Exinda How To Guide:

Edge Cache

exinda.

Copyright

Document Built on Tuesday, December 23, 2014 at 11:16 AM

Documentation conventions

- **bold** - Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
- *italics* - Reference to other documents. For example: Refer to the *Exinda Application List*.
- **>** - Separates navigation elements. For example: Select **File > Save**.
- `monospace text` - Command line text.
- `<variable>` - Command line arguments.
- `[x]` - An optional CLI keyword or argument.
- `{x}` - A required CLI element.
- `|` - Separates choices within an optional or required element.

Table of Contents

How Edge Cache Works

Edge Cache enables single-sided caching of Internet-based content, including web objects, videos and software updates. Edge Cache requires only one Exinda appliance.

When web objects are downloaded from the Internet or across WAN links, Edge Cache stores them at the network's edge. When subsequent requests come for the same material, the content is quickly delivered from Edge Cache, without the need to re-download the data over the WAN. The result is the ability to experience LAN speeds of WAN objects, and provide users with a better network experience.

Edge Cache also supports HTTPS sites allowing the appliance to be a forward proxy and decrypt content for caching. This is important as more and more applications and services are moving to the cloud. These SaaS-based applications are typically delivered over HTTPS and so to be effective, Edge Cache must support caching this HTTPS traffic.

Edge Cache also offers cache statistics, which provide insight into the amount of repetitive data being off-loaded from the WAN link, how cacheable the network data is, and how frequently the cache is being accessed.

Caching Internet-based Content

To cache web traffic, a client-side Exinda appliance is put in line to the traffic. When a network user visits a URL with cacheable content, Edge Cache first determines if the content is available in it's cache. If not, Edge Cache retrieves the content from the URL. Upon retrieving the content, it is stored in the cache with its expiry date as specified on the source website. This assumes that the content is cacheable and falls within the Edge Cache setting parameters, such as size of object and whether the URL was blacklisted. The next time a network user visits the same URL, Edge Cache determines that the content is available in the cache and that the content is not stale by looking at the object's expiry date. The content is then served to the client from the cache, rather than retrieving from the URL over the WAN.

Edge Cache uses a least recently used (LRU) algorithm for expiring cached data to make room for new objects. This means the most popular and most used content is stored the longest. You also have the ability to manually clear the entire cache if desired.

Edge Cache operates as a transparent proxy since it is running on an inline device. As a result, your browsers do not need to be configured with an explicit proxy configuration.

Caching Encrypted Internet-based Content

Version Info: As of version 7.0.2, Edge Cache can cache HTTPS content, as well as HTTP content.

When the network user visits an HTTPS URL, if HTTPS caching is not enabled, Edge Cache is unable to determine what is being requested because the traffic is encrypted, including the URL being requested. Even if it

could cache the encrypted data, the next request for the same HTTPS URL would not contain the same cached data because the encryption pattern would be different. By enabling HTTPS caching, Edge Cache is able to act as a forward proxy, and retrieve the content from the server, decrypt it, and provide it to the client over an encrypted communication channel. Later requests can then be served from the cache.

To support this feature, you will need to upload a trusted certificate to the appliance, which will be used by Edge Cache to sign all dynamically generated site certificates. All client devices must trust this certificate as a signing authority.

To cache encrypted web traffic, the client tries to communicate with the HTTPS web server. The Exinda appliance intercepts, keeping the communication open with the client. Then Edge Cache tries to establish a conversation with the server. Upon receiving the certificate details from the server, Edge Cache extracts the certificate details, constructs a new certificate and signs it using the signing certificate that was loaded and specified in the Edge Cache settings. Edge Cache then presents this new certificate to the client. The client trusts this certificate because the details match its HTTPS URL request and the client has previously been told to trust anything signed by this signing certificate (see below). The communication negotiation between the client and Edge Cache is now complete. The client then requests the specific web object from Edge Cache as if it were the server. Edge Cache then requests the web object from the server over its previously established trusted connection. The server provides the content to Edge Cache, which then stores the content, if applicable. The connection with the server can be closed. Edge Cache then serves the content to the client and the connection with the client can then be closed.
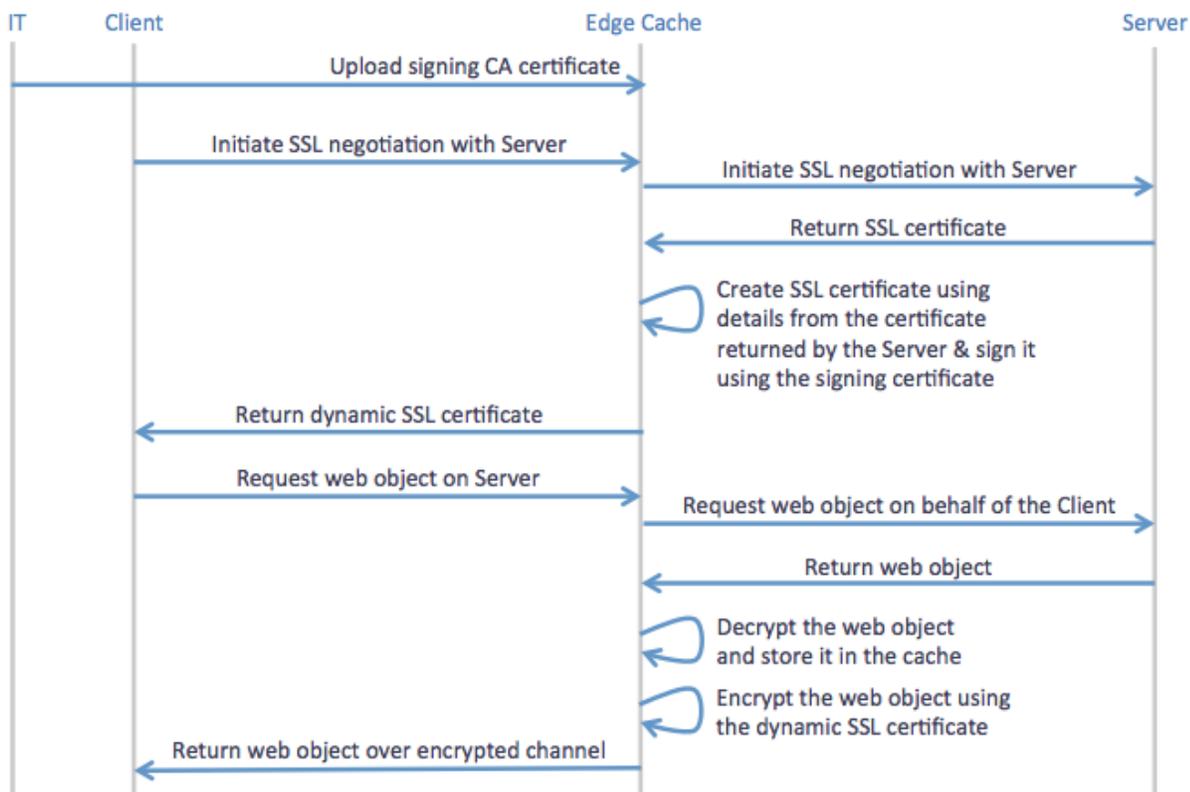

