Configuración de la función de rechazo de Cisco ASA para eximir al dispositivo virtual

Contenido

Introducción

Este documento describe cómo configurar Cisco ASA para eximir el dispositivo virtual del componente de detección de amenazas. El componente de detección de amenazas de Cisco ASA realiza una inspección de paquetes en DNS y otros protocolos. Umbrella support recomienda estos cambios de configuración de ASA para evitar que esta función entre en conflicto con nuestro dispositivo virtual:

- Exima el dispositivo virtual de la función "rechazar" de detección de amenazas, como se describe en este artículo.
- Exima al dispositivo virtual de la inspección de paquetes DNS para permitir el cifrado DNS (DNScrypt) que se trata en este artículo: El firewall Cisco ASA bloquea DNScrypt.

Función "Shun" de detección de amenazas

Cuando la función "Shun" está activada, el ASA puede bloquear por completo una dirección IP de origen que active reglas de detección de amenazas. Encontrará más información en el artículo de Cisco: Funcionalidad y configuración de la detección de amenazas ASA.

El dispositivo virtual normalmente envía un número muy alto de consultas DNS a los resolvers de Umbrella DNS. En los casos en los que exista un problema local de conexión con los solucionadores (como una interrupción o latencia temporal de la red), estas consultas pueden fallar. Debido al gran volumen de consultas que se envían, incluso un pequeño porcentaje de errores hace que el ASA rechace el dispositivo virtual; lo que provoca una interrupción completa del DNS durante un período de tiempo.

Exención del dispositivo virtual

Nota: Los comandos de este artículo sólo sirven de guía y se recomienda consultar a un experto de Cisco antes de realizar cambios en un entorno de producción.

A través de CLI:

- Para eximir el rechazo de la IP del dispositivo, ejecute este comando: **no shun**

Vía la interfaz ASDM:

- Elija el panel Configuration > Firewall > Threat Detection.
- Para eximir la dirección IP del dispositivo de que no se rechace, introduzca una dirección en el campo 'Redes excluidas del rechazo'. Puede introducir varias direcciones o subredes separadas por comas.

Determine si el dispositivo ha sido 'rechazado'

Si no se han seguido estos pasos, el dispositivo podría "rechazarse" en algunas circunstancias, lo que provocaría una interrupción del DNS.

Cuando el dispositivo virtual no tiene conectividad externa, la consola de Cisco ASA registra el evento de la siguiente manera:

4|6 de junio de 2014 14:00:42|401004: Paquete rechazado: 192.168.1.3 ==> 208.67.222.222 en la interfaz interior
4|6 de junio de 2014 14:00:42|401004: Paquete rechazado: 192.168.1.3 ==> 208.67.222.222 en la interfaz interior

Para ver una lista de direcciones IP rechazadas actualmente, ejecute este comando en el ASA: **show shun**

Para borrar inmediatamente las direcciones IP rechazadas actualmente, ejecute este comando en el ASA: **clear shun**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).