Multiple SSL Certificates, Server Name Indication (SNI) for HTTPS

KB 22637 | Last updated on 2022-11-30 | Last updated by Barry de Graaff | 0.00 (0 votes) | Verified in: ZCS 10.0, ZCS 9.0, ZCS 8.8, ZCS 8.7

- This is **certified documentation** and is protected for editing by Zimbra Employees & Moderators only.

Note: This feature will not enable SSL Certificate for IMAP/POP or smtps connections. RFE #103282

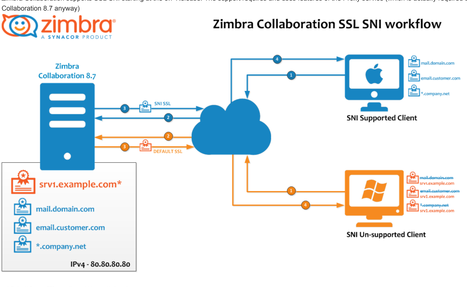
Server Name Indication (SNI) is an extension to the TLS computer networking protocol by which a client indicates which hostname it is attempting to connect to at the start of the handshaking process. This allows a server to present multiple certificates on the same IP address and TCP port number and hence allows multiple secure (HTTPS) websites (or any other Service over TLS) to be served off the same IP address without requiring all those sites to use the same certificate. It is the conceptual equivalent to HTTP/1.1 name-based virtual hosting, but for HTTPS. The desired hostname is not encrypted, so an eavesdropper can see which site is being requested.

To make SNI useful, as with any protocol, the vast majority of visitors must use web browsers that implement it. Users whose browsers do not implement SNI are presented with a default certificate and hence are likely to receive certificate warnings. Source:Wikipedia

Contents

Getting Started

Zimbra Collaboration supports SSL SNI starting at the 8.7 Release. The support requires and uses features of the Proxy service (which is actually required by Zimbra Collaboration 8.7 anyway)



* Default Server SSL, usually could be a self-signed

Prerequisites

- Zimbra proxy service must be installed and enabled on the server. In a multi server environment, these steps should be performed on the proxy node
- You should have a signed certificate + matching key pair and the trusted chain certs from your CA (Certificate Authority) (This is a common issue, so please, make sure you check your files before deploying them)
- You can bind Multiple SSL Certificates to just one ipv4 address, which will pair to the respective domain names. For example:

```
1.1.1.1 => example.com
1.1.1.1=> otherdomain.com
```

and you could even have another IPv4 address, for Customer reasons with other group of SSL Certificates, even different type of SSL Certificates:

```
3.3.3.3 => yetanotherdomain.com (A Comodo Wildcard SSL Certificate)
3.3.3.3 => thisisanotherdomain.com (A free Let's Encrypt SSL Certificate)
3.3.3.3 => customer001.net (A RapidSSL Certificate)
etc.
```

Browser support for SNI

The following browsers do offer support for SNI, however Zimbra hasn't tested all of them, it is the responsibility of the web-browser, to support the application part of SNI :

Software	Type	Supported	Notes	Supported since
Internet Explorer	Web browser	✔	Since version 7 on Vista (not supported on XP)	2006
Mozilla Firefox	Web browser	✔	Since version 2.0 Reference 116169	2006
curl	Command-line tool and library	✔	Since version 7.18.1	2008
Safari	Web browser	✔	Not supported on XP	
Google Chrome	Web browser	✔	Since 6.0	2010
BlackBerry OS	Web browser	✔	7.2 or later	
Windows Mobile	Web browser	✔	Some time after 6.5<ref>Template:Cite web</ref>	
Android default browser	Web browser	✔	Honeycomb (3.x) for tablets and Ice Cream Sandwich (4.x) for phones<ref>Template:Cite web</ref>	2011
wget	Command-line tool	✔	Since version 1.14	2012
Nokia Browser for Symbian	Web browser	✘		
Opera Mobile	Web browser	✘	Not supported on Series60	