Figure - Sequence of operations for caching encrypted traffic using Edge Cache

When determining whether the content should be stored in the cache, Edge Cache evaluates whether it's the appropriate size and whether it's whitelisted or blacklisted. The whitelist and blacklist can consist of source IP, destination IP, source domain, and destination domain. Note the domains are resolved using DNS, then the resulting IPs are reverse mapped to determine the domain that is used to configure the Edge Cache engine.

The next time a client requests the same content, the same negotiation happens where the client requests a secure communication channel with the server, the Exinda appliance intercepts and forms a secure communication channel with the server, forges the certificate and establishes a secure communication channel with the client (on behalf of the server). The client then requests the specific web content. Edge Cache determines that the requested content is available in cache and serves it to the client. It then closes the communication channels with both the server and the client.
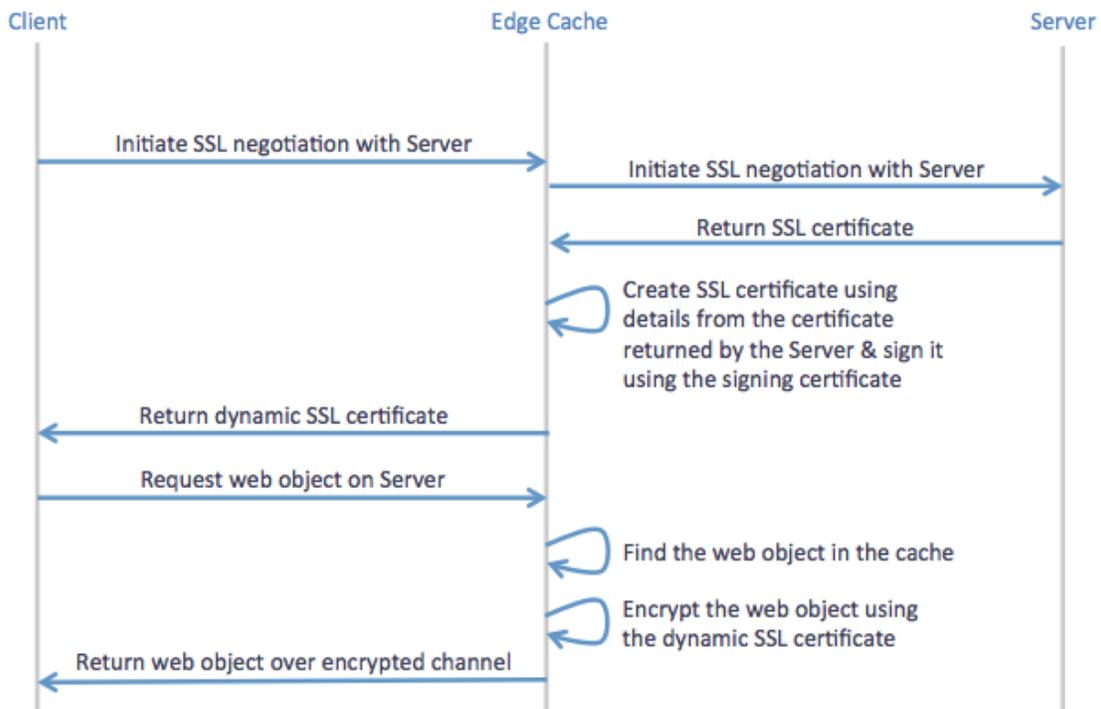
Figure - Sequence of operations for use of previously cached objects from encrypted sites using Edge Cache

Licensing

The Edge Cache Acceleration feature is a separately licensed component. To see if you are licensed for Edge Cache, go to **Configuration > System > Setup > License**. You are licensed for Edge Cache, if the **Max Edge Cache Connections** is listed and is greater than 0. For more details about licensing, see *Licensing* in the main user guide.

Please contact your local Exinda representative if you wish to enable this feature.

Overview - Configuration & Usage

To use Edge Cache,you'll need to ensure all the required configuration is set.

- Configure the Edge Cache settings, including

    - indicating what size of objects you want to cache

    - specifying how long you are willing to let Edge Cache wait for a response from the WAN when fetching objects

    - specifying the signing certificate and private key if you plan to cache content from HTTPS sites

    - specifying blacklisted sites to not cache

    - or specifying to only cache whitelisted sites (for HTTPS sites only)

    - clearing out the cache, if desired.

> **Version Info:** Before version 7.0.2, Edge Cache requires you to restart the Edge Cache process after making any modifications to the Edge Cache configuration. With 7.0.2 and later, the Edge Cache process will automatically restart when needed.

For more details, see Edge Cache Configuration.

- You also need to ensure that the DNS server configuration information is set. See DNS Configuration.

- For HTTPS caching, you need to ensure that the certificate used for HTTPS caching is trusted by your clients.

- If you have an upstream proxy in your environment, you can configure it as a proxy peer to ensure that Edge Cache can fetch content from the internet.

- You can add one or more Edge Cache policies to a virtual circuit in the Optimizer.See Creating an Edge Cache Policy in the Optimizer.

- Since the appliance has dynamic disk partitioning, if needed, you can increase the cache storage capacity dynamically. See *Allocate Disk Storage for System Services* in the main user guide.

Once Edge Cache is configured and started, you can monitor the caching performance.

- You can look at the Edge Cache monitor to determine the reduction ratio or throughput comparing the LAN (cached and non-cached) data to the WAN (non-cached) data. The Edge Cache monitor will also report the requests per second versus the hits per second, where hits are the number of requests that could be satisfied by cached content. These charts can look at long term historical caching or can be as little as the last 5 minutes with 10 second samples. See Edge Cache Report.

