Protezione da spoof mediante verifica mittente

Sommario

[Introduzione](#)
[Protezione da spoof mediante verifica mittente](#)
[Configura HAT](#)
[Configura tabella eccezioni](#)
[Verifica](#)
[Informazioni correlate](#)

Introduzione

Per impostazione predefinita, Cisco Email Security Appliance (ESA) non impedisce il recapito in entrata dei messaggi indirizzati "dallo stesso dominio" allo stesso dominio. Questo permette alle aziende esterne di "falsificare" i messaggi per condurre affari legittimi con il cliente. Alcune aziende si affidano a organizzazioni di terze parti per l'invio di e-mail per conto dell'azienda, ad esempio assistenza sanitaria, agenzie di viaggio, ecc.

Protezione da spoof mediante verifica mittente

Configura criteri flusso di posta

1. Dall'interfaccia grafica: **Criteri di posta > Criteri flusso di posta > Aggiungi criterio...**
2. Creare una nuova copia multifunzione utilizzando un nome appropriato, ad esempio SPOOF_ALLOW
3. Nella sezione *Verifica mittente* modificare la configurazione *Usa tabella eccezioni di verifica mittente* da **Utilizza predefinito** a **DISATTIVATO**.
4. In **Mail Policies > Mail Flow Policies > Default Policy Parameters**, impostare *Use Sender Verification Exception Table* configuration su **On**.

Configura HAT

1. Dalla GUI: **Mail Policies > HAT Overview > Add Sender Group...**
2. Impostare il nome di conseguenza sulla stampante multifunzione creata in precedenza, ad esempio SPOOF_ALLOW.
3. Impostare l'ordine in modo che sia superiore ai gruppi di mittenti ALLOWLIST e BLOCKLIST.
4. Assegnare il criterio **SPOOF_ALLOW** a queste impostazioni del gruppo di mittenti.
5. Fare clic su **Invia e aggiungi mittenti...**
6. Aggiungere IP o domini per le parti esterne a cui si desidera consentire lo spoofing del dominio interno.

Configura tabella eccezioni

1. Dall'interfaccia grafica: **Criteri di posta > Tabella eccezioni > Aggiungi eccezione di verifica mittente...**
2. Aggiungi il dominio locale alla tabella delle eccezioni di verifica del mittente
3. Impostare *Comportamento* a **Rifiuta**

Verifica

A questo punto, i messaggi provenienti da *your.domain* e inviati a *your.domain* verranno rifiutati a meno che il mittente non sia elencato nella tabella SPOOF_ALLOW del gruppo di mittenti, in quanto verrebbero associati a un programma multifunzione che non utilizza la tabella delle eccezioni di verifica del mittente.

Un esempio di ciò può essere dato dal completamento di una sessione telnet manuale con il listener:

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

La risposta SMTP 553 è una risposta diretta risultante dalla tabella delle eccezioni configurata sull'ESA dai passaggi precedenti.

Dai log di posta, è possibile verificare che l'indirizzo IP 192.168.0.9 non è incluso nell'indirizzo IP valido per il gruppo di mittenti corretto:

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

Un indirizzo IP consentito corrispondente all'esempio di configurazione illustrato nei passaggi precedenti verrà visualizzato come segue:

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
```

```
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

Informazioni correlate

- ESA, SMA e WSA Grep con Regex per cercare i log
- Determinazione della disposizione del messaggio ESA
- Documentazione e supporto tecnico – Cisco Systems