# Technical Support Advisory: Recommended SSL Templates for PFS (Perfect Forward Secrecy) Ciphers

Updated: November 4, 2014
Revision: 003

## Synopsis:

With default SSL template, AX or Thunder device configured with SSL offload on software releases 2.7.2-P3 patch code train may experience high data CPU utilization or SSL handshake failures under minimal SSL traffic load. In addition, SSL connections may fail intermittently if GCM ciphers are used for negotiation (Bug ID: 221545).

## Applicable Hardware:

AX or Thunder devices contain PX and/or Nitrox III SSL Cards

## Applicable Software:

SLB code train: 2.7.2-P3, 2.7.2-P3-SP3

## Root Cause:

Any client using DHE ciphers or ECDHE ciphers with ec-names not offloaded in hardware will result in high CPU usage because traffic is forced to be processed by data CPUs .

Nitrox III SSL card only offers hardware support for two Elliptical Curve, ec-name secp256r1 and secp384r1, which must be explicitly configured in the client SSL template to take advantage of hardware offload. Hardware offload for DHE ciphers on Nitrox III card has not been implemented but will be available in future software releases. For server side SSL, only handshakes for RSA ciphers are offloaded to hardware. DHE/ECDHE ciphers are processed by data CPUs.

The software defect 221545, which affects both Nitrox III and PX cards and causes SSL handshake failure due to GCM ciphers, will be addressed in 2.7.2-P4.

## Workarounds:

Configure specific ciphers supported by PX or Nitrox III SSL cards in the SSL templates. Following are recommended client or server SSL templates that can be configured to avoid potential issues due to lack of hardware support for some Elliptical Curve ciphers in current software releases.

## For PX card:

```
slb template client-ssl clientssl
   cert cert
   key key
   cipher TLS1_RSA_EXPORT1024_RC4_56_MD5
   cipher TLS1_RSA_EXPORT1024_RC4_56_SHA
   cipher SSL3_RSA_RC4_40_MD5
   cipher SSL3_RSA_RC4_128_MD5
   cipher SSL3_RSA_RC4_128_SHA
   cipher SSL3_RSA_DES_40_CBC_SHA
   cipher SSL3_RSA_DES_64_CBC_SHA
   cipher SSL3_RSA_DES_192_CBC3_SHA
   cipher TLS1_RSA_AES_128_SHA
   cipher TLS1_RSA_AES_256_SHA
   cipher TLS1_RSA_AES_128_SHA256
   cipher TLS1_RSA_AES_256_SHA256
```

## For Nitrox III card:

```
slb template client-ssl clientssl
   cert cert
   key key
   ec-name secp256r1
   ec-name secp384r1
   cipher TLS1_RSA_EXPORT1024_RC4_56_MD5
   cipher TLS1_RSA_EXPORT1024_RC4_56_SHA
   cipher SSL3_RSA_RC4_40_MD5
   cipher SSL3_RSA_RC4_128_MD5
   cipher SSL3_RSA_RC4_128_SHA
   cipher SSL3_RSA_DES_40_CBC_SHA
   cipher SSL3_RSA_DES_64_CBC_SHA
   cipher SSL3_RSA_DES_192_CBC3_SHA
   cipher TLS1_RSA_AES_128_SHA
   cipher TLS1_RSA_AES_256_SHA
   cipher TLS1_ECDHE_RSA_AES_128_SHA
   cipher TLS1_ECDHE_RSA_AES_256_SHA
   cipher TLS1_ECDHE_ECDSA_AES_128_SHA
   cipher TLS1_ECDHE_ECDSA_AES_256_SHA
   cipher TLS1_RSA_AES_128_SHA256
   cipher TLS1_RSA_AES_256_SHA256
   cipher TLS1_ECDHE_RSA_AES_128_SHA256
  cipher TLS1_ECDHE_ECDSA_AES_128_SHA256
```

Following server-ssl template is recommended if end-to-end SSL offload is deployed with devices with Nitrox III card. For devices with PX card, default template can be used.

```
slb template server-ssl serverssl
   cipher TLS1_RSA_EXPORT1024_RC4_56_MD5
   cipher TLS1_RSA_EXPORT1024_RC4_56_SHA
   cipher SSL3_RSA_RC4_40_MD5
   cipher SSL3_RSA_RC4_128_MD5
   cipher SSL3_RSA_RC4_128_SHA
   cipher SSL3_RSA_DES_40_CBC_SHA
   cipher SSL3_RSA_DES_64_CBC_SHA
   cipher SSL3_RSA_DES_192_CBC3_SHA
   cipher TLS1_RSA_AES_128_SHA
   cipher TLS1_RSA_AES_256_SHA
   cipher TLS1_RSA_AES_128_SHA256
   cipher TLS1_RSA_AES_256_SHA256
```

## Notes:

1. Customers are encouraged to evaluate their user base to determine the validity of disabling weak ciphers.
2. Use the command "show hardware" to determine whether the A10 device has either Nitrox III or PX cards or both.

```
TH1030S#show hardware
Thunder Series Unified Application Service Gateway TH1030S
      Serial No : TH10A53313390024
      CPU       : Intel(R) Xeon(R) CPU
                  8 cores
                  9 stepping
      Storage   : Single 74G drive
      Memory    : Total System Memory 8150 Mbyte, Free Memory 2873 Mbyte
      SMBIOS    : Build Version: 4.6.5
                  Release Date: 07/24/2013
      SSL Cards : 1 device(s) present
                  1 Nitrox III
      GZIP      : 0 compression device(s) present
      FPGA      : 0 instance(s) present
      L2/3 ASIC : 0 device(s) present
      IPMI      : Present
      Ports     : 10
```

## About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: www.a10networks.com


### Corporate Headquarters

**A10 Networks, Inc**
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666

www.a10networks.com

### Worldwide Offices

**North America**
sales@a10networks.com
**Europe**
emea_sales@a10networks.com
**South America**
latam_sales@a10networks.com
**Japan**
jinfo@a10networks.com
**China**
china_sales@a10networks.com
**Taiwan**
taiwan@a10networks.com
**Korea**
korea@a10networks.com
**Hong Kong**
HongKong@a10networks.com
**South Asia**
SouthAsia@a10networks.com
**Australia/New Zealand**
anz_sales@a10networks.com


To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.