Contenido

Introducción

¿Por abandono el dispositivo de seguridad del correo electrónico de Cisco (ESA) no previene la salida entrante de los mensajes se dirigen que? ¿de? el 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:

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:

Una dirección IP permitida que corresponde con con los ejemplos de configuración de los pasos antedichos sería considerada como sigue:

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