Adding a new GPO

Input new name for the GPO (for example "Set proxy"). Now right click the newly created GPO, select *Edit…* and navigate to *User Configuration* / *Windows Settings* / *Internet Explorer Maintenance*. Double click in the list on *Proxy Settings* and add the IP address of the Appliance, as showed in the Figure 7.10, “Setting the proxy IP address”.

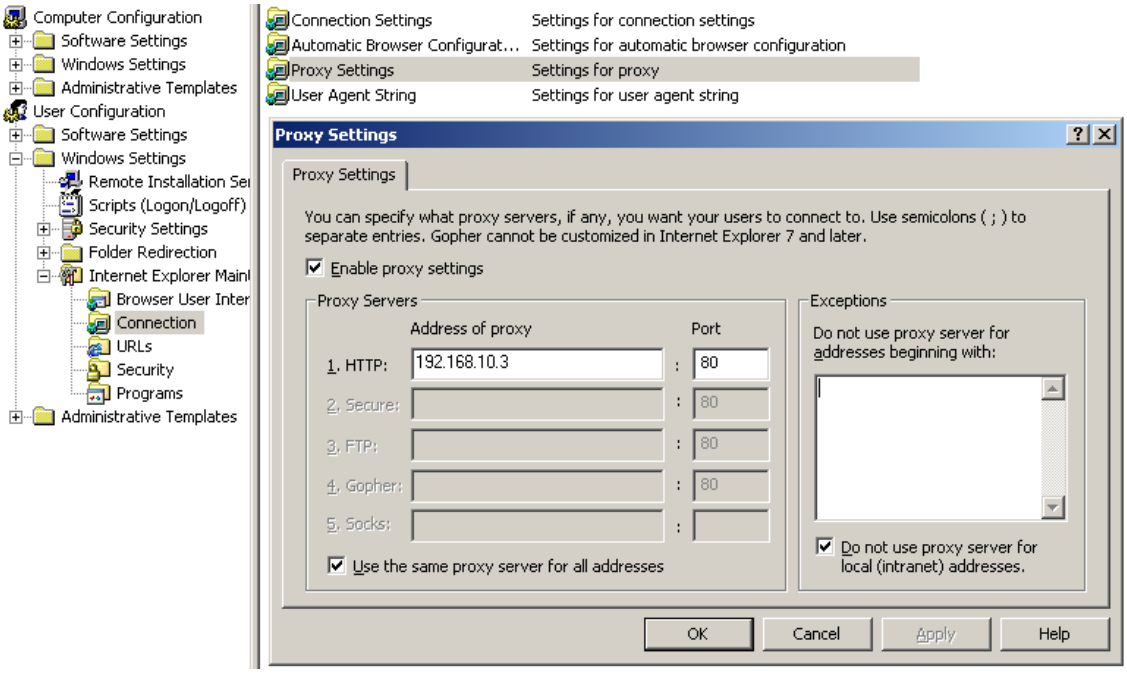

Figure 7.10. Setting the proxy IP address

Now it is necessary to link the "Set proxy" GPO to the desired OU (in this example OU *company*). It can be done simply by dragging the GPO and dropping it on the desired OU. The other way is right clicking the OU in the list, selecting *Link an Existing GPO…* and selecting the "Set proxy" GPO from the list. The following figure shows the desired result:

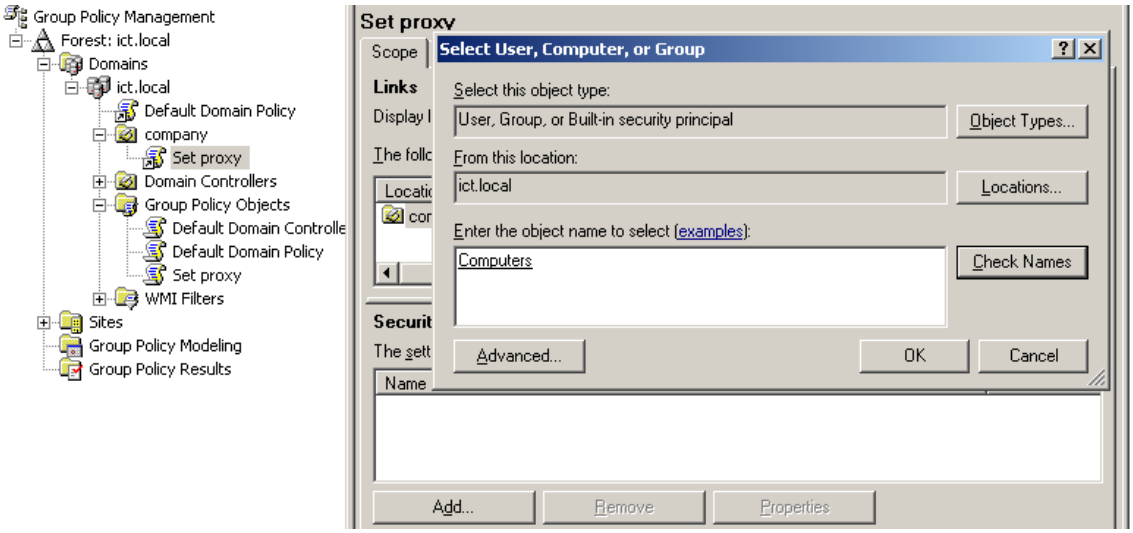

Figure 7.11. Configuring the GPO

By default, the GPO is restricted to all objects present in the *Authenticated Users* group. This group should cover all the objects (Users, Computers, etc.), that can successfully connect to the domain. To limit the GPO just to a group of selected computers (in this example grouped in the Security Group *Computers*), in the GPO view, tab *Scope*, click on the *Add…* button and select the appropriate Security Group. You can also remove the *Authenticated Users* group with the *Remove* button.