Configuring the IP address per domain

- 1. Add the new domain, in this case **example.com**. Set **zimbraVirtualHostName** to **mail.example.com** and **zimbraVirtualIPAddress** to **1.2.3.4**. Make sure the zimbraVirtualHostName is set to the name which will be used to access the domain (URL) and the SSL certificate is signed for the same name.

```
zmprov md example.com zimbraVirtualHostName mail.example.com zimbraVirtualIPAddress 1.2.3.4
```

NOTE: If the server is behind a firewall and NAT'ed with an external address, make sure external requests for "mail.example.com" hit the aliased IP address and not the actual local IP address of server.

Verifying and Preparing the Certificates

We should have three files received from the CA (might vary depending on the Certificate Authority). The server (domain) certificate, and two chain certs. Also, you should have an existing key file (which was used to generate the csr)

- 1. Save the **example.com certificate**, **key** and **chain files** to a directory **/tmp/example.com**. You can receive single or multiple chain certs from your CA. Here we have two chain certs from the CA. i.e. example.com.root.crt and example.com.intermediate.crt.

```
ls /tmp/example.com
example.com.key
example.com.crt
example.com.root.crt
example.com.intermediate.crt
```

- 2. Add the chain certs to a single file called example.com_ca.crt

```
cat example.com.root.crt example.com.intermediate.crt >> example.com_ca.crt
```

- 3. Confirm if the key and certificate matches and chain certs completes the trust. As zimbra user:

```
/opt/zimbra/bin/zmcertmgr verifycrt comm /tmp/example.com/example.com.key /tmp/example.com/example.com.crt /tmp/example.com/example.com_ca.crt
```

- Check the output, it should say something like this. If not, make sure you have the correct key and chain cert files.

```
** Verifying '/tmp/example.com.crt' against '/tmp/example.com.key'
Certificate '/tmp/example.com.crt' and private key '/tmp/example.com.key' match.
** Verifying '/tmp/example.com.crt' against '/tmp/example.com_ca.crt'
Valid certificate chain: /tmp/example.com.crt: OK
```

Deploying the Certificate or Certificates on the domain

- 1. Add the domain certificate and chain files to a single file called **example.com.bundle**

```
cat example.com.crt example.com_ca.crt >> example.com.bundle
```

- 2. Run the following command as the **zimbra** user to save the certificates and key in LDAP:

```
/opt/zimbra/libexec/zmdomaincertmgr savecrt example.com example.com.bundle example.com.key
** Saving domain config key zimbraSSLCertificate...done.
** Saving domain config key zimbraSSLPrivateKey...done.
```

- The syntax is:

```
/opt/zimbra/libexec/zmdomaincertmgr savecrt <domainname> <certificate with chain certs> <keyfile>
```

- 3. Run the following command as the **zimbra** user to deploy the domain certificate. This will save the certificate and key as **/opt/zimbra/conf/domaincerts/example.com**:

```
/opt/zimbra/libexec/zmdomaincertmgr deploycrts
** Deploying cert for example.com...done.
```

Proxy Check

Run these commands on proxy hosts, or on the server if it's Single Server:

- zimbraReverseProxySNIEnabled should be set to TRUE in server and global config.

```
zmprov mcf zimbraReverseProxySNIEnabled TRUE
```

Re-write and restart Proxy

- Restart the proxy to re-write the changes to proxy config

```
zmproxyctl restart
```

- Once the restart is successfull, try to access the domain using the URL which is set in "zimbraVirtualHostName" over https. And check the certificate loaded in the browser. In this case the URL will be https://example.com

Testing

You can go now to a Web browser and check that for each different **zimbraVirtualHostName**, you see a different SSL certificate and that its details are correct for that virtualhostname.

