

Configure Prosody To Use Forward Secrecy

05/02/2015 07:24 PM - Daniel Curtis

Status:	Closed	Start date:	05/02/2015
Priority:	Normal	Due date:	
Assignee:	Daniel Curtis	% Done:	100%
Category:	XMPP Server	Estimated time:	0.50 hour
Target version:	Debian	Spent time:	1.00 hour

Description

This is a guide for setting up forward secrecy with Prosody XMPP server.

Prepare the Environment

- Make sure the system is up to date:

```
apt-get update && apt-get upgrade
```

Harden Prosody

Prosody automatically defaults to use forward secrecy if the host system supports it. However, a DH parameter file is not created during installation.

- Generate a DH parameter file:

```
openssl dhparam -out /etc/prosody/certs/dh-2048.pem
```

- Now edit the prosody config file:

```
nano /etc/prosody/prosody.cfg.lua
```

- And modify the ssl location:

```
ssl = {  
    key = "/etc/prosody/certs/prosody.example.com.key";  
    certificate = "/etc/prosody/certs/prosody.example.com.crt";  
    options = { "no_sslv2", "no_ticket", "no_compression", "no_sslv3" };  
    ciphers = "HIGH+kEDH:HIGH+kEECDH:HIGH:!CAMELLIA:!PSK:!SRP:!3DES:!aNULL";  
    dhparam = "/etc/prosody/certs/dh-2048.pem";  
}
```

- **NOTE:** Make sure to have luasec 0.5 or higher for DHE and ECDHE to work properly.

Testing

- Test the connection with starttls:

```
openssl s_client -starttls xmpp -connect prosody.example.com:5269
```

- *Truncated output:*

```
SSL-Session:  
  Protocol : TLSv1.2  
  Cipher   : ECDHE-RSA-AES256-GCM-SHA384
```

Resources

- <http://prosody.im/doc/security>
- http://prosody.im/doc/advanced_ssl_config

History

#1 - 05/02/2015 07:44 PM - Daniel Curtis

- *Status changed from New to Resolved*
- *% Done changed from 0 to 100*

#2 - 05/10/2015 09:21 AM - Daniel Curtis

- *Status changed from Resolved to Closed*