

Configure CRES Secure Encryption Service Message Replies using TLS Encryption

Contents

[Introduction](#)

[Cisco RES: How to Use TLS to Secure Unencrypted RES Replies](#)

[Sender Policy Framework](#)

[Hostnames and IP Addresses](#)

[Solution](#)

[Related Information](#)

Introduction

This document describes actions to configure TLS encryption for CRES inbound secure replies instead of a Secure Envelope attachment.

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 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 eliminate the need for user authentication when opening a Cisco RES secure message reply, Cisco RES delivers in an "unencrypted" form to mail gateways that support Transport Layer Security (TLS). In most cases, the mail gateway is the Cisco Email Security Appliance (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 - 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 support TLS, you can have Cisco RES confirm this and get you set up for "unencrypted" replies to secure emails.

Sender Policy Framework

In order to avoid Sender Policy Framework (SPF) verification failures, add these values to your SPF record.

The Cisco Registered Envelope Service (CRES) SPF record value matches the IP/hostnames of this table, "Hostnames and IP Addresses".

The output using the Cisco-provided SPF mechanism:

```
<#root>
~ dig txt
res.cisco.com
+short
```

```
"v=spf1
```

```
mx:res.cisco.com
```

```
exists:%{i}.spf.res.cisco.com
```

```
-all"
```

Add this mechanism to your existing SPF record:

```
<#root>
```

```
include:res.cisco.com
```

Sample of a FAKE/test SPF record containing the new **res.cisco.com** mechanism:

```
<#root>
```

```
"v=spf1 mx:sampleorg1.com ip4:1.2.3.4
```

```
include:res.cisco.com
```

```
-all"
```


Where and how you add Cisco RES to your SPF record depends on how your Domain Name System (DNS) is implemented within your network topology. 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 does not match the listed IP addresses at the end of the recipient, 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

Hostname	IP Address	Record Type
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

- Obtain and install a signed certificate and intermediate certificate on the ESA.

 **Note:** You must obtain the intermediate certificate from your signing authority as the demo certificate that comes on the appliance causes the CRES verification process to fail.

- Create a new mail flow policy:
 - a. From the GUI, choose Mail Policies > Mail Flow Policies > Add Policy.
 - b. Enter a name and leave all else at default except for 'Security Features: TLS'. Set this to **Required**.
- Create a new sender group:
 - a. From the GUI, choose Mail Policies > HAT Overview > Add Sender Group.
 - b. Enter a name and set the 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.
 - c. Click Submit and Add Senders.
- 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)

- **Submit** and commit the changes.
- After you are confident the ESA is prepared to negotiate TLS encryption from the Cisco RES servers, pursue the steps within the CRES Admin Portal [How do I test if my domain supports TLS with Cisco RES?](#)

Related Information

- [Cisco RES: IP Addresses and Hostnames for Key Servers](#)
- [Cisco Email Security Appliance - End-User Guides](#)
- [Technical Support & Documentation - Cisco Systems](#)