Troubleshooting

- If you do not see the correct domain cert by accessing the domain with its zimbraVirtualHostName (example.com). Make sure that the https connection from the Internet/intranet is going to the server's local IP address which is defined in **zimbraVirtualIPAddress**, and make sure you have activated **zimbraReverseProxySNIEnabled** to **TRUE**
- If you are using multiple proxy servers or adding new proxy servers, make sure you copy all the contents of **/opt/zimbra/conf/domaincerts/** to all the proxy servers. **Otherwise the proxy service will fail to start.**

Known Issues

- Bug 102913 - **Multiple SSL domains on single server (SNI) for HTTPS connections**
- Bug 103362 - **Multiple SSL domains on single server (SNI) for IMAPS/POP3S connections**

ZBUG-3125. Impacts multi-domain environments with some domains having Virtual Hosts and others not, where SNI is in use.

Symptoms: Customers connecting new clients on domains without Virtual Hosts using the PublicServiceHostname of the front-end Layer 4 load balancer (or the fqdns of individual proxy servers) will get an SSL certificate error. Running the Qualys SSL Labs test will result in Qualys reporting two different certificates used, one for SNI clients (the correct SSL certificate) and a mismatched certificate for non-SNI clients. Running both of the following commands should produce the same certificate but don't as a result of this bug:

```
openssl s_client -connect <fqdn of the PSHN>:443
openssl s_client -connect <fqdn of the PSHN>:443 -servername <fqdn of the PSHN>
```

Apple clients in particular seem now to query Zimbra for all available certificates, and since Zimbra serves up both certificates, Apple clients will complain if either certificate doesn't match, and not always possible to accept the certificate mismatch.

Immediate Cause: The `server` entry for a Virtual Host appears at the top of the /opt/zimbra/conf/nginx/includes/nginx.conf.mail.imaps and /opt/zimbra/conf/nginx/includes/nginx.conf.web.https files. nginx seemingly doesn't obey its own rules for serving the `default` SSL certificate for non-SNI clients and instead just serves up the cert for the `server` (i.e. Virtual Host) listed at the top of either of these files (which file of course depending on the connection method of the client, i.e. ActiveSync or IMAPS).

Workaround: Edit both files to move the `server` section for the PSHN to the top of the two files, then run `zmproxyctl reload` to avoid having the files rewritten. After deploying the workaround, Qualys will report only one SSL certificate as being presented. Note: This host only supports SNI-capable browsers error presented before deploying the workaround. The two openssl commands above will now report the same certificate as well, and Apple clients will now connect successfully.

If using a Layer 4 load balancer, the PSHN is typically set to the fqdn of the load balancer, not the fqdn of the proxy server, which means the PSHN will also need to be a Virtual Host on the domain. If the PSHN fqdn is included in the Zimbra proxy server's SSL certificate, no domain certificate need be added; else a domain certificate should be added to cover the PSHN fqdn.

Same issue as reported here: https://www.reddit.com/r/nginx/comments/8shlsm/nginx_always_serving_2_certificates_and_one_of/

Verified Against: {{{1}}}	Date Created: {{{2}}}
Article ID: https://wiki.zimbra.com/index.php?title=Multiple_SSL_Certificates,_Server_Name_Indication_(SNI)_for_HTTPS	Date Modified: 2022-11-30

Try Zimbra
Try Zimbra Collaboration with a 60-day free trial.
Get it now »

Want to get involved?
You can contribute in the Community, Wiki, Code, or development of Zimlets.
Find out more. »

Other help Resources
User Help Page »
Official Forums »
Zimbra Documentation Page »

Looking for a Video?
Visit our YouTube channel to get the latest webinars, technology news, product overviews, and so much more.
Go to the YouTube channel »

Categories:
- ZCS 8.8
- ZCS 8.7
- Certified
- Certificates
- ZCS 10.0
- ZCS 9.0

Jump to: navigation, search

Copyright © 2005 - 2024 Zimbra, Inc. All rights reserved.
Legal Information | Privacy Policy | Do Not Sell My Personal Information | CCPA Disclosures