

# IP Addresses and Hostnames for CRES Key Servers

## Contents

[Introduction](#)

[IP Addresses and Hostnames for CRES Key Servers](#)

[ESA Configuration](#)

[Related Information](#)

## Introduction

This document provides information that might be required to configure a firewall and Cisco Email Security Appliance (ESA) for Cisco Registered Envelope Service (CRES) communication to CRES key servers. Customers with strict firewall rules require permissions for specific IP addresses or hostnames in order to allow communication for CRES. Encryption via CRES on the ESA requires firewall rules for port 80 and 443 in order to send key requests to CRES to encrypt a message.

**Note:** The information provided in this document might be updated and changed at any time. If there are questions or concerns, open a Cisco Technical Assistance Center (TAC) support case.

## IP Addresses and Hostnames for CRES Key Servers

CRES uses these IP address ranges in order to initiate SMTP - Transport Layer Security (TLS) sessions:

Active (184.94.241.96 - 184.94.241.99)

IP Address	Hostname
------------	----------

184.94.241.96	mxnat3.res.cisco.com
---------------	----------------------

184.94.241.97	mxnat4.res.cisco.com
---------------	----------------------

184.94.241.98	mxnat5.res.cisco.com
---------------	----------------------

184.94.241.99	mxnat6.res.cisco.com
---------------	----------------------

Backup (208.90.57.32 - 208.90.57.35)

IP Address	Hostname
------------	----------

208.90.57.32	mxnat1.res.cisco.com
--------------	----------------------

208.90.57.33	mxnat2.res.cisco.com
--------------	----------------------

208.90.57.34	mxnat7.res.cisco.com
--------------	----------------------

208.90.57.35	mxnat8.res.cisco.com
--------------	----------------------

Some customers might restrict access to the CRES key server res.cisco.com. The CRES key server res.cisco.com has two (2) blocks of VIPs. Add them to your network device's access rules where appropriate:

Active (184.94.241.74 - 184.94.241.78)

IP Address	Hostname
184.94.241.74	sv4.res.cisco.com
184.94.241.75	applet-sv4.res.cisco.com
184.94.241.76	prod-cres-app-mail.sv4.ironport.com
184.94.241.77	pxmail.com
184.94.241.78	verify.res.cisco.com

Backup: (208.90.57.15 - 208.90.57.18)

IP Address	Hostname
208.90.57.15	vega.res.cisco.com
208.90.57.16	applet-vega.res.cisco.com
208.90.57.17	
208.90.57.18	verify.res.cisco.com

## ESA Configuration

Add the previously listed IP addresses and hostnames by their IP address range to your existing sender group that is used for TLS (Incoming):

1. Log in to the ESA GUI.
2. Navigate to **Mail Policies > Host Access Table > HAT Overview** and edit your TLS sender group (naming convention might vary).
3. Add the IP address range and hostname: **184.94.241.96-99, .res.cisco.com**  
**208.90.57.32-35, .res.cisco.com**
4. Submit and commit changes.

**Note:** It is highly recommended to add the hostname *.res.cisco.com* along with the IP address range, since any future additions will use the Domain Name Server (DNS) in order to do the lookup for the IP address information.

The previous CRES key server hostnames might have been listed as:

vega.res.cisco.com  
soma.res.cisco.com

It is recommended to update your network and/or firewall rules and definitions as well to match the previous information.

## Related Information

- [Cisco Email Security Appliance - End-User Guides](#)
- [Technical Support & Documentation - Cisco Systems](#)