Please note that depending on the Active Directory settings, it may take up to 20 minutes to see the changes on the targeted computers and a re-login may be required after this time. To speed up the changes, it may help to issue command *gpupdate /force* on the targeted computers (but it is not required).

7.3.2. Testing access

Now enter some URL (for example http://www.cnn.com/) into the address bar and press *Enter* to load the web page. If everything works correctly, you will be served a blocking page because in the default profile *defaultrestrictive*, all categories are blocked.

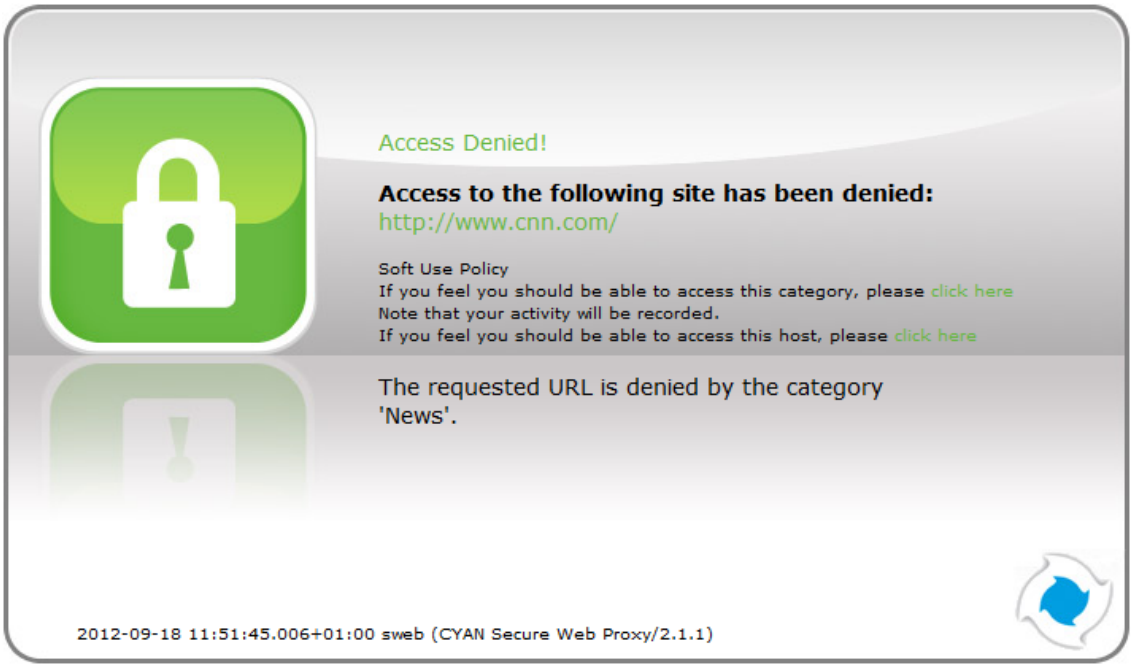

Figure 7.12. Category blocking page

Since Soft Use Policy is enabled in the *defaultrestrictive* profile, you may now click on *click here* to access the page regardless of the profile settings denying it.

To test the Anti Virus engine, direct your browser to http://www.eicar.org/download/eicar.com and acknowledge the Soft Use Policy that will allow you to download the content, even though *Archive* is not an allowed Application Type in the *defaultrestrictive* profile. This link contains harmless testing code that was designed specifically for testing reactions of anti-virus engines. There is no need to be concerned that you will access a page with an actual virus on it.

