

¿Cómo puede un Firewall o el proxy S TP afectar a los servicios ESMTP?

Contenido

[Pregunta](#)

[Respuesta](#)

[Información Relacionada](#)

Pregunta

¿Cómo puede un Firewall o el proxy S TP afectar a los servicios ESMTP?

Respuesta

Conjuntamente con el correo que procesa a través de un dispositivo de seguridad del correo electrónico de Cisco (ESA), hay varios Firewall y los servicios de representación S TP disponibles que proporcionan las características significadas para proteger los servidores del correo contra el exploit.

Algunos de estos métodos de protección pueden impedir los servicios ESMTP tales como autenticación de TLS y S TP.

Los servicios, tales como autenticación de TLS y S TP, el uso ESMTP (S TP extendido) ordenan. Para acceder el comando set ESMTP, el comando EHLO debe alcanzar el servidor de recepción. Algún Firewall y funciones de seguridad del proxy bloquearán o modificar el comando EHLO adentro transite. Cuando el dispositivo de seguridad no permite EHLO, no hay servicios ESMTP disponibles. En este caso, solamente los comandos S TP especificados en la sección 4.5.1 del [RFC 821](#) se permiten en un mail server. Estos incluyen: HELO, CORREO, RCPT, DATA, RSET, NOOP, y SALIDO. No hay comandos ESMTP disponibles.

Otra función de seguridad usada por estos dispositivos es modificación del anuncio SMTP. Para ocultar el tipo y la versión del mail server protegido, algunos dispositivos obscurecerán todos pero las 220 porciones del banner que se requiere para la comunicación.

El banner aparecerá a menudo similar a:

```
220*****
```

La parte de la información que es ocultada es el anuncio ESMTP en el banner. Cuando se quita este anuncio, un servidor de envío no será consciente que los comandos ESMTP están validados.

En resumen, los Firewall y los servidores proxy S TP pueden bloquear los comandos EHLO y ocultar los anuncios del banner ESMTP. Cuando estas medidas de seguridad existen, los

comandos ESMTP pueden no ser accesibles. Para asegurarse de que otros host puedan comunicar con su ESA usando el ESMTP, usted puede necesitar inhabilitar estas funciones de seguridad en su dispositivo de seguridad

Información Relacionada

- [Prueba de la función de vigilancia de correo del firewall PIX](#)
- [Cisco PIX: Funciones avanzadas y guardias del ataque](#)
- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)