- You can also look at the Real Time page to see which conversations are passing through Edge Cache. The conversations with a blue background indicate that the flow passed through Edge Cache, however, it does not necessarily mean that any of the requests were satisfied by cached content. See Monitor Edge Cache Traffic in Real Time.

Configuring Edge Cache

You need to ensure that DNS is properly configured. You'll also need to create one or more Edge Cache policies in the Optimizer, and configure the Edge Cache settings. If you expect to cache encrypted traffic, you'll need to prepare a trusted certificate for Edge Cache to use to re-encrypt the traffic and distribute that trusted certificate to all of your client machines.

Preparing & Trusting a Certificate for Encrypted Traffic

When caching encrypted content, you need to specify a certificate that Edge Cache will use to create and sign a dynamically created certificate on behalf of the server. You will need to ensure that this certificate is trusted by all the computers on your network that will have traffic that passes through Edge Cache. It is recommended that you create a self-signed CA certificate (as opposed to a self-signed certificate without the CA designation) to simplify loading and trusting the certificate by the computers in your network.

How to create a self-signed CA certificate for Edge Cache to use

When using Edge Cache for encrypted traffic, you must create and import a signing certificate in the **Certificates and Keys** store. This certificate and its corresponding key will be used by Edge Cache to generate and sign dynamic SSL certificates for proxied sites. For all practical purposes, this certificate becomes a root certificate and you become a Root CA.

To create a CA certificate and private key using OpenSSL

Use the following OpenSSL commands:

```
openssl genrsa -out myCompanyCA.key 2048

openssl req -x509 -new -key myCompanyCA.key -out myCompanyCA.cer -days 1000

-subj /CN="myCompany CA"
```

This will generate two files: a.key file and a .cer file that can be uploaded in the CA certificates UI.

To import your CA certificate and private key to the appliance's Certificates and Keys store

Import Certificate and Key Details

Name   [   ] (optional)

Certificate/Key Format   ◉ PKCS#12
                       ○ PEM

Key Passphrase   [   ] (optional)

Certificate File   [Choose File] no file selected

Private Key File   [Choose File] no file selected (optional)

[Import]

Figure - Import certificate in CA Certificates store

1. Go to **Configuration > System > Certificates > CA Certificates**.

2. Select the **Import Certificate** radio button.

3. (Optional) Type a **Name** for the certificate. If no name is specified, the filename of the certificate is used.

   Private keys are stored separately from certificates, and are automatically named the same as the certificate, with '_key' appended to the end.

4. Select the **Certificate/Key Format**.

   - **PKCS#12**—Format used when the certificate and key are stored together, and usually have extensions such as `.pfx` and `.p12`..

   - **PEM**—Common format for certificates issued by Certificate Authorities. PEM certificates usually have extentions such as `.pem`, `.crt`, `.cer`, and `.key`. If PEM format is selected, an additional upload field is exposed so that the private key can be uploaded with the certificate.

5. If the key is password protected, in the **Key Passphrase** field type the password.

6. In the **Certificate File** field, click **Choose File** and navigate to the file to be uploaded to the appliance.

7. If the PEM format is selected, the private key must be uploaded. In the **Private Key File** field, click **Choose File** and navigate to the private key file.

8. Click **Import**.

   The certificates are displayed in the **Certificates and Keys** table on the CA Certificates and Keys table on the CA Certificates tab. From the tables the contents of a certificate can be viewed, or the certificate can be deleted or exported.

How to tell client computers to trust the installed certificate

If the browsers in your network don't trust the certificate, you may get a warning or the sites may fail to load. In this case, each computer needs to import the certificate so that the certificate will be trusted when negotiating with Edge Cache over SSL.

You will need to export the certificate from the appliance and import it to the desired computers.

To export the certificate from the appliance

1. Go to **Configuration > System > Certificates > CA Certificates** and find your desired certificate in the list.

2. Export the certificate by clicking the **Export** button.

3. Ensure that the Export **Certificate Format** is set to **PEM**.

   The PEM format encodes the certificate and private key. It may include an entire certificate chain including public key, private key, and root certificates.

4. Click the **Save** button.

To use a domain controller to deliver and install the certificate on Windows machines across your network

It is recommended that you follow the instructions provided by Microsoft:

http://technet.microsoft.com/en-us/library/cc772491.aspx

> **Note:** These instructions assume that you are using a domain controller or a workstation running the domain admin MMC snapins while logged into a domain as a domain admin. Some of the elements that are referred to in the instructions won't exist if you a using Windows Server 2008 R2.

To import the certificate into a Mac's Keychain Access program

To install a certificate, you must use the **Keychain Access** program. To start the **Keychain Access** program,double-click certificate file.

If you are importing a CA certificate:

1. Double-click the exported PEM file for the CA certificate to start the Keychain Access program.

2. When prompted, enter your computer's admin password.

3. The **Keychain Access** window appears.

   The certificate has automatically been installed with no additional steps.

If you are importing a non-CA certificate:

1. Double-click the exported PEM file for the non-CA certificate to start the Keychain Access program.

2. When prompted, enter your computer's admin password.

3. In the **Keychain Access** window, select the **System** keychain to install for all users on the machine, or **Login** keychain to install only for the current user account.

4. Find the desired certificate in the list and right-click and select **Get Info**.

5. In the **Trust** section, select **Always Trust** for the **When using this certificate** drop-list.

Configuring DNS

If DNS is not configured, Edge Cache will not work properly. That is the DNS server(s) must either be specified on **Configuration > System > Network > DNS** or by selecting **DHCP** on **Configuration > System > Network > IP Address**.

The user interface will not allow you to get into a state where DNS is not configured when using HTTPS Caching. For instance, if DNS is not configured, then a warning will be shown next to the **HTTPS Caching** section and the enable checkbox will be disabled. Also if HTTPS Caching and DNS are configured, and you attempt to remove DNS configuration, then the system will warn you and prevent you from making the change.

> ⚠️ **Caution:** The system does not prevent using non-encrypted caching when DNS is not configured. In this case, the system will not warn you and Edge Cache will fail. The logs will report the issue.

To learn more about configuring DNS. See *DNS and Domain Names Configuration* in the main user guide.

