SSL Acceleration

Exinda ExOS Version 6.3

Table of Contents

Part

1 Introduction

SSL Acceleration

Exinda Firmware Version: 6.3

1.1 Using this Guide

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

Note: This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

Caution: This is a caution.

1.2 Further Reading

In addition to this How to Guide, the following relevant user documentation is available and should be read in conjunction with this guide:

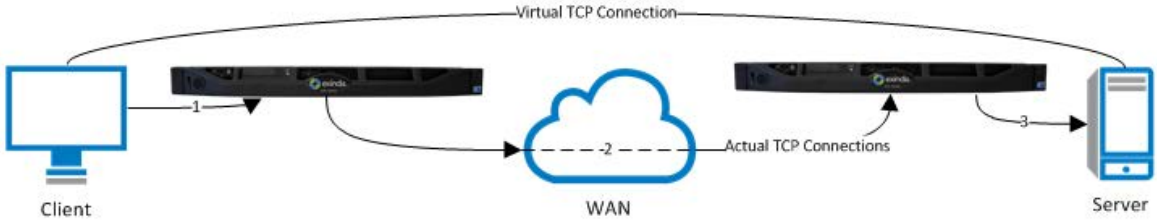
- Exinda User Manual

Please visit http://www.exinda.com for more information.

Part II

2 Overview

Exinda's Application Acceleration technology transparently intercepts TCP connections and terminates them on the appliances closest to the client and closest to the server. Acceleration techniques such as TCP Acceleration and WAN Memory are then applied to the TCP connection that exists between the 2 terminating Exinda appliances.

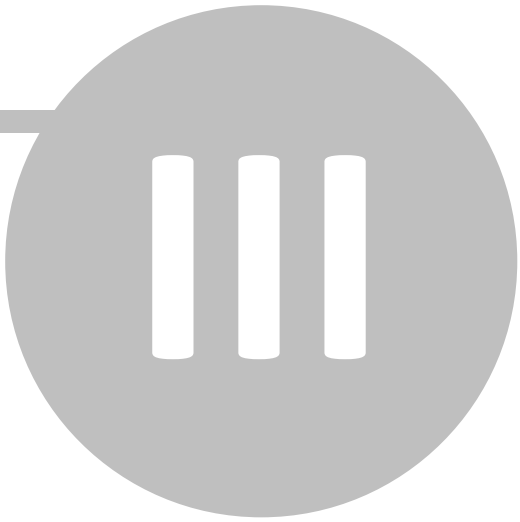


If the connection between the client and the server uses SSL to encrypt the payload, then the benefits that can be gained by Application Acceleration are limited. For example, Exinda's WAN Memory technology will achieve higher reduction on clear text rather than encrypted data.

SSL Acceleration is designed to overcome these limitations by transparently decrypting accelerated traffic, performing the relevant Application Acceleration techniques, then re-encrypting the traffic again. This means Exinda can perform apply all Application Acceleration technologies to the traffic as if it were clear text, while still maintaining SSL connections.

Note: SSL Acceleration requires an additional, optional license before this feature can be configured and used. Please contact Exinda TAC or your local Exinda representative if you do not have this license and you wish to use this feature.

Part



3 Configuring SSL Acceleration

SSL Acceleration can be configured in 3 easy steps. Only Exinda appliances with a valid SSL Acceleration license will be able to configure SSL Acceleration.

1. Configure SSL Certificates and Private Keys to use for SSL Acceleration.
2. Configure the Servers to use for SSL Acceleration.
3. Create Optimizer Policies that allow SSL traffic to be accelerated.

Note: Currently, it is a requirement that SSL Acceleration settings on each Exinda appliance be configured exactly the same.