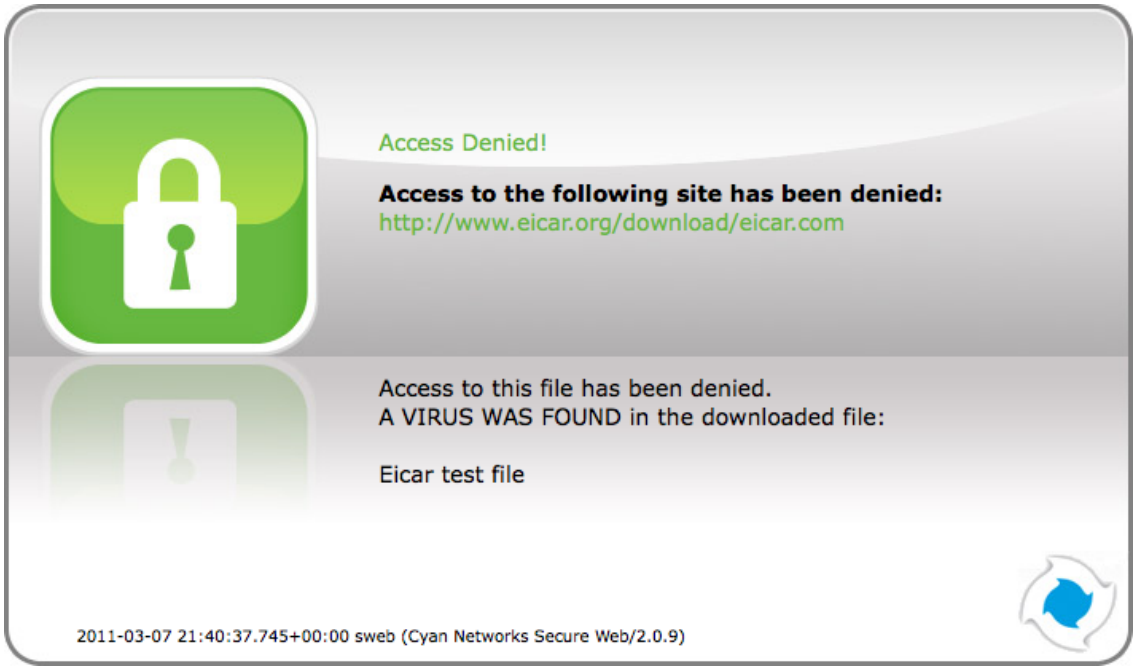

Figure 7.13. AV blocking of eicar.com download

After the virus scanning will take place and if the scanning is successful, the download will be denied from the Anti Virus engine.

Only integrated anti virus engines, like ESET and Avira, are capable of returning the virus name.

For performance reasons, we strongly recommend you usage of the integrated Anti Virus engine.

In case of any troubles, please refer to the troubleshoot section of this document (see Appendix A, *Troubleshooting*) or contact support at support@cyan-networks.com for help.

8. Initial Configuration

8.1. Initial Authentication Setup

Secure Web is installed on the Appliance with a default configuration. This configuration includes for the purpose of authentication an IP List instance named “IP List”, with one IP list named “global” representing “the world” (0.0.0.0/0). You can access this default instance by navigating into the menu *Services/Authentication/Instances*, double clicking the *"IP list"* instance in the list and navigating to the *IP List* tab (as shown in the following figure).

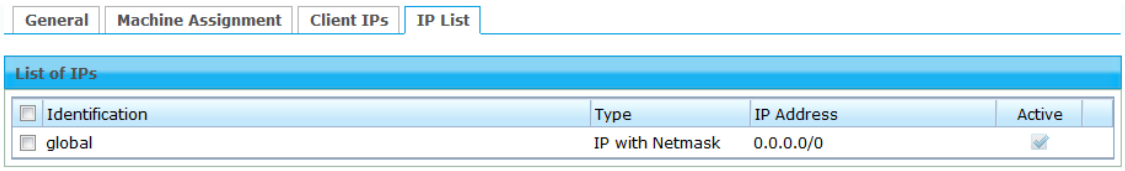

Figure 8.1. IP Instance default configuration

According to the order of evaluation as defined in Section 8.3, “Initial Profile Assignment Setup”, the IP List instance is evaluated first. Consequently the "global" IP list, which matches any IP address will affect all requests.

8.2. Initial Profile Setup

Complementary to the default authentication configuration, there is also a default setup of access rules. The profile tree shows the top level profile named "organization" and a sibling called "defaultrestrictive".

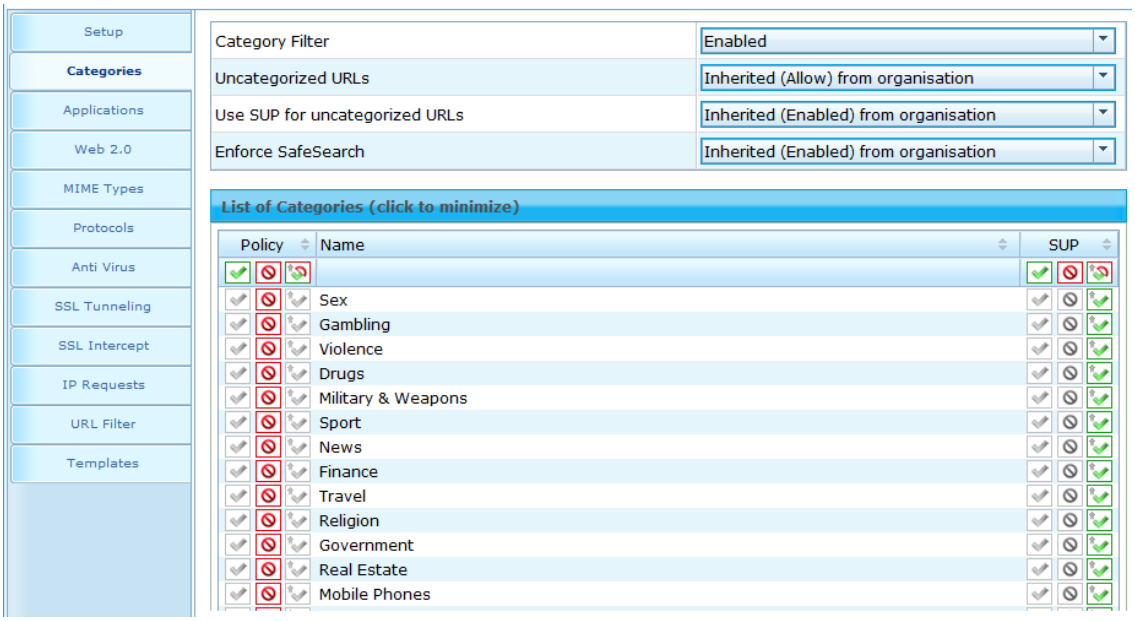

Figure 8.2. Profile default configuration

As shown in the Figure 8.2, “Profile default configuration”, the "defaultrestrictive" profile applies a rather strict type of Internet access by blocking all categories that are available in the CYAN Networks URL database.

