Spoof-Schutz durch Absenderverifizierung

Inhalt

Einführung

Standardmäßig verhindert die Cisco E-Mail Security Appliance (ESA) nicht, dass eingehende Nachrichten, die "von" derselben Domäne "aus" adressiert sind, an dieselbe Domäne weitergeleitet werden. So können Nachrichten von externen Unternehmen "gefälscht" werden, die legitime Geschäfte mit dem Kunden betreiben. Einige Unternehmen verlassen sich darauf, dass eine Drittfirma E-Mails für das Unternehmen sendet, z. B. im Gesundheitswesen, bei Reisebüros usw.

Spoof-Schutz durch Absenderverifizierung

Mail Flow Policy (MFP) konfigurieren

1. Über die Benutzeroberfläche: **Mail-Policys > Mail Flow Policies > Add Policy..**
2. Erstellen Sie einen neuen MFP mit einem Namen, der relevant ist, wie SPOOF_ALLOW
3. Ändern Sie im Abschnitt *Absenderverifizierung* die Konfiguration *Ausnahmetabelle für die Absenderverifizierung* von **Standard** verwenden in **AUS**.
4. Legen Sie unter **Mail-Policys > Mail Flow Policies > Default Policy Parameters** (E-Mail-Datenflussrichtlinien > Standard-Richtlinienparameter) die Konfiguration *Use Sender Verification Exception Table* configuration auf **On fest**.

Konfigurieren von HAT

1. Von der GUI: **Mail Policies > HAT Overview > Add Sender Group..**
2. Legen Sie den Namen entsprechend dem zuvor erstellten MFP fest, d. h. SPOOF_ALLOW.
3. Legen Sie die Reihenfolge so fest, dass sie über den Absendergruppen ALLOWLIST und BLOCKLIST liegt.
4. Weisen Sie den Einstellungen der Absendergruppe die **SPOOF_ALLOW**-Richtlinie zu.
5. Klicken Sie auf **Senden und Absender hinzufügen...**
6. Fügen Sie IP(s) oder Domänen für alle externen Parteien hinzu, die Sie die Spoofing-Funktion der internen Domäne zulassen möchten.

Ausnahmetabelle konfigurieren

1. Über die Benutzeroberfläche: **Mail-Policys > Ausnahmetabelle > Ausnahme für die Absenderverifizierung hinzufügen..**
2. Hinzufügen der lokalen Domäne zur Ausnahmetabelle für die Absenderverifizierung
3. Legen Sie *Verhalten* an **Ablehnen**

Überprüfen

An diesem Punkt werden E-Mails, die von *Ihrer Domäne* auf *Ihre Domäne* kommen, abgelehnt, es sei denn, der Absender wird in der Absendergruppe SPOOF_ALLOW aufgeführt, da er einem MFP zugeordnet ist, der die Ausnahmetabelle für die Absenderverifizierung nicht verwendet.

Ein Beispiel hierfür ist das Abschließen einer manuellen Telnet-Sitzung mit dem 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
```

Die 553 SMTP-Antwort ist ein direktes Antwortergebnis aus der Ausnahmetabelle, die auf der ESA wie oben beschrieben konfiguriert wurde.

In den Mail-Protokollen wird die IP-Adresse 192.168.0.9 nicht in der gültigen IP-Adresse für die richtige Absendergruppe angezeigt:

```
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
```

Eine zulässige IP-Adresse, die mit dem oben beschriebenen Konfigurationsbeispiel übereinstimmt, wird wie folgt angezeigt:

```
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
```

Zugehörige Informationen

- ESA, SMA und WSA Grep mit Regex to Search Logs
- Bestimmung der ESA-Nachrichtenverteilung
- Technischer Support und Dokumentation - Cisco Systems