3.1 Certificate and Key Management

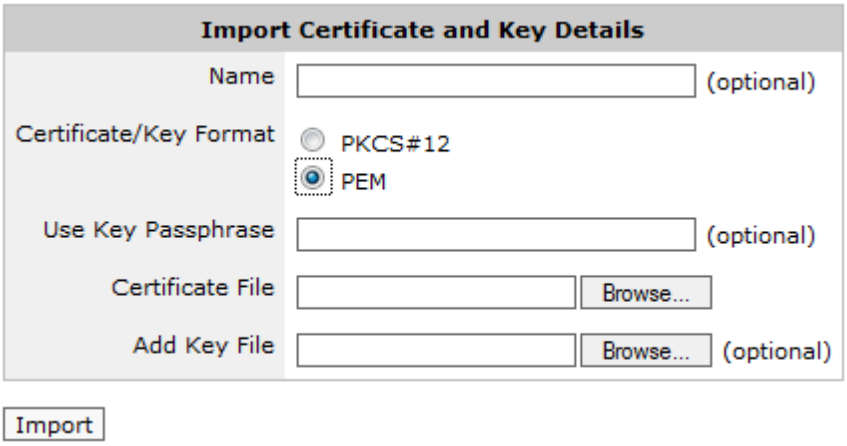
The first step to configuring SSL Acceleration is to load Certificates and Keys, to be used for SSL Acceleration, onto the Exinda appliances. This can be done using the form on the System | Certificates page on the Web UI, advanced mode.

There are 2 choices at this point:

1. **Load the real certificate and private key from the server that is hosting the accelerated SSL application.**
   Advantage: The end user will see the real certificate when they access the accelerated SSL application.
   Disadvantage: The private key of the accelerated SSL application needs to be loaded on ALL Exinda appliances.

2. **Load different or self-signed certificate and private key.**
   Advantage: Private keys never leave the server, a different set of private keys are installed on the Exinda appliances.
   Disadvantage: End users will receive a warning notifying them that that certificate is invalid unless the common name (CN) in the certificate loaded on the Exinda appliances matches the common name of the accelerated SSL application AND the end-user trusts the certificate loaded on the Exinda appliances.

Regardless of which option is chosen, the certificate and private key can be imported onto the Exinda appliances using the form below.



Name	Optionally specify a name to give the certificate. If no name is specified, the filename of the certificate is used. Private keys are stored separately to certificates and are automatically named the same as the certificate, with '_key' appended to the end.
Certificate/Key Format	Select the certificate/private key format. Currently, PKCS#12 and PEM formats are supported. If PEM is selected, an additional upload field is exposed so that the private key can be uploaded with the certificate.
Key Passphrase	If the certificate/private key is password protected, specify the password here.
Certificate File	Select the PKCS#12 certificate to upload to the Exinda appliance.
Key File	If PEM is selected, select the private key to upload to the Exinda appliance.

Once certificates and keys have been uploaded, they are displayed in a table at the top of the page. Here, you can view the certificate contents and also permanently delete them from the Exinda appliance.

Note: Certificates and keys are stored securely on the Exinda appliance. It is not possible to export/view the private key once it's been imported. If you loose the configuration, or need to migrate the configuration to another appliance, you will need to manually load the private key again.

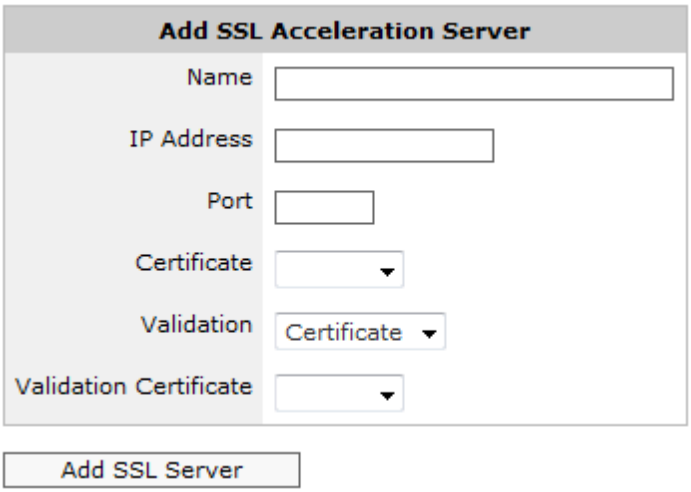
Certificates and keys can also be configured using the CLI `crypto certificate` commands.

3.2 Configuring Servers

The next step to configuring SSL Acceleration is to specify the SSL accelerated servers. This can be done using the form on the System | Acceleration | SSL page on the Web UI, advanced mode.

Note: Only servers that are explicitly configured will be SSL accelerated. Any SSL traffic that the Exinda appliance sees that does not belong to a configured server will be ignored.

Using the form below, you can add SSL Acceleration servers. This will need to be done on all Exinda appliances.



