Cisco RES: How to use TLS to secure unencrypted RES replies

Contents

Introduction

This document describes how to to use Transport Layer Security (TLS) to secure replies from the Cisco Registered Envelope Service (CRES), which allows a user to not need to decrypt them, in association with the Cisco Email Security Appliance (ESA).

Cisco RES: How to use TLS to secure unencrypted RES replies

By default, replies to a secure email are encrypted by Cisco RES and sent on to your mail gateway. They then pass through to your mail servers encrypted for the end-user to open with their Cisco RES credentials.

In order to avoid the need for the user to authenticate with Cisco RES to open up the secure reply, Cisco RES delivers in an "unencrypted" form to mail gateways that support TLS. In most cases, the mail gateway is the ESA, and this article applies.

However, if there is another mail gateway that sits in front of the ESA such as an external spam filter, there is no need for the certificate/TLS/mail flow configuration on your ESA. In this case, you can skip steps 1 to 3 in the Solution section of this document. For unencrypted replies to work in this environment, the external spam filter (mail gateway) is the appliance that needs to support TLS. If they do support TLS, you can have Cisco RES confirm this and get you set up for "unencrypted" replies in order to secure emails.

Sender Policy Framework

In order to avoid Sender Policy Framework (SPF) verification failures, you must add mx:res.cisco.com, mxnat1.res.cisco.com, and mxnat3.res.cisco.com to your SPF record. Or, you can 'include' **spfc._spf.cisco.com** in your SPF record.

Example:

```
~ dig txt spfc._spf.cisco.com +short
```

```
"v=spf1 mx:res.cisco.com mx:sco.cisco.com ~all"
```

Where and how you add Cisco RES to your SPF record depends on how your Domain Name System (DNS) is implemented with-in your network topology. Please be sure to contact your DNS administrator for more information.

If DNS is not configured to include Cisco RES, when secure compose and secure replies are generated and delivered through the hosted key servers, the outgoing IP address will not match the listed IP addresses at the recipient's end, resulting in an SPF verification failure.

Hostnames and IP Addresses

Hostname	IP Address	Record Type
res.cisco.com	184.94.241.74	A
mxnat1.res.cisco.com	208.90.57.32	A
mxnat2.res.cisco.com	208.90.57.33	A
mxnat3.res.cisco.com	184.94.241.96	A
mxnat4.res.cisco.com	184.94.241.97	A
mxnat5.res.cisco.com	184.94.241.98	A
mxnat6.res.cisco.com	184.94.241.99	A
mxnat7.res.cisco.com	208.90.57.34	A
mxnat8.res.cisco.com	208.90.57.35	A
esa1.cres.iphmx.com	68.232.140.79	MX
esa2.cres.iphmx.com	68.232.140.57	MX
esa3.cres.iphmx.com	68.232.135.234	MX
esa4.cres.iphmx.com	68.232.135.235	MX

> **Note**: Hostname and IP addresses are subject to change based on service/network maintenance or service/network growth. Not all hostnames and IP addresses are used for service. They are provided here for reference.

Solution

1. Obtain and install a signed certificate and intermediate certificate on the ESA. **Note**: It is important you obtain the intermediate certificate from your signing authority as the demo certificate that comes on the appliance causes the CRES verification process to fail.
2. Create a new mail flow policy: From the GUI, choose **Mail Policies > Mail Flow Policies > Add Policy...**.Enter a name and leave all else at default except for *Security Features: TLS.* Set this to **Required**.
3. Create a new sender group: From the GUI, choose **Mail Policies > HAT Overview > Add Sender Group...**.Enter a name and set order number to #1. You can also enter an optional comment. Choose the mail flow policy you created in step 2. Leave everything else blank.Click **Submit and Add Senders >>**.
4. In the Sender field, enter these IP ranges and hostnames:
   ```
   .res.cisco.com
   .cres.iphmx.com
   208.90.57.0/26 (current CRES IP network range)
   204.15.81.0/26 (old CRES IP network range)
   ```
5. Submit and commit the changes.
6. After you are confident the ESA is prepared for TLS from the Cisco RES servers, follow the steps in How do I test if my domain supports TLS with Cisco RES? in order to request the Cisco RES servers to start to use TLS.

Related Information

- **Cisco RES: IP Addresses and Hostnames for Key Servers**
- **Cisco Email Security Appliance - End-User Guides**
- **Technical Support & Documentation - Cisco Systems**