Configurazione delle risposte ai messaggi del servizio di crittografia sicura CRES tramite crittografia TLS

Sommario

Introduzione

In questo documento vengono descritte le azioni da eseguire per configurare la crittografia TLS per le risposte sicure in ingresso del CRES anziché per un allegato Secure Envelope.

Cisco RES: Come utilizzare TLS per proteggere le risposte RES non crittografate

Per impostazione predefinita, le risposte a un'e-mail protetta vengono crittografate da Cisco RES e inviate al gateway di posta. e quindi passano ai server di posta crittografati in modo che l'utente finale possa aprirli con le credenziali Cisco RES.

Per eliminare la necessità dell'autenticazione dell'utente all'apertura di una risposta al messaggio protetto Cisco RES, Cisco RES effettua la consegna in formato "non crittografato" ai gateway di posta che supportano Transport Layer Security (TLS). Nella maggior parte dei casi, il gateway di posta è Cisco Email Security Appliance (ESA) e questo articolo è applicabile.

Tuttavia, se davanti all'ESA c'è un altro gateway di posta, ad esempio un filtro antispam esterno, non è necessario configurare il flusso di certificati/TLS/posta sull'ESA. In questo caso, è possibile ignorare i passaggi da 1 a 3 nella sezione Soluzione di questo documento. Affinché le risposte non crittografate funzionino in questo ambiente, il filtro antispam esterno (gateway di posta) è l'accessorio che deve supportare TLS. Se supportano TLS, è possibile chiedere a Cisco RES di confermarlo e configurare le risposte "non crittografate" per l'invio di e-mail protette.

Framework criteri mittente

Per evitare errori di verifica di Sender Policy Framework (SPF), aggiungere questi valori al record SPF.

Il valore del record SPF Cisco Registered Envelope Service (CRES) corrisponde ai nomi IP/host di questa tabella, "Nomi host e indirizzi IP".

L'output viene generato utilizzando il meccanismo SPF fornito da Cisco:

<#root>

```
~ dig txt
```

res.cisco.com

```
 +short
"v=spf1
```

mx:res.cisco.com

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

```
 -all"
```

Aggiungere questo meccanismo al record SPF esistente:

<#root>

include:res.cisco.com

Esempio di record SPF di test/FALSO contenente il nuovo meccanismo res.cisco.com:

<#root>

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

include:res.cisco.com

```
 -all"
```

La posizione e la modalità di aggiunta di Cisco RES al record SPF dipendono dall'implementazione del DNS (Domain Name System) nella topologia di rete. Per ulteriori informazioni, contattare l'amministratore DNS.

Se il DNS non è configurato per includere Cisco RES, quando la composizione sicura e le risposte sicure vengono generate e recapitate tramite i server chiave ospitati, l'indirizzo IP in uscita non corrisponde agli indirizzi IP elencati alla fine del destinatario, determinando un errore di verifica SPF.

Nomi host e indirizzi IP

Nome host	Indirizzo IP	Tipo di record
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

Nota: il nome host e gli indirizzi IP sono soggetti a modifiche in base alla manutenzione del servizio/rete o alla crescita del servizio/rete. Non tutti i nomi host e gli indirizzi IP vengono utilizzati per il servizio. Sono fornite qui come riferimento.

Soluzione

- Ottenere e installare un certificato firmato e un certificato intermedio sull'ESA.

Nota: è necessario ottenere il certificato intermedio dall'autorità di firma in quanto il certificato demo presente sull'accessorio impedisce il completamento del processo di verifica CRES.

- Crea un nuovo criterio flusso di posta:
  a. Dalla GUI, selezionare Mail Policies > Mail Flow Policies > Add Policy.

    - Immettere un nome e lasciare invariate le altre impostazioni, ad eccezione di 'Funzioni di sicurezza: TLS'. Impostare su **Obbligatorio**.

- Crea un nuovo gruppo di mittenti:

  a. Dalla GUI, selezionare Mail Policies > HAT Overview > Add Sender Group.

    - Immettere un nome e impostare il numero di ordine su #1. È inoltre possibile immettere un commento facoltativo. Scegliere il criterio del flusso di posta creato nel passaggio 2. Lasciare tutto il resto in bianco.

    - Fare clic su Submit andAdd Senders.

- Nel campo Sender (Mittente), immettere i seguenti intervalli IP e nomi host:

```
.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)
```

-

Inviare e confermare le modifiche.

- Dopo aver verificato che l'ESA è pronta a negoziare la crittografia TLS dai server Cisco RES, eseguire i passaggi all'interno del portale di amministrazione di CRES Come verificare se il dominio supporta TLS con Cisco RES?

Informazioni correlate

- Cisco RES: Indirizzi IP e nomi host per i server chiave

- Cisco Email Security Appliance - Guide per l'utente

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).