Spraak-bescherming met gebruikersverificatie

Inhoud

[Inleiding](#)
[Spraak-bescherming met gebruikersverificatie](#)
[HAT configureren](#)
[Uitzonderingstabel configureren](#)
[Verifiëren](#)
[Gerelateerde informatie](#)

Inleiding

Standaard verhindert de Cisco e-mail security applicatie (ESA) niet de inkomende levering van berichten die zijn gericht "van" hetzelfde domein en naar hetzelfde domein gaan. Dit laat berichten toe om "gespoofd" te worden door buitenbedrijven die zaken doen met de klant. Sommige bedrijven vertrouwen erop dat een derde partij een e-mail verstuurt namens het bedrijf, zoals de gezondheidszorg, reisbureaus, enzovoort.

Spraak-bescherming met gebruikersverificatie

Mail Flow Policy configureren (MFP)

1. Via de GUI: **Mail Policies > Mail Flow Policies > Add Policy...**
2. Maak een nieuw MFP met een naam die relevant is zoals SPOOF_ALLOW
3. Wijzig in het gedeelte *Sender Verification* de configuratie van de *Uitzonderingstabel* gebruiken *van* **Standaard** naar **UIT**.
4. In **Mail Policies > Mail Flow Policy > Default Policy parameters**, stel de *Use Sender Verification Table* configuratie in op **On**.

HAT configureren

1. Vanuit de GUI: **Mail Policies > HAT - Overzicht > Add Sender Group...**
2. Stel de naam dienovereenkomstig in op de MFP die eerder is gemaakt, d.w.z. SPOOF_ALLOW.
3. Stel de volgorde in zodat deze boven de ALLOWLIST- en BLOCKLIST-sendergroepen staat.
4. Wijs het **SPOOF_ALLOW** beleid aan deze instellingen van de Zender Groep toe.
5. Klik op **Senders indienen en toevoegen...**
6. Voeg IP(en) of domeinen toe voor alle externe partijen die u wilt toestaan om het interne domein te verlaten.

Uitzonderingstabel configureren

1. Via de GUI: **Mail Policies > Exception Table > Add Sender Verification Exception...**
2. Voeg het lokale domein toe aan de Tabel van de Uitzondering van de Kender
3. Instellen *gedrag* aan **afwijzen**

Verifiëren

Op dit moment wordt e-mail die afkomstig is van *uw.domein* naar *uw.domein* verworpen tenzij de afzender in de Sender Group SPOOF_ALLOW is opgenomen, omdat dit gekoppeld zou worden aan een MFP dat niet gebruikmaakt van de uitzonderingstabel voor verificatie van afzender.

Een voorbeeld hiervan is de voltooiing van een handmatig telnet-sessie aan de luisteraar:

```
$ 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
```

De respons van 553 MTP is een direct resultaat van de uitzonderingstabel zoals die op de ESA is ingesteld uit de hierboven beschreven stappen.

Vanaf de maillogs kunt u zien dat het IP-adres van 192.168.0.9 niet in het geldige IP-adres voor de juiste sendergroep aanwezig is:

```
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
```

Een toegestaan IP-adres dat overeenkomt met de configuratie van de bovenstaande stappen, wordt als volgt gezien:

```
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
```

Gerelateerde informatie

- ESA, SMA en WSA Grep met Regex om Logs te zoeken
- ESR Berichtenbepaling
- Technische ondersteuning en documentatie – Cisco Systems