Proto Balance SSL – TLS Off-Loading, Load Balancing

http://www.protonet.co.za/

User Manual - SSL

Proto Balance SSL - User Manual

March 13, 2010

Contents

1 Introduction

Proto Balance SSL is the third of Proto Co Networking's suite of network utility software products.

Proto Balance SSL includes all the features of Proto Balance and Proto Balance Advanced, while also being a lot more. Before reading this manual, please refer to the Proto Balance User Manual for installation instructions and operating system specific configuration.

Before reading this manual, you should be familiar with the actions of:

- Creating a cluster.
- Adding boxes to a cluster.
- Enabling a box.
- Modifying the configuration options of a cluster.

For information on load balancing, transparent fall-over, and features preventing denial-of-service attacks, please see the Proto Balance User Manual.

Please also refer to the product comparison chart:

`http://www.protonet.co.za/productcomparison.html`

2 SSL Off-Loading

Proto Balance SSL has built-in optimized support for the SSL/TLS encryption standard supported by all major browsers. Proto Balance SSL receives an incoming SSL connection and negotiates the SSL connection with the client. It makes an ordinary non-SSL connection to your server application - in the case of a web server, it makes an http:// connection to your web server. It then transparently forwards all data between the client and the server application.

This means that your web server does not have to handle the CPU intensive actions of SSL negotiation and encryption. Instead, Proto Balance SSL takes this load.

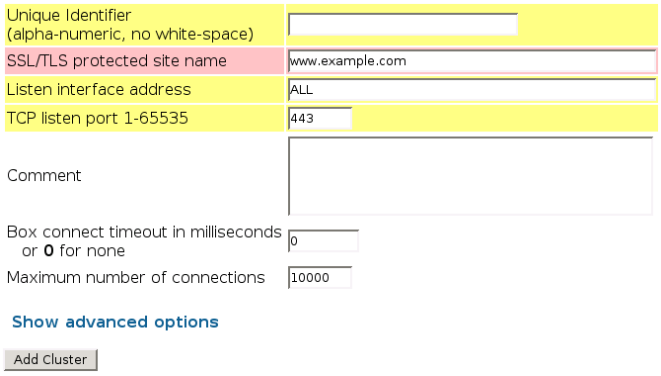
Typically a web server will spend 90% of its CPU on SSL, and 10% of its CPU handling your web site pages. By installing Proto Balance SSL on a different machine you can increase your web site's responsiveness by a factor of 10.

Note that Proto Balance SSL can turn any service into a secure service - not just HTTP.

3 Certificate Management

Proto Balance SSL is more than just an SSL off-loading application. It can also properly handle the full life cycle of your web site's certificates.

To create a new SSL cluster, click on "Add SSL Cluster". You will be presented with the following form:



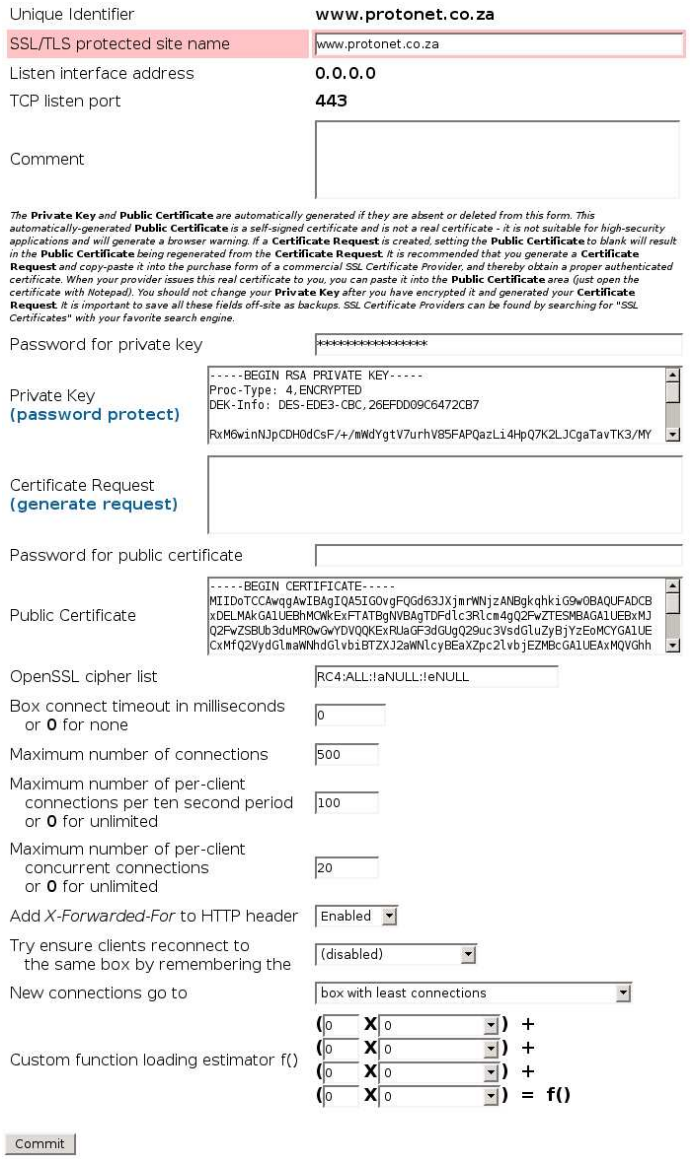
The only special entry field above is the "SSL/TLS protected site name". All other entry fields have the same meaning as for regular (non-ssl) clusters. The site name is critical to the correct operation of your https:// web site. The site name must be the same as the official domain of your site. This means that the site name must be carefully chosen, since it will be the name in which you will purchase certificates and must correspond exactly with the Internet Domain registrar you are using as well as with all links and HTTP redirections. For example, choosing a URL https://secure.mysite.com/ for your site and then later changing it to https://www.mysite.com/ will not work, and can be costly and time-consuming to correct.