Configuring Edge Cache

When web objects are downloaded from the Internet or across WAN links, Edge Cache stores them at the network's edge. When subsequent request come for the same material, the content is quickly delivered from Edge Cache, without the need to re-download the data over the WAN. Edge Cache can cache web objects, videos, software updates, and other content on the WAN. You can control whether to exclude particular sources, or sizes of objects from being cached. The cache objects can also be shared amongst peer appliances if desired, that is if the content cannot be found in the cache of the appliance that the traffic is passing through, then the appliance can request the content from peer appliances. You are also able to clear out the cache, if desired.

You may want to limit the size of objects that can be cached. Since the cache storage size is limited, you may want to decide whether to allow few large objects or lots of little objects. You should ensure that the size is aligned with the types of objects that you want to be cached. For example, iOS updates tend to be approximately 1 GB and Mac updates tend to be 6 GB and so if you want Edge Cache to help with caching of these updates, you'll want to ensure that the minimum and maximum allowed objects size accommodates these sizes.

You may want to blacklist particular sites if Edge Cache is not working properly and is preventing the network user from getting access to the site. Also, you may want to blacklist secure sites because you don't want to cache sensitive data such as financial or banking sites. Alternately, if you want to only cache particular secure sites once they've been identified as important sites or the most impactful to your network, you can whitelist them such that only those sites listed will be cached. Whitelisting is only available for HTTPS caching. You can specify your whitelist and blacklist as source IP, destination IP, source domain, or destination domain. Domains are resolved using the DNS.

To use HTTPS caching, you will need to specify which signing certificate will be used by Edge Cache to generate a certificate to negotiate with the client on behalf of the server.

Version Info: Before version 7.0.2, Edge Cache requires you to restart the Edge Cache process after making any modifications to the Edge Cache configuration. With 7.0.2 and later, the Edge Cache process will automatically restart when needed.

Note: Objects in the traffic that are matched with an Edge Cache policy but are excluded from storage in Edge Cache due to these settings, will still pass through Edge Cache unprocessed and will be highlighted on the Real Time conversations screen in blue (indicating that they passed through and were evaluated by Edge Cache).

Where do I find this functionality?

Go to **Configuration >System > Optimization > Edge Cache**.

To set the range of object size that you would like to cache

Memory Object Options

Min Object Size	0	kB
Max Object Size	8190000	kB
Connection Timeout	20	seconds

Apply Changes

Figure - Setting the size of the objects that can be cached

1. In the **Memory Object Options** area, type the minimum and maximum size of the objects to be cached.

   Only objects that are within this size range will be stored in Edge Cache.

2. Click the **Apply Changes** button.

   Version Info: Before version 7.0.2, you will need to restart Edge Cache for the changes to take effect. Go to **Configuration > System > Optimization > Services**, and click the Edge Cache **Restart** button.

To set the fetch connection timeout

Memory Object Options

Min Object Size	0	kB
Max Object Size	8190000	kB
Connection Timeout	20	seconds

Apply Changes

Figure - Setting the connection timeout

1. In the **Memory Object Options** area and in the **Connection Timeout** field, type the maximum time in seconds that the Edge Cache will wait for a response from the WAN when fetching objects.

   You may need to increase this if connection timeouts are occurring regularly. Browsers typically return a message similar to the following when this occurs: `(110) Connection timed out`

2. Click the **Apply Changes** button.

   > **Version Info:** Before version 7.0.2, you will need to restart Edge Cache for the changes to take effect. Go to **Configuration > System > Optimization > Services**, and click the Edge Cache **Restart** button.

To blacklist certain HTTP URLs to never cache

URL	Delete
docs.exinda.com	Delete

Add URL/Domain

URL	

Add URL

Figure - HTTP caching with blacklisted sites

1. In the **Add URL/Domain** area, type the HTTP URL or domain that will be excluded from the Edge Cache.

2. Click the **Add URL** button.

3. Repeat until you have your desired blacklist.

4. Remove an HTTP URL or domain from the list by clicking the **Delete** button for the specified URL/domain.

> **Version Info:** Before version 7.0.2, you will need to restart Edge Cache for the changes to take effect. Go to **Configuration > System > Optimization > Services**, and click the Edge Cache **Restart** button.

To blacklist certain (encrypted) HTTPS URLs to never cache

All https traffic can be cached according to the policy except those sites listed in the blacklist.

Figure - Enabling HTTPS caching with blacklisted sites

1. In the **HTTPS Caching** area, select the **Enable caching of HTTPS content** checkbox.

   Note: You will not be able to enable caching if DNS is not configured.

2. Select the **signing certificate** to use to re-sign the traffic.

3. Select **Attempt to cache all HTTPS sites except for blacklisted exceptions** from the drop-list.

4. Click the **Apply Changes** button.

5. In the **Add IP or Domain** area, specify the type of traffic you want to blacklist and the **Value**(IP or domain name) for that type of traffic.

   You can specify **Source IP**, **Destination IP**, **Source Domain**, or **Destination IP**.

   Domains are resolved using the DSN. Ensure the domains are in the format that are required by DNS (i.e. without https://).

   The specified domain name is resolved to an IP address, then the IP address is reverse mapped to the actual domain name that corresponds to that IP address. Note that the domain name may resolve to multiple IP addresses and multiple other domain names.

6. Click the **Add URL** button.

7. Repeat until you have your desired blacklist.

   The blacklist will take effect immediately as Edge Cache will automatically be restarted.

8. Remove an HTTPS URL or domain from the list by clicking the **Delete** button for the specified URL/domain.

To only allow specified whitelisted (encrypted) HTTPS URLs

Only https traffic specified in the policy and in this whitelist will be cached.

HTTPS Caching

Enable caching of HTTPS Contents   ☑

Signing Certificate   edge-cache-cert ⬍

HTTPS Site Exceptions   ⦿ Only allow specified (whitelisted) HTTPS sites to be cached

    ◯ Attempt to cache all HTTPS sites except for blacklisted exceptions

Apply Changes

Configure which HTTPS URL/Domains can be cached

Type	Value	Delete
Destination IP	106.21.113.215/32	Delete
Destination Domain	www.youtube.com	Delete

Add IP or Domain

Type   Source IP ⬍   Value [ ]

Add To List

Figure - Enabling HTTPS caching with whitelisted sites

1. In the **HTTPS Caching** area, select the **Enable caching of HTTPS content** checkbox.

   Note: You will not be able to enable caching if DNS is not configured.