The following figure shows the *General* dialog found at *Services* / *Authentication* / *Settings*, including the setting for the default profile which gets applied to all connections without a dedicated profile assignment. In this case it is the default "defaultrestrictive" profile.

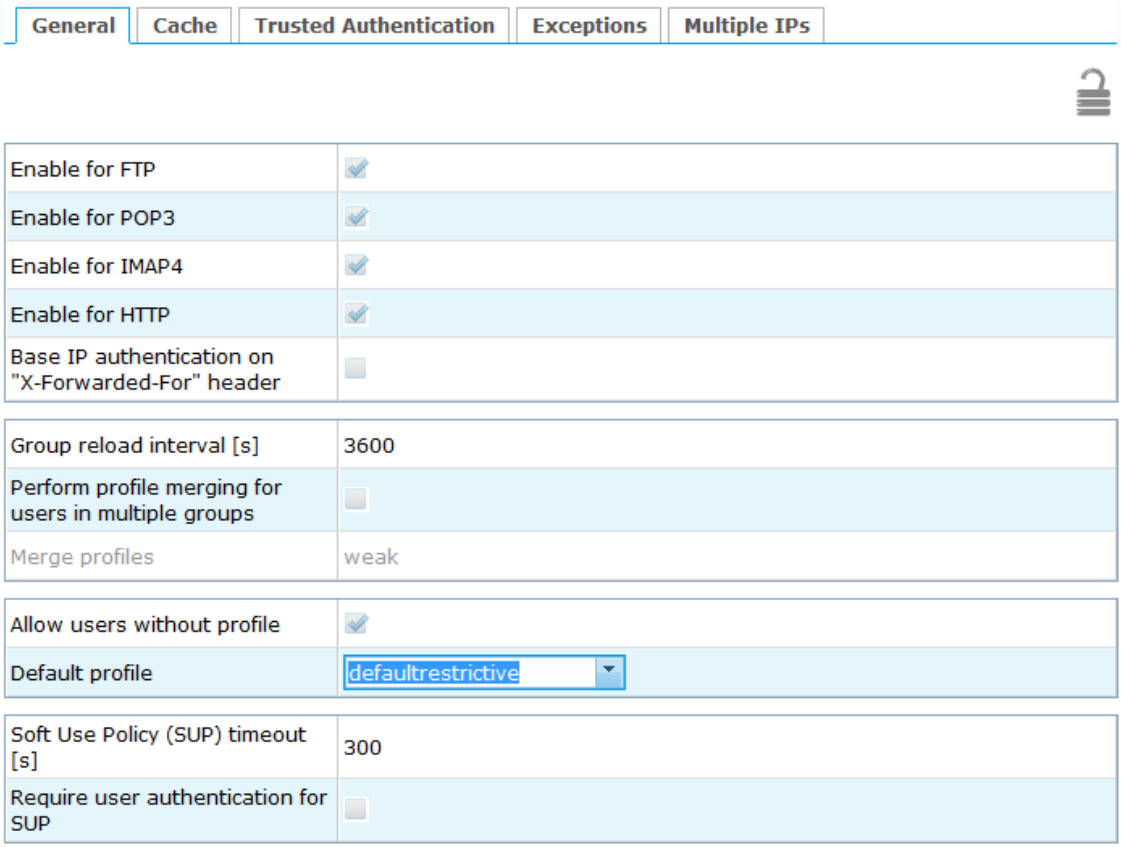

Figure 8.3. Default profile used

8.3. Initial Profile Assignment Setup

Per default, all requests served through the Secure Web Proxy are restricted by the *defaultrestrictive* profile, as set up in the *General* dialog found in *Service / Authentication / Settings* (see Section 8.2, “Initial Profile Setup”).

To assign profiles to different users, groups or IPs in the network, the administrator has to set up authentication and assign profiles to the user objects.

The following figure shows an example setup of an IP List authentication instance and assignments based on the IP objects. It can be created in the menu *Service / Authentication / Instances*.

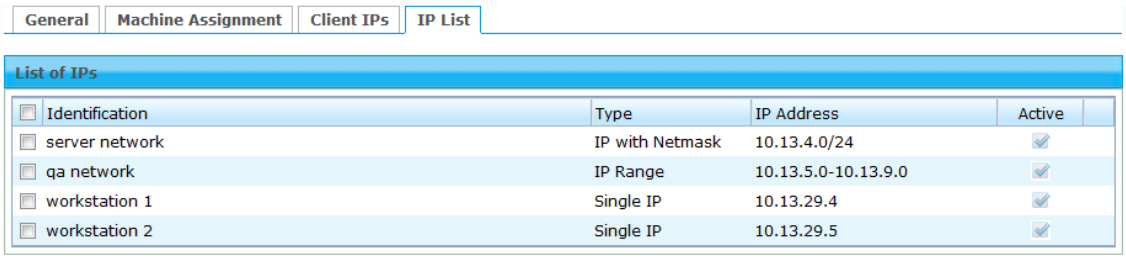

Figure 8.4. Example IP List instance

In this example, four IP objects are created based on the layout of the IP network. A network for servers and QA machines is created and two single IP objects represent workstations.

In the following figure the server and QA networks are assigned to the *defaultrestrictive* profile. This profile is rather restrictive and blocks all categories per default. This assignment can be done in the menu *Services* / *Profile Assignment*.

