Contents

Introduction

This document describes the necessary steps to be applied if encountering an issue with TLS communication, or accessing the web interface, after upgrading to AsyncOS for Email Security version 9.5 or newer on the Cisco Email Security Appliances (ESA).

Legacy certificates (MD5) cause TLSv1.2 communication to fail on 9.5 AsyncOS for Email Security upgrades and newer

> **Note**: The following is a listed workaround for the current demo certificates applied on the appliance. However, the below steps may also appliance apply to any MD5 signed certificates.

Upon performing an upgrade to AsyncOS for Email Security version 9.5 and newer, any of the legacy IronPort demo certificates still in use and applied for delivery, receiving or LDAP, may experience errors while trying to communicate via TLSv1/TLSv1.2 with some domains. The TLS error will cause all inbound or outbound sessions to fail.

If the certificates are applied to the HTTPS interface, modern web browsers will fail to access the web interface of the appliance.

Mail Logs should look similar to the following example:

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
```

This error is caused by the signature algorithm applied to the older certificate being MD5; however, the certificates associated with the connecting appliance/browser only supports SHA signature based algorithms. Although, the older demo certificates which has the MD5 signature is on the appliance the same time the new SHA based demo certificate the above error will only manifest itself if the MD5 signature based certificate is applied to the specified sections (i.e. receiving, delivery, etc.)

Below is an example pulled from the cli of an appliance that has both the older MD5 certificates in addition to the new Demo Certificate (Note: the newer certificate (Demo) should be the newer the SHA algorithm and have a longer expiration date than the older demo certificates).:

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
```

Corrective Actions

1. Navigate to the Web (UI): **Network > Certificates**
2. Verify that you currently have the older certificates installed and also have the new SHA Demo certificate.
3. Based on where the older demo certificates are applied replace this with new Demo certificate.

Typically these certificates can be found being applied in the following sections:

- **Network > Listeners > Then name of the listener > Certificate**
- **Mail Polices > Destination Controls > Edit Global Settings > Certificate**
- **Network > IP Interface > Choose interface associated with GUI access > HTTPS Certificate**
- **System Administration > LDAP > Edit Settings > Certificate**

4. Once all certificates have been replaced verify from the command line that TLS communication is now successful.

Example of working TLS communication being negotiated using TLSv1.2:

```
Thu Jul  2 16:38:30 2015 Info: New SMTP ICID 4435675 interface Data1 (10.0.10.1)
address 209.85.213.182 reverse dns host mail-ig0-f182.google.com verified yes Thu Jul 2 16:38:30
2015 Info: ICID 4435675 ACCEPT SG UNKNOWNLIST match sbrs[0.0:10.0] SBRS 4.8 Thu Jul 2 16:38:30
2015 Info: ICID 4435675 TLS success protocol TLSv1.2 cipher AES128-GCM-SHA256
```

CLI Corrective Actions (if GUI cannot be accessed)

The certificate may need to be modified on each IP interface that has a certificate enabled for HTTPS service. In order to modify the certificate in use for interfaces, please run the following commands on the CLI:

1. Type **interfaceconfig**.
2. Select **edit**.
3. Enter the number of the interface you wish to edit.
4. Use the return key to accept the current settings for each question presented. When the option for the certificate to apply is presented, select the Demo certificate:
    1.
       ```
       1. Ironport Demo Certificate
       2. Demo
       Please choose the certificate to apply:
       [1]> 2

       You may use "Demo", but this will not be secure.
       Do you really wish to use the "Demo" certificate? [N]> Y
       ```
5. Finish stepping through the settings prompts until all configuration questions are completed.
6. Use the return key to exit to the main CLI prompt.
7. Use**commit** to save your changes to the configuration.

    Note: Please remember to **commit** changes after changing the certificate in use on the interface.

Related Information

- Comprehensive Setup Guide for TLS on ESA
- Cisco Email Security Appliance - End-User Guides
- Cisco Security Management Appliance - End-User Guides
- Technical Support & Documentation - Cisco Systems