2. Select the **signing certificate** to use to re-sign the traffic.

3. Select **Only allow specified whitelisted HTTPS sites to be cached** from the drop-list.

4. Click the **Apply Changes** button.

5. In the **Add IP or Domain** area, specify the type of traffic you want on the whitelist and the **Value** (IP or domain name) for that type of traffic.

   You can specify **Source IP**, **Destination IP**, **Source Domain**, or **Destination IP**.

   Domains are resolved using the DSN. Ensure the domains are in the format that are required by DNS (i.e. without https://).

The specified domain name is resolved to an IP address, then the IP address is reverse mapped to the actual domain name that corresponds to that IP address. Note that the domain name may resolve to multiple IP address and multiple other domain names.

6. Click the **Add URL** button.

7. Repeat until you have your desired whitelist.

   The whitelist will take effect immediately as Edge Cache will automatically be restarted.

8. Remove an HTTPS URL or domain from the list by clicking the **Delete** button for the specified URL/domain.

To not blacklist or whitelist any URLs

1. Set the blacklist mode, but don't add any URLs.

   This allows all sites to be cached except those listed. Since the list is empty, all sites are allowed.

To clear the Edge Cache cache

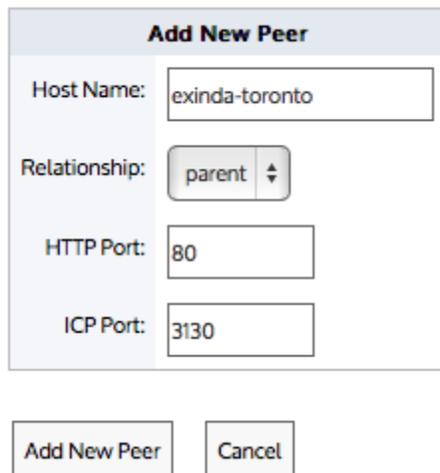The **clear** action removes all objects from the memory.

Clear

1. Click the **Clear** button.

   This removes all objects from storage.

To manage with which appliance peers to share Edge Cache content

When Edge Cache appliance peers are specified, if the requested content is not available in the appliance's cache, Edge Cache can request the content from it's appliance peers.

Add New Peer

Host Name: exinda-toronto

Relationship: parent

HTTP Port: 80

ICP Port: 3130

Add New Peer   Cancel

Figure - To add a new peer appliance for Edge Cache

Add New Peer

Host Name	Type	HTTP Port	ICP Port	Edit	Delete
exinda-toronto	parent	80	3130	Edit	Delete

Figure - Peer appliances for Edge Cache

1. Click the **Add New Peer** button.

   An **Add New Peer** screen appears.

2. Type the **Host Name** of the peer.

3. Select the **Relationship** with the peer.

4. Type the **HTTP Port** of the new peer.

5. Type the **ICP Port** of the new peer.

6. Click the **Add New Peer** button.

   The peer appears in the list of configured peers.

7. Peers can be edited or deleted by clicking the **Edit** or **Delete** button for the specified peer.

Creating an Edge Cache Policy in the Optimizer

Edge Cache works on outbound, HTTP based conversations (and HTTPS based conversations, for version 7.0.2 and later). To enable Edge Cache, create a policy that will capture the HTTP application traffic that you wish to cache and add the policy to the appropriate virtual circuit in the Optimizer. You can specify a subset of the network to use Edge Cache by specifying the source network object.

> ⚠️ **Caution:** You can create an Edge Cache policy on anything except a L7 signature. That is, you can set the policy filter using VLAN, source and/or destination network objects, ToS/DSCP, or applications that are based on protocol, ports, network objects, or DSCP.

To learn more about configuring policies, see *Policy* in the main user guide.

Edit Policy

Policy Name:	Cache Web for Marketing		☐ Guaranteed Bandwidth:	128	kbps
Schedule:	ALWAYS		Burst (Max) Bandwidth:	2048	kbps
Action:	Optimize		Burst Priority:	1 (High)	
Policy Enabled:	☑		☑ Acceleration:	Edge Cache	
			☐ Packet Marking		

Filter Rules:	VLAN	Source	Direction	Destination	ToS/DSCP	Application
	ALL	Marketing	Both	ALL	ALL	HTTP
	ALL	Marketing	Both	ALL	ALL	HTTPS
			Both			
			Both			
			Both			
			Both			

To create an Edge Cache policy

1. Click **Optimizer > Policies > Create New Policy** or click **Create New Policy** in the appropriate virtual circuit.

2. Type a name for the policy.

3. Select the **Acceleration** checkbox and select **Edge Cache** from the Acceleration list.

4. Create the filter rules for the policy, ensuring that HTTP (or HTTPS) or an application based on protocol, port, network object, or dscp is selected from the application list.

5. Click **Add New Policy**.

To apply Edge Cache to a subset of the network

1. When creating the policy, specify a network object as the source in the policy filter.

2. Click **Add New Policy**.

   Only the traffic in that source network object will use Edge Cache.

Reporting

You can see the effectiveness of Edge Cache by either looking at the Edge Cache monitor or by looking at Real Time conversations.

Edge Cache Report

The Edge Cache Report shows the amount of traffic reduction achieved due to caching techniques and the number of requests and the number of hits from the cache. These charts can answer questions such as, "How much traffic reduction am I getting due to Edge Cache?" "How cacheable is the network data and how frequently is the cache being accessed?"

The chart can show the traffic reduction over time as either throughput or percentage reduction. The reported LAN throughput is the amount of traffic that was served to the client whether it was served from Edge Cache or not. This represents all traffic that was handled by Edge Cache policies. The reported WAN throughput is the amount of traffic that was not available in Edge Cache and needed to be retrieved from the application server. Therefore, the difference between WAN and LAN is the amount of traffic that could be served from Edge Cache.