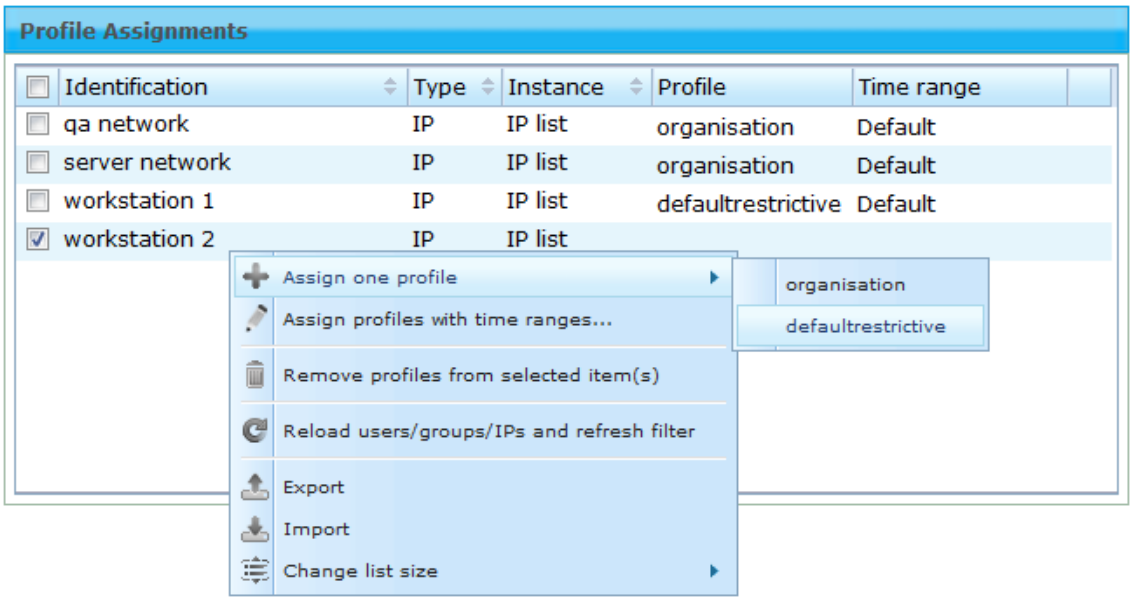

Figure 8.5. Example IP profile assignments

The two workstations in this example setup are assigned to the *organisation* profile, which is a very relaxed setup as this profile allows any request made to the Secure Web Proxy. Profile assignment can be modified by selecting some Authentication Instance from the list and using appropriate action from the context menu. New profile can be assigned by selecting *Assign one profile*, existing profile assignment can be removed by selecting *Remove profiles from selected item(s)*. More advanced manipulation can be done in *Assign profiles with time ranges…*

After finishing all desired changes do not forget to save them all using the *Save* button and then to apply them using the *Apply* button in the top right corner of the page.

9. Updating / Upgrading the Appliance

In order to get the latest product version of your CYAN Appliance, go to the menu *Appliances / Maintenance / Firmware*.

To start the update you have to press the *"Upgrade"* button as shown on the following figure:

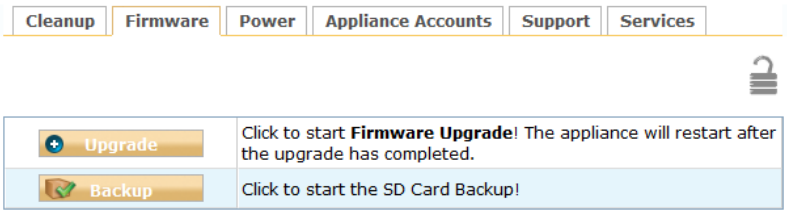

Figure 9.1. Firmware upgrade screen

After pressing the *"Upgrade"* button you will be taken to a different screen where you can perform the actual update of your Appliance (see Figure 9.2, “Upgrade Service screen - upgrade”).

Pressing the *Upgrade* button will start an update procedure that includes complete shutdown of all services running on the Appliance. This means any proxy functionality will unavailable until restart of the Appliance is performed.

Again press the *"Upgrade"* button. You will be informed about the ongoing update in the box bellow the button. In the example screen no update was neccessary and no new packages were downloaded.

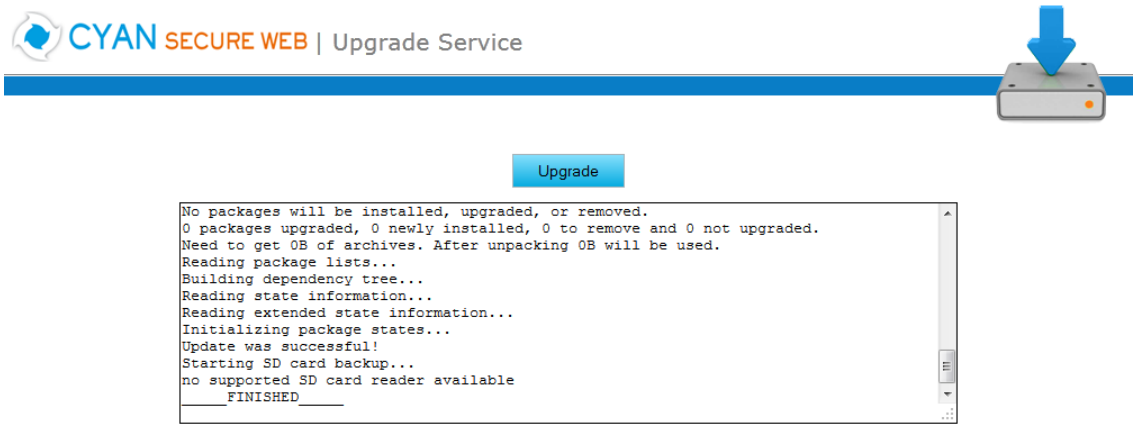

Figure 9.2. Upgrade Service screen - upgrade

After the update is finished you are advised to restart your Appliance. This can be performed by clicking the *"Restart"* button that appears below the information box (see the following figure).

