¿SenderBase funciona correctamente detrás del NAT?

Contenido

Introducción

Este documento describe SenderBase y sus funciones detrás del Network Address Translation (NAT) para el dispositivo de seguridad del correo electrónico de Cisco (ESA).

¿SenderBase funciona correctamente detrás del NAT?

SenderBase es un servicio basado en IP de la reputación que asigna las calificaciones del servicio de la reputación de SenderBase (SBR) a los IP Addresses. SenderBase anota el rango a partir de la -10 a +10, que refleja la probabilidad que una dirección IP de envío intenta enviar Spam. Las calificaciones altamente negativas indican a los remitentes que son muy probables enviar el Spam; las calificaciones altamente positivas indican a los remitentes que son poco probables enviar el Spam.

El módulo de escucha S TP en un ESA hace las interrogaciones de la calificación SBR usando las interrogaciones DNS basadas en la dirección IP de la conexión TCP entrante. Si la dirección IP que el dispositivo del correo electrónico ve es el direccionamiento “real” del remitente, entonces los SBR funcionan como se esperaba.

> Nota: Si un Firewall utiliza el NAT para la dirección IP de origen, no insertará un nuevo encabezado del mensaje que contenga la dirección IP de la fuente original. Sin un encabezado del mensaje que contenga el IP Address original, la función de relay entrante no trabajará. Sin la información de encabezado para la dirección IP de origen, el ESA no puede determinar el IP Address de la fuente original.

La mayoría de las empresas que utilizan el NAT para ocultan tan a las direcciones internas de Internet (o porque no tienen suficientes IP Addresses a actuar sin una función NAT o del NAPT). En esos casos, SenderBase trabaja con éxito porque la dirección IP del remitente externo no se modifica de ninguna manera.

Algunas empresas con más topologías de red compleja hacen la traducción de dirección de red o las conexiones proxy hacia el interior de sus redes. En esos casos, las interrogaciones de SenderBase no trabajarán correctamente y se deben inhabilitar en el módulo de escucha entrante. (del CLI, el **listenerconfig > edita > puesto**.)

Si usted tiene alguna duda si se están convirtiendo los direccionamientos o no o si las conexiones proxied, examine simplemente el archivo de los mail_logs (utilice un comando CLI tal como **mail_logs de la cola**). Esto muestra le cada conexión entrante a cada módulo de escucha, y le podrá rápidamente ver si los IP Addresses que el ESA ve es del Internet general o no.

> Nota: Tenga cuidado de mirar solamente las conexiones a los módulos de escucha públicos o entrantes en los registros del correo ESA.

Información Relacionada

- Guías del usuario del dispositivo de seguridad del correo electrónico de Cisco
- Soporte Técnico y Documentación - Cisco Systems