When reduction statistics are displayed as throughput, there is one time series plotted for LAN throughput and one for WAN throughput. You should expect the LAN throughput to be higher than WAN throughput. When the LAN throughput is greater than the WAN throughput, the more traffic was served up from Edge Cache than was needed to be retrieved from the WAN.
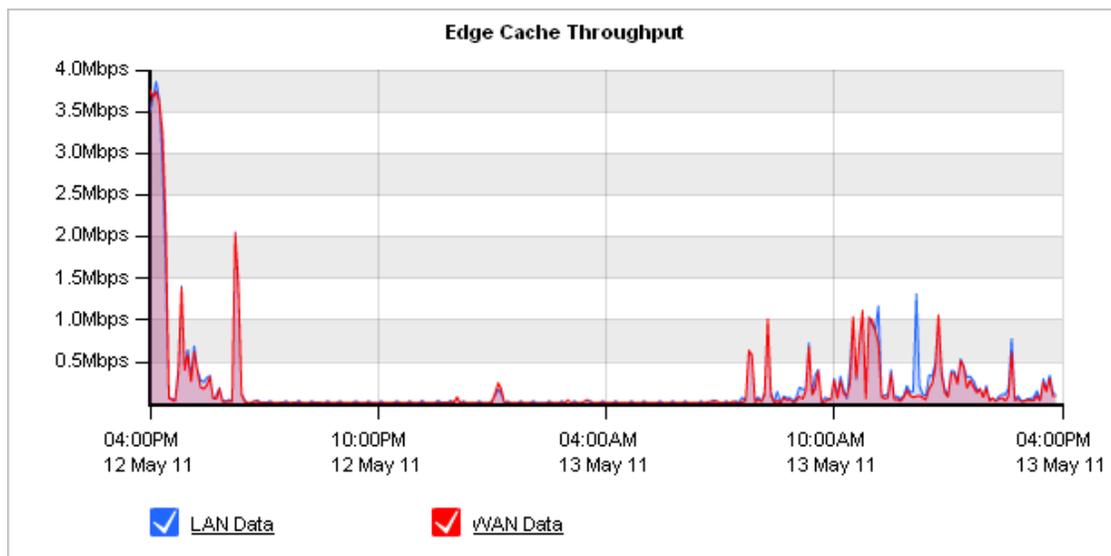
When displayed as percentage reduction, it displays one line graph to represent the percentage of data transferred that was sent from Edge Cache instead of from the application server.
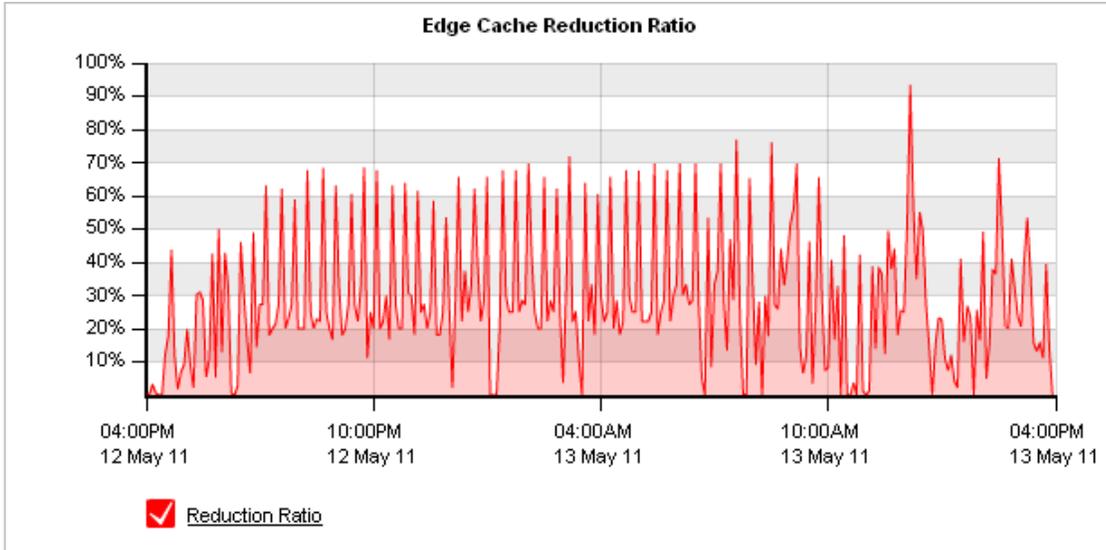
The Edge Cache Statistics chart display the number of requests per second and the number of hits per second. A request occurs when Edge Cache is checked for particular data. A hit occurs when a request is satisfied by an object already stored in the Edge Cache.
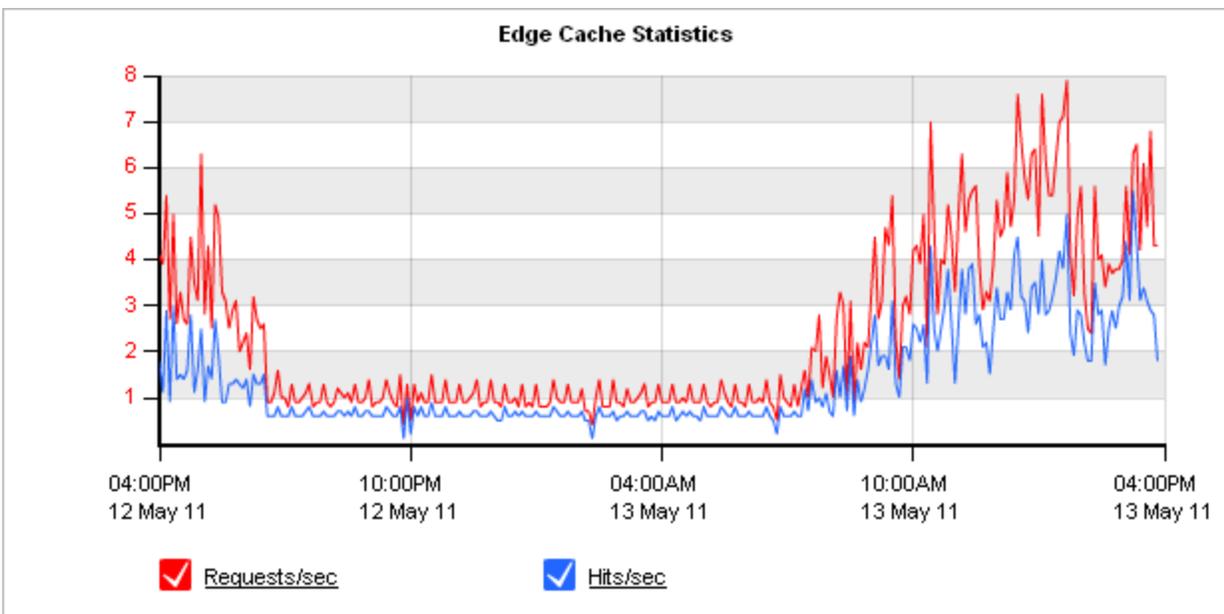
The table shows a summary of Edge Cache reduction for the selected time period.