Figure 9.3. Upgrade Service screen - upgrade

When the restart of the Appliance is completed you can navigate back to the Web Admin Interface using the browser navigation button.

There is no need to perform periodic checks if updates are available. Information about available updates of the Appliance can be found in the CYAN Networks newsletter. It is necessary to register in the company web pages to subscribe to it. Please visit http://www.cyan-networks.com/index.php/en/my-cyan to register (registration is for free).

10. Starting the Reporting System

The initial configuration of the appliance includes a pre-configured but yet inactive Reporting System. The following actions need to be completed to activate the Reporting System:

1. Setting up the Reporting Database
2. Enabling the Log Feed Service

It is strongly recommended to install the reporting database on a separate system. This especially applies for cluster setups, where a local database setup is highly discouraged. A local database system can cause performance impacts when reports are calculated and is not synchronised in cluster environments!

10.1. Login to the Reporting System

Point your browser to the address assigned via DHCP or the management IP, as the case may be. Replace *<appliance-ip>* in the following URL with the real IP address of your Appliance.

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

The welcome screen allows you to either access the Secure Web Web Admin Interface or the Reporting System.

Figure 10.1. Welcome screen

Click on *"Login"* next to *"CYAN Reporting System"* to navigate to the Web Admin Interface of the Reporting System.

The Reporting System uses different login credentials than the Secure Web. You may want to assign a different password to the Secure Web login in order restrict the administration of the machine parameters and the reporting to different people.

The default login values after setup are:

- **User:** `admin`

- **Password:** `admin`

We strongly recommended to change the administrator password as soon as possible. Navigate to the menu *Users / User* and double-click on the **admin** user or click on the person-shaped icon next to your login name in the top right corner of the screen to change the password.

10.2. Setting up the Reporting Database

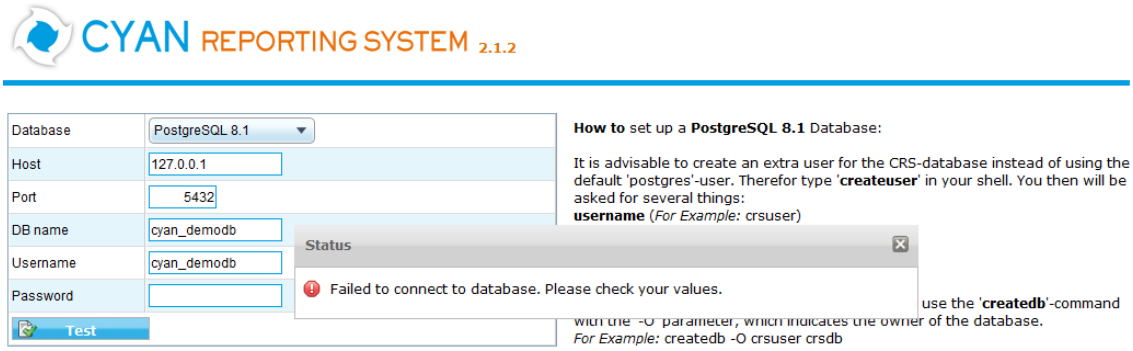

Figure 10.2. Setup the reporting database

If you have not setup any database access previously, at login, you will be informed about incorrect values (as seen in figure Figure 10.2, “Setup the reporting database”). There are many different database engines supported for using the Reporting System:

- PostgreSQL 8.0 or higher
- Microsoft SQL Server 2005 or higher
- MySQL 5.0 or higher
- Oracle
- DB2
- H2 Database

For each database engine there is available a short quide what SQL commands to issue to correctly make the initial database setup. You can test the settings using the *"Test"* button.

The configuration of the Reporting System database assumes you already have setup a database engine of your choice and you can connect to it. If after filling in all required information a connection error still appears please check all the login credential, priviledges, firewall settings and whether the database engine daemon is running.

Whenever any new version of the Reporting System should require any changes to the database, your explicit confirmation is requested in order to proceed with the upgrade. That will be most likely your case since there is no database structure yet and it needs to be created. An example of such upgrade request shows the following figure:

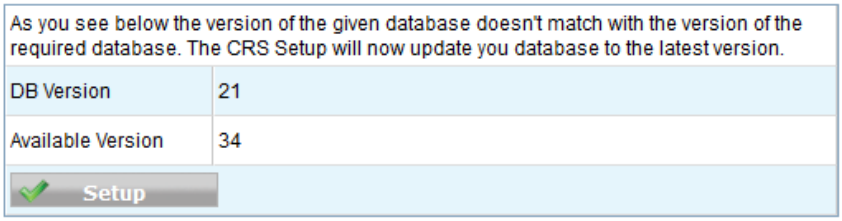

Figure 10.3. Upgrade of the reporting database

Database upgrades may take a long time and can cause significant impact on the operation and performance of the system. Therefore the Reporting System will never upgrade the database automatically, but leave this decision to the administrator.