Therefore it is best to decide up front on a site name and use the same site name for the life of the web page.

Once you have submitted the form, Proto Balance SSL automatically generates a private key and web site certificate. However, this certificate will not be a real certificate, but a self-signed certificate. A self-signed certificate is really a dummy certificate that allows you to get your web site up and running quickly before you go about purchasing a real certificate. An https:// web site with such a dummy certificate does indeed provide better security than a plain http:// web site, but it is no substitute for purchasing a proper certificate from a certificate vendor.

If you do not purchase a proper certificate, users visiting your https:// web site will be presented with the warning dialog (Netscape/Mozilla/Firefox),

Below is an example configuration for a cluster. You may already have a private key and certificate. In this case you can delete the private key and certificate generated by Proto Balance SSL, and paste your own private key and certificate into the text entry field as show. Note that the text entries are editable - be sure not to modify them by accident. Note the "Certificate Request" section which will be discussed below.



4 Choosing a Certificate Vendor

Note that Proto Co Networking does not endorse any particular certificate provider.

Before going to a popular certificate vendor, check with your domain registrar (the company that issued your site name) if they are already a certificate authority. Many domain name registrars also sell cheap certificates as a value added service. A good reason to use your own registrar is that it is easy for them to authenticate existing customers, so you will get your certificate very quickly.

Alternatively, a list of certificate advertisers can be found at:

`http://www.protonet.co.za/certificatevendors.html`

When purchasing a certificate, your vendor may at some point ask you what software was used to generate the certificate request. In this case select "Apache-ModSSL".

5 Obtaining the Private Key and Certificate from Apache

You can easily move your certificate from Apache to Proto Balance SSL. Apache usually stores its private key and certificate in the files:

/etc/apache2/ssl.key/server.key
/etc/apache2/ssl.crt/server.crt

These files contains certificates in PEM format - which is a plain ascii text format that can be copied and pasted into the editable text entry field of the cluster configuration form.

6 Generating a Certificate Request (CSR)

A certificate request or Certificate Signing Request (CSR) is a short block of text that encapsulates all your details. Like certificates, the text looks like gobbledygook and is not human readable.

If you do not yet have a certificate and would like to purchase one from a certificate vendor, start by visiting the certificate vendor's web site and beginning the application process. At some point you will be asked for the "Certificate Request" or CSR.

Proto Balance SSL generates the certificate request for you - just click on "(generate request)" in the cluster configuration and complete the form. When you have submitted the form, the certificate request text entry field will be filled.

Copy and paste this text according to your certificate vendor's instructions. When you have completed your purchase, the certificate vendor will provide you with a public certificate that you can paste into the text entry field "Public Certificate".

7 Certificate Issuing Process - Tips

The most important detail when applying for your certificate is that a) the email address through which you correspond with your certificate vendor, and b) the email address in your certificate request, and c) the email address listed by your domain registrar, must all be the same.

These email addresses are the primary test of who is allowed to own a certificate for the site.

Your vendor may also allow you to choose whether you would like a certificate in the name of your company or a certificate in your personal capacity. It doesn't matter which you choose, but keep in mind that company applications will require you to prove the physical address and Incorporation of the company - documentation you will have to gather and submit.

8 Password Protecting Your Private Key

To password protect your private key, click on "(password protect)" on the cluster configuration page. Password protection of your private key is important for security. Should your private key fall into the hands of a malicious party, they can easily create a trojan site with the same site name, and eavesdrop on communications to your site.

9 Supported Ciphers

Proto Balance SSL has a configuration option under the "Info" tab, in the text entry field "Default OpenSSL cipher list for new clusters". The default cipher pattern for this option is:

RC4:ALL:!aNULL:!eNULL

This means Proto Balance SSL will support any client that may wish to use RSA, DES, AES, RC4, MD5, and SHA ciphers and hash algorithms, with any key size, including key sizes too small to be secure. It also means that Proto Balance SSL will try to encourage use of the RC4 cipher since this is the fastest algorithm, consuming the least CPU.

Proto Balance SSL does not support the less widely used algorithms. If you require these then please contact us for a custom build.

For security, you should immediately set your cipher pattern to:

RC4-SHA:RC4-MD5

This has the benefit of forcing the use of RSA with RC4 (RC4 is about twice the speed of AES) as well as the benefit of disabling weak encryption (used only in a few countries). Very few web browsers will be adversely affected by this setting.

10 Log File Errors

- sslv3 alert bad certificate

This error means that the web browser or other client rejected the certificate. It usually happens when the user gets presented with a dialog box questioning the validity of the certificate, and then clicks to reject access to the site.

This also means that you are using the self-signed free certificate that Proto Balance SSL has generated. If you purchase a proper certificate you will avoid this error.

- key values mismatch

This error occurs if you update your key, but do not change your certificate to match it. To fix this error, delete the certificate by replacing the certificate text entry field with blank spaces - it will be automatically regenerated. Otherwise replace it with a purchased certificate by generating a certificate request and submitting it to a registered certificate authority.