LAN (MB)	WAN (MB)	Reduction Ratio (%)		Requests	Hits	Hit Ratio (%)	
2138.61	1930.90		9.71	204030	120030		58.83

Where do I find this report?

Go to **Monitor > Optimization > Edge Cache**.

How do I change the Edge Cache Throughput chart to a Edge Cache Reduction Ratio chart?

Select the desired type of chart from the Edge Cache Graph Type selector below the chart.

How is the Edge Cache Reduction Ratio calculated?

```
Reduction Ratio = (Data Transfer Size Before Exinda - Data Transfer Size After
Exinda) / Data Transfer Size Before Exinda
```

Monitor Edge Cache Traffic in Real Time

The Conversations in Real Time monitor shows the top conversations by throughput observed by the Exinda appliance during the last 10 seconds. This report can answer questions such as, "Is the traffic being processed by Edge Cache properly?"

The Conversations in Real Time monitor shows inbound conversation traffic separately from outbound conversation traffic.The conversations are represented as external IP, internal IP, and application. For HTTP or HTTPS, the URL will appear in square brackets following the application. The traffic is sorted by transfer rate. The packet rate and number of flows for each conversation in that 10 second period is also shown. You can set the chart to refresh frequently or infrequently or not at all. Each refresh shows 10 seconds of data.

	External IP	Internal IP	Application	Transfer Rate (kbps)	Packet Rate (pps)	Flows
Inbound Conversations						
	Total			**1408.428**	**284**	**24**
	192.168.10.1	192.168.10.128	MAPI	570.834	82	1
	192.168.10.9	192.168.10.128	MAPI	483.247	54	2
	192.168.10.7	192.168.10.128	MAPI	275.334	92	2
	192.168.10.10	192.168.10.128	MAPI	65.153	51	2
	192.168.10.7	192.168.10.128	HTTPS[perf-win2k8]	5.496	1	1
	192.168.10.9	192.168.10.128	LDAP	2.939	1	1
	10.20.4.1	239.255.255.250	udp ports 62612 -> 3702	1.097	0	1
	10.20.4.1	239.255.255.250	udp ports 62610 -> 3702	1.069	0	1
	192.168.10.1	192.168.0.1	NetBIOS	0.623	1	1
	192.168.10.10	192.168.10.128	LDAP	0.556	0	2
	192.168.10.132	255.255.255.255	DHCP	0.541	0	1
	192.168.10.9	192.168.0.1	NetBIOS	0.225	0	1
	10.20.3.118	10.20.255.255	NetBIOS	0.225	0	1
	192.168.10.9	192.168.255.255	NetBIOS	0.225	0	1
	10.20.11.100	224.0.0.252	udp ports 58633 -> 5355	0.212	0	1
	10.20.0.14	10.20.255.255	NetBIOS	0.193	0	1
	192.168.10.9	192.168.10.128	LDAP	0.174	0	1
	192.168.10.1	192.168.10.128	MSRPC	0.106	0	1
	192.168.10.9	192.168.0.1	DNS	0.102	0	1
	10.20.0.181	10.20.255.255	NetBIOS	0.075	0	1

When a conversation has been processed by Edge Cache, it is highlighted in blue.

74.125.237.41	172.16.0.96	HTTP[books.google.com]	0.366

Note that all conversations that are evaluated by Edge Cache will be highlighted in blue even if the object is excluded from storage in Edge Cache due to Edge Cache settings.

To learn more about this monitor, see *Conversations in Real Time* in the main user guide.

Troubleshooting Edge Cache

I don't know if Edge Cache is caching any traffic

- You can determine if any traffic is passing through Edge Cache by looking at the real time conversations monitor available at **Monitor > Real Time > Conversations**.

  Any traffic that is currently being processed by Edge Cache will have a blue background. This will tell you if Edge Cache is evaluating whether data could be retrieved from its cache or evaluating whether the data should be stored in it. However, it does not indicate whether it is successful in either retrieving or storing the data.

- You can determine if any traffic has passed through Edge Cache over time by looking at the Edge Cache report available at **Monitor > Optimization > Edge Cache**.

  The Edge Cache monitor report will show the amount of data over time processed through Edge Cache served on the LAN and the amount of data retrieved from the WAN. It will also show the requests to Edge Cache and the hits. These two charts will show you if data is going through Edge Cache and if so how many hits and how much data is served from the cache.

- Check the logs for any errors related to Edge Cache, including DNS not being configured.

- You should ensure that DNS is configured properly by visiting **Configuration > System > Network > DNS**. For help configuring DNS, see the main user guide.

- If the Real Time monitor and the Edge Cache monitor indicate that data is not passing through Edge Cache, you should ensure that the Edge Cache process is running.

  Go to **Configuration > System > Optimization > Services** and ensure that Edge Cache is running. You may want to restart Edge Cache.

I don't know if Edge Cache is caching encrypted traffic

- All the steps for troubleshooting caching above apply.

- Try browsing to an encrypted site then look at the real time conversations. The encrypted traffic will be reflected in the application name, such as HTTPS. If processed through Edge Cache, the conversation will have a blue background.

- Ensure HTTPS caching is enabled and a certificate is configured.

- If the traffic that you are concerned about is specified in a caching whitelist or blacklist using source or destination domains, then try restarting Edge Cache at **Monitor > Optimization > Services**. If the reverse mapped domains have changed, then the domains that are specified in the whitelists and blacklists may need to be re-resolved and re-reverse mapped. This is done upon Edge Cache startup, when there is a change to the whitelist or blacklist, or when there is a change to the DNS information.

I want to increase the effectiveness of Edge Cache

- You can restrict the size of the objects that can be cached to more closely match the type of data that you want cached by visiting **Configuration >System > Optimization > Edge Cache**.

- You can increase the amount of storage available for Edge Cache to use by visiting **Configuration >System > Setup > Storage**.