After a successful completion of the setup / upgrade of the database, a *"Login"* button appears at the end of the page and allows you to go to the login screen.

10.3. Enabling the Log-Feeder

In order to activate the import of the reporting information into the reporting database, the log feeder service of Secure Web must be enabled. This service picks up the log files generated by Secure Web and feeds them into the reporting database.

Change to the Secure Web administrative interface, select the menu *Services* / *Logging* / *Reporting Log* and browse to the dialog *Log Feeder* as shown in the following screenshot:

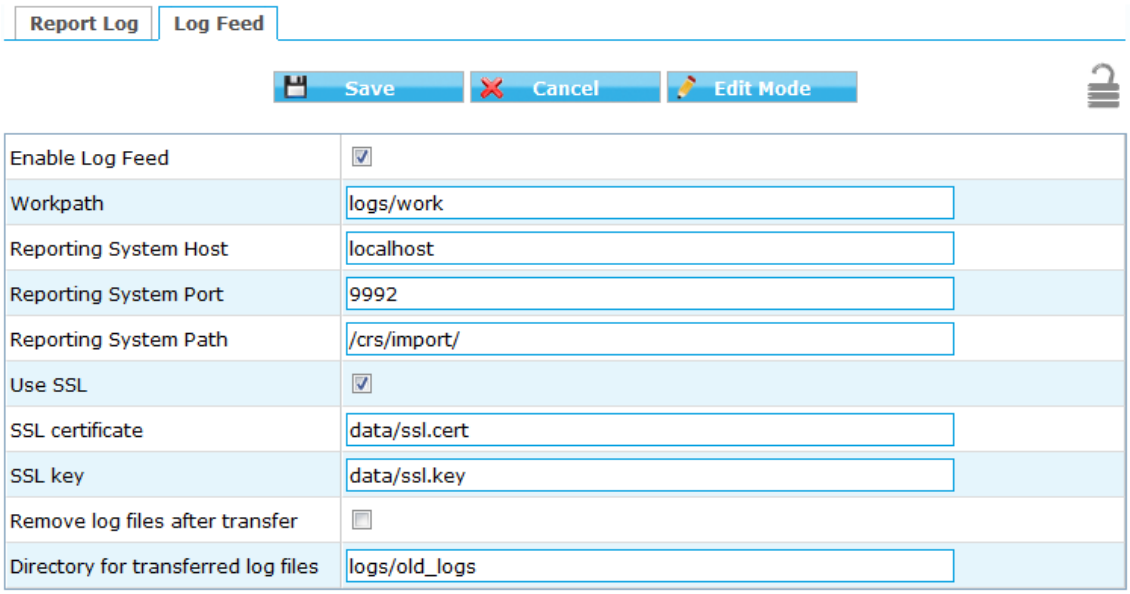

Figure 10.4. Log feeder

The default values in this dialog are prepared to operate with the Reporting System on the same machine. In case you want to run the Reporting System on a separate machine, please refer to the Secure Web Reference Guide that describes the necessary steps.

Do not forget to save any changes you have made by the *Save* button and then apply them using the *Apply* button.

The first time you enable the Log-Feeder it may time some time to generate output from all the available logs.

Appendix A. Troubleshooting

A.1. Getting access to the command line

A.1.1. Access via SSH

The Appliance can be accessed using SSH protocol. This access is enabled by the factory defaults. During the initial setup is created a special user account in the Appliances system with username *csupport* and the same password as the one used for *Super Administrator* account in the Web Admin Interface (in the following text denoted as *Password*). For connecting to the Appliance via SSH you also need to know the Appliances IP address (for example 192.168.1.1, in the following text denoted as <appliance-ip>).

A.1.1.1. From Unix/Linux

Accessing the Appliance from a Unix based system is fairly easy. In the command line issue the following command:

```
ssh csupport@<appliance-ip>
```

If this is the first time you are connecting to the Appliance via SSH from current system, confirm the security warning and input the *Password* when asked to.

A.1.1.2. From Microsoft Windows

Accessing the Appliance via SSH from a Windows system is a little more complicated. Windows systems do not have by default installed any SHH client programm, so you will need to obtain one. One of the most popular ones is a freeware software called *PuTTY*, which does not require any installation. All versions are available for download from the following web page:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

A direct link to the latest executable 32bit version for Windows is following:

http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe

When the download is complete, run the downloaded executable and the SSH client login screen should appear (as you can see in Figure A.1, “PuTTY window”). In the window input login information in the *Host Name (or IP address)* field. Use the same format (substitute the example IP address *192.168.1.1* with the real IP address of your Appliance). Then click on the *Open* button, confirm a security warning if it appears and input the *Password* when asked for one.

