Protección de suplantación mediante verificación de remitente

Contenido

Introducción

De forma predeterminada, el dispositivo de seguridad Cisco Email Security Appliance (ESA) no impide la entrega entrante de mensajes que se dirigen "desde" el mismo dominio y se dirigen al mismo dominio. Esto permite que los mensajes sean "falsificados" por empresas externas que hacen negocios legítimos con el cliente. Algunas empresas confían en que una organización externa envíe mensajes de correo electrónico en nombre de la empresa, como Health Care, Travel Agencies, etc.

Protección de suplantación mediante verificación de remitente

Configuración de la política de flujo de correo (MFP)

1. Desde la GUI: **Políticas de correo > Políticas de flujo de correo > Agregar política...**
2. Cree una nueva MFP utilizando un nombre que sea relevante como SPOOF_ALLOW
3. En la sección *Verificación del Remitente*, cambie la configuración *Usar Tabla de Excepción de Verificación del Remitente* de **Usar valor predeterminado** a *Desactivado*.
4. En **Políticas de Correo > Políticas de Flujo de Correo > Parámetros de Política Predeterminada**, establezca la configuración *Usar Tabla de Excepción de Verificación de Remitente* en **On**.

Configurar HAT

1. Desde la GUI: **Políticas de correo > Descripción general de HAT > Agregar grupo de remitentes...**
2. Establezca el nombre en consecuencia en la MFP creada anteriormente, es decir, SPOOF_ALLOW.
3. Configure el pedido de modo que esté por encima de los grupos de remitentes ALLOWLIST y BLOCKLIST.
4. Asigne la política **SPOOF_ALLOW** a esta configuración de Grupo de Enviadores.
5. Haga clic en **Enviar y agregar remitentes...**
6. Agregue IP o dominios para cualquier parte externa que desee permitir que suplanten el dominio interno.

Configurar tabla de excepciones

1. Desde la GUI: **Políticas de correo > Tabla de excepciones > Excepción de verificación de remitente...**

2. Agregar el dominio local a la tabla de excepción de verificación de remitente
3. Establecer el *Comportamiento* a **Rechazar**

Verificación

En este momento, el correo que viene de *su.dominio* a *su.dominio* se rechazaría a menos que el remitente aparezca en la lista SPOOF_ALLOW del grupo de remitentes, ya que se asociaría a una MFP que no utiliza la tabla de excepciones de verificación del remitente.

Un ejemplo de esto se vería al completar una sesión telnet manual para el receptor:

```
$ 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 respuesta 553 SMTP es un resultado directo de la tabla de excepciones tal como se configuró en el ESA a partir de los pasos anteriores.

En los registros de correo, puede ver que la dirección IP de 192.168.0.9 no se encuentra en la dirección IP válida para el grupo de remitentes correcto:

```
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
```

Una dirección IP permitida que coincida con el ejemplo de configuración de los pasos anteriores se vería de la siguiente manera:

```
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
```

Información Relacionada

- Saldo de ESA, SMA y WSA con respecto a los registros de búsqueda
- Determinación de la disposición del mensaje ESA
- Soporte Técnico y Documentación - Cisco Systems