Command Line Interface (CLI)

Edge Cache can be configured via CLI, such as configuring the Edge Cache settings including specifying the object size to cache, cache timeout, blacklists and whitelists, and specifying upstream peers. You can also import your CA certficates via CLI.

CLI: Edge Cache Acceleration

You can use the `acceleration edge-cache` command to configure Edge Cache acceleration. Edge Cache enables single-sided caching of Internet-based content, including web objects, videos and software updates. Edge Cache requires only one Exinda appliance.

When web objects are downloaded from the Internet or across WAN links, Edge Cache stores them at the network's edge. When subsequent requests come for the same material, the content is quickly delivered from Edge Cache, without the need to re-download the data over the WAN. The result is the ability to experience LAN speeds of WAN objects, and provide users with a better network experience.

Edge Cache also supports HTTPS sites allowing the appliance to be a forward proxy and decrypt content for caching. This is important as more and more applications and services are moving to the cloud. These SaaS-based applications are typically delivered over HTTPS and so to be effective, Edge Cache must support caching this HTTPS traffic.

> **Version Info:** As of version 7.0.2, Edge Cache can cache HTTPS content, as well as HTTP content.

Configuring Edge Cache

```
acceleration edge-cache {administrator-email|application|cache|connect-timeout|enable-
https|https-black-list|https-cert|https-list-type|https-white-list|never-cache|never-
direct|object-size|peer|range-offset}

no acceleration edge-cache {application|enable-https|https-black-list|https-white-
list|never-cache|never-direct|peer}
```

To specify the maximum and minimum size of objects to store:

```
acceleration edge-cache object-size {maximum|minimum> <size>
```

- `<size>` - The size parameter should use SI units e.g. 100M or 512k.

To specify how long Edge Cache should wait for a response when fetching objects from the server:

```
acceleration edge-cache connect-timeout <seconds>
```

To add or remove an HTTP URL or domain that should be blacklisted (i.e. should never be cached):

```
[no] acceleration edge-cache never-cache <URL or domain>
```

To add or remove HTTP applications that should be cached:

```
[no] acceleration edge-cache application <application>
```

- ■ `application <application>` - Note: Only applications that use the HTTP protocol are supported.

To enable [or disable] HTTPS caching:

```
[no] acceleration edge-cache enable-https
```

To specify the signing certificate to use to create dynamic SSL certificates during HTTPS caching:

```
acceleration edge-cache https-cert <cert-name>
```

To specify an HTTPS black-list of IPs or domains:

```
acceleration edge-cache https-list-type black-list
```

- ■ Specifies that Edge Cache will use a black-list for determining what sites can not be cached. All others will be allowed.

```
acceleration edge-cache https-black-list {dest-domain|dest-ip|src-domain|src-ip}
```

- ■ `src-domain <domain>` - The domain that initiated the conversation.
- ■ `src-ip <ip>` - The IP that initiated the conversation. The IP can include a mask.
- ■ `dest-domain <domain>` - The domain that was the destination of the conversation.
- ■ `dest-ip <ip>` - The IP that was the destination of the conversation. The IP can include a mask.
- ■ Note: Domains are resolved using the DSN. Ensure the domains are in the format that are required by DNS (i.e. without https://)

To remove a domain or IP from the black-list:

```
no acceleration edge-cache https-black-list <internal ID>
```

- ■ `https-black list <internal ID>` - To determine the internal ID, type: `no acceleration edge-cache https-black-list ?`, which presents the list of HTTPS black-list sites in the format: Internal ID, Type, Value

To specify an HTTPS white-list of IPs or domains:

```
acceleration edge-cache https-list-type white-list
```

- ■ Specifies that Edge Cache will use a white-list for determining what sites can be cached. No others will be allowed.

```
acceleration edge-cache https-white-list {dest-domain|dest-ip|src-domain|src-ip}
```

- ■ `src-domain <domain>` - The domain that initiated the conversation.
- ■ `src-ip <ip>` - The IP that initiated the conversation. The IP can include a mask.
- ■ `dest-domain <domain>` - The domain that was the destination of the conversation.
- ■ `dest-ip <ip>` - The IP that was the destination of the conversation. The IP can include a mask.
- ■ Note: Domains are resolved using the DSN. Ensure the domains are in the format that are required by DNS (i.e. without https://)

To remove a domain or IP from the white-list:

```
no acceleration edge-cache https-white-list <internal ID>
```

- `https-white list <internal ID>` - To determine the internal ID, type: `no acceleration edge-cache https-white-list ?`, which presents the list of HTTPS whit-list sites in the format: Internal ID, Type, Value

To clear the object cache:

```
acceleration edge-cache cache clear
```

To configure an Edge Cache peer:

If you have an upstream proxy in your environment, you can configure it as a proxy peer to ensure that Edge Cache can fetch content from the internet.

```
[no] acceleration edge-cache peer <hostname> [http-port|icp-port|option]
```

- `<hostname>` - The hostname of the peer object memory.
- `http-port <port>` - The HTTP port for the peer command
- `icp-port <port>` - The ICP port for the peer command
- `option default` - Use the default peer options
- `option proxy-only` - Do not cache objects from this peer.
- `option no-query` - This peer does not support ICP
- `option weight=n` - Specify the peer priority. Peers with higher priority will be consulted first.
- `option round-robin` - Specify that peers should be consulted in round-robin order.
- `option closest-only` - Only forward closest parent ICP misses.
- `option originserver` - Specify that this peer is an origin server

To never fetch a file directly; always use the peer:

```
[no] acceleration edge-cache never-direct
```

To prevent delays when skipping ahead during video downloads:

```
acceleration edge-cache range-offset <limit>
```

Viewing configuration settings

To show the current Edge Cache configuration settings:

```
show acceleration edge-cache
```

CLI: Certificates

You can use the **crypto** command to import keys and certificates.

Configuring Certificates and Keys

```
crypto certificate [generate|import|setkey]
crypto key import
```

To import a certificate or key in PEM format:

```
crypto {certificate|key} import <name> pem data "<pem-data>"
```

- `import <name>` - The name of the certificate or key.
- `pem data <pem-data>` - The PEM data. Ensure to quote the PEM data.

To generate a self-signed certificate:

```
crypto certificate generate self-signed <cert-name> instance {<instance-name>|exinda-
autogen}
```

To assign a key to a certificate:

```
crypto certificate setkey <certificate_name> {key|test}
```