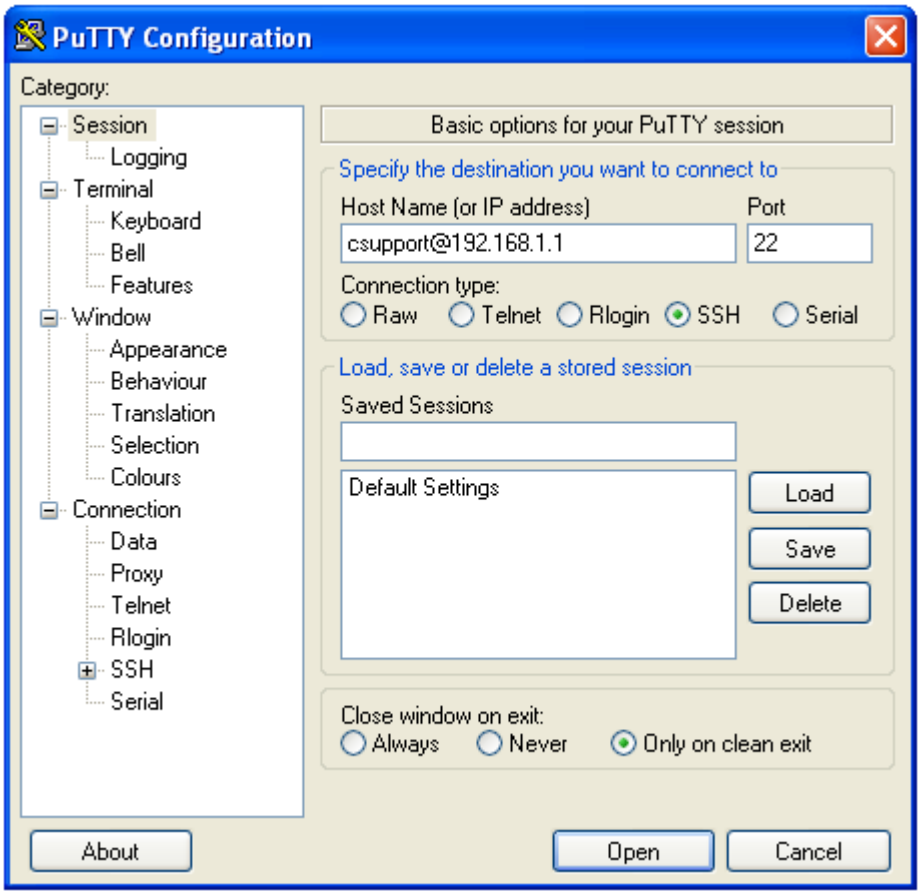

Figure A.1. PuTTY window

Once you are logged in to the system, you will be able to see a simple text menu providing quick access to some of the useful maintenance functions:

```
Welcome to CYAN Secure Web
==========================

The menu system lets you easily perform various tasks on the appliance.
Please be carefull when changing network configuration or rebooting
the appliances, since these tasks may interrupt your operation of
CYAN Secure Web.

1. Network management
2. Restart/shutdown appliance
3. Perform network analysis (ping, dns, http)
4. Remove cluster configuration
5. Maintainance on web admin
6. Watch log files
7. Watch appliance performance values
8. Set a 'root' password
9. Open 'root' shell
0. Exit

Please choose [1-9 or 0] to continue.
```

Figure A.2. Console main menu

A.1.2. Access using monitor and keyboard

With a keyboard and a monitor attached to your appliance machine, you may login to the command line using the credentials of the csupport user (as described in the previous section).

After logging in to the system you will be able to see and operate the same way as shown in the previous section.

A.2. Recover from an invalid IP address

In case that you have set up an IP address which is not reachable by your client PC, there is an alternative way to change the IP address of the appliance by using the command line interface (see Section A.1, “Getting access to the command line”).

If you have already successfully logged into the system using the csupport account, navigate to menu *Network management / Display interfaces* to see the list of available interfaces on the Appliance. Make a note of the name of the interface which IP address you want to change:

```
Interface   :  eth0
IP          :  192.168.1.9
Netmask     :  255.255.255.0
Link        :  yes
Speed       :  1000Mb/s
Duplex      :  Full
```

Figure A.3. Network interfaces

Press any key to return to the previous menu and this time choose *Temporarily change network configuration* menu item. You will be asked for a name of the interface you have noted down in the previous step, new IP address, network mask and optionally gateway IP address.

If you are connected to the appliance via SSH and you changed the IP address of the interface to which you are currently connected, the connection will be dropped without any warning and you will have to reconnect to the newly set up IP address.

After changing the IP address of the Appliances port via console menu you have to change the IP address again in the Web Admin Interface! Please refer to the Section 6.5, “Changing the IP Address(es)” to get information about changing the IP address permanently. Any changes done using the console menu will last just until a reboot of the Appliance.

Appendix B. Contact data

B.1. How to contact our sales department

Tel.: +43 (1) 33933-0

Email: sales@cyan-networks.com

B.2. How to contact our support department

Tel.: +43 (1) 33933-333

Email: support@cyan-networks.com

B.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 B.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 B.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.

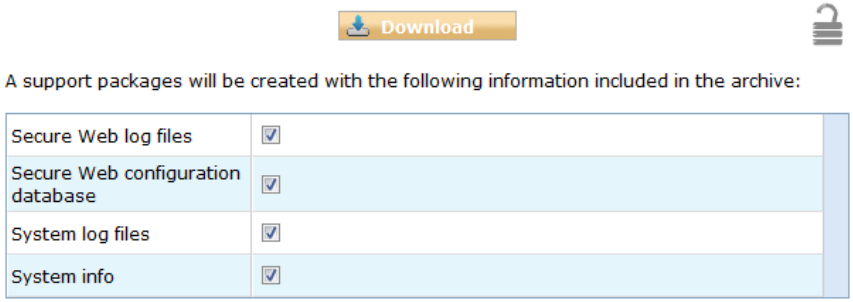

Figure B.3. Support Package

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