Protección del spoof usando la verificación del remitente

Contenido

Introducción

Por abandono el dispositivo de seguridad del correo electrónico de Cisco (ESA) no previene la salida entrante de los mensajes que se dirigen “” del mismo dominio que va al mismo dominio. Esto permite que los mensajes sean “spoofed” por las compañías exteriores que legitiman el negocio con el cliente. Algunas compañías confían en la organización de otras compañías para enviar el correo electrónico en nombre de la compañía tal como atención sanitaria, agencias de viajes, etc.

Protección del spoof usando la verificación del remitente

Directiva del flujo de correo de la configuración (MFP)

1. Desde la GUI: **Envíe la directiva de las directivas > de las directivas del flujo de correo > Add…**
2. Cree un nuevo MFP usando un nombre que sea relevante como SPOOF_ALLOW
3. En la sección de la *verificación del remitente*, cambie la configuración de la *tabla de la excepción de la verificación del remitente del uso del* **valor por defecto del uso a APAGADO**.
4. En las **directivas del correo > las directivas del flujo de correo > los parámetros de la política predeterminada**, fije la configuración de la *tabla de la excepción de la verificación del remitente del uso a* **encendido**.

Configure el SOMBRERO

1. Desde la GUI: **Envíe el grupo del remitente de las directivas > de la descripción del SOMBRERO > Add…**
2. Fije el nombre por consiguiente al MFP creado anterior, es decir SPOOF_ALLOW.
3. Fije la orden así que está sobre los grupos del remitente WHITELIST y de la LISTA NEGRA.
4. Asigne la directiva **SPOOF_ALLOW a las** configuraciones de grupo de este remitente.
5. El tecleo **somete y agrega los remitentes…**
6. Agregue el IP o los dominios para cualquier partido externo que usted quiera para permitir al spoof el dominio interno.

Configure la tabla de la excepción

1. Desde la GUI: **Envíe las directivas > la excepción de la verificación del remitente de la tabla**

de la excepción > Add…

2. Agregue el dominio local a la tabla de la excepción de la verificación del remitente
3. Fije el *comportamiento* **para rechazar**

Verificación

En este momento, el correo que viene de *your.domain a* your.domainwould se rechace a menos que el remitente se enumere en el grupo SPOOF_ALLOW del remitente, pues sería asociado a un MFP que no utiliza la tabla de la excepción de la verificación del remitente.

Un ejemplo de esto sería considerado completando a una sesión telnet manual al módulo de escucha:

```
$ 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 de 553 S TP es un resultado de la respuesta directa de la tabla de la excepción según lo configurado en el ESA de los pasos arriba.

De los registros del correo, usted puede ver que la dirección IP de 192.168.0.9 no está en el IP Address válido para el grupo correcto del remitente:

```
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 corresponde con con los ejemplos de configuración de los pasos antedichos sería considerada como sigue:

```
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

- Grep ESA, S A, y WSA con Regex para buscar los registros
- Determinación de la disposición del mensaje ESA
- Soporte Técnico y Documentación - Cisco Systems