Name	Specify a name for the server/application you wish to enable for SSL Acceleration.
IP Address	Specify the IP address of the server running the SSL enabled application.
Port	Specify the port number running the SSL enabled application on the server.
Certificate	Select the Certificate to use for re-encryption of the SSL session. The certificates available here are those that are configured in the Certificate and Key Management section.
Validation	Select the type of validation to apply to the server's certificate. Options are None, Certificate or Reject. • **None** means that SSL Acceleration will accept and process the connection even if the server's SSL certificate is invalid or expired.

	• **Reject** means that SSL Acceleration will not process the connection if the server's SSL certificate is invalid or expired. The connection will still be accelerated, but not SSL accelerated. • **Certificate** means that SSL Acceleration will accept and process the connection only if the server's certificate matches the validation certificate, specified below. Otherwise, the connection is not processed.
Validation Certificate	If 'Certificate' is selected as the validation method above, this is the certificate that's used to validate against the server's certificate.

Once the SSL accelerated servers have been configured, they will be listed in the table at the top of this page. Here you can edit and delete individual servers.

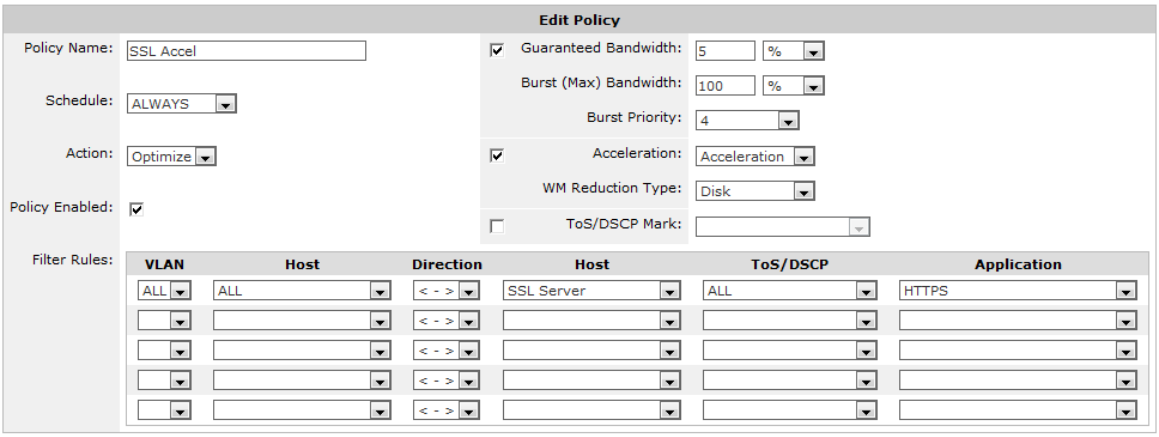
Note: If there are any problems with the certificate or key associated with a configured SSL server (E.g. missing key, expired certificate), then SSL Acceleration will ignore that traffic until the issue is resolved.

SSL accelerated servers can also be configured using the CLI `acceleration ssl` commands.

3.3 Creating Policies

The final step to configuring SSL Acceleration is to create an acceleration Policy in the Optimizer for the SSL server/application you want to accelerate. By default, SSL traffic is captured by a QoS only Policy, meaning no attempt is made to accelerate any SSL traffic by default.

Below is an example of a policy that accelerates an SSL application. This Policy is placed above any other Policy that captures SSL traffic in the policy tree.



Once these desired Policies are in place on all Exinda appliances, restart the Optimizer. Any SSL traffic that matches an acceleration policy will be passed to SSL Acceleration. If a valid certificate and key are configured for that SSL traffic, then SSL Acceleration will occur.

Part IV

4 Appendix A: Supported Ciphers

SSL Acceleration supports the following ciphers.

Protocol	Key Length	Cipher Name
SSLv3	256 bits	AES256-SHA
SSLv3	128 bits	AES128-SHA
SSLv3	168 bits	DES-CBC3-SHA
SSLv3	128 bits	RC4-SHA
SSLv3	128 bits	RC4-MD5
TLSv1	256 bits	AES256-SHA
TLSv1	128 bits	AES128-SHA
TLSv1	168 bits	DES-CBC3-SHA
TLSv1	128 bits	RC4-SHA
TLSv1	128 bits	RC4-MD5

If the client does not support any of these ciphers, the SSL connection is rejected.

If the server does not support and of these ciphers, it is automatically removed from SSL Acceleration and any connections to this server will not be accelerated.