Contenido

Introducción

Este documento describe diversos escenarios con el Marco de políticas del remitente (SPF) en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Prerequiste

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ESA
- Todas las versiones de AsyncOS

¿Cuál es SPF?

El Marco de políticas del remitente (SPF) es correo electrónico simple un sistema de la validación diseñado para detectar el spoofing del email proporcionando a un mecanismo para permitir el recibir de los cambiadores de correo para marcar que el correo entrante de un dominio se está enviando de un host autorizado por los administradores de ese dominio. La lista de host de envío autorizados para un dominio se publica en los expedientes del Domain Name System (DNS) para ese dominio bajo la forma de expediente especialmente formatado de TXT. Los direccionamientos forjados uso del remitente del Spam y del phishing del correo electrónico a menudo, así que la publicación y marcar de los expedientes SPF se pueden considerar las técnicas del anti-Spam.

¿Habrá mucho impacto del rendimiento en los ESA?

De la perspectiva CPU, no habrá impacto del rendimiento enorme. Sin embargo, habilitar la verificación SPF aumentará las interrogaciones del número DNS y el tráfico DNS. Para cada mensaje, el ESA pudo tener que iniciar 1-3 interrogaciones SPF DNS y éste dará lugar al caché de expiración DNS anterior entonces antes. Por lo tanto, el ESA generará más interrogaciones para los otros procesos también.

Además de la información previa, el expediente SPF será un expediente del .TXT que puede ser más grande entonces los expedientes normales DNS y podría causar un cierto tráfico adicional DNS.

¿Cómo usted habilita el SPF?

Estas instrucciones son del guía del usuario anticipado en configurar la verificación SPF:

Para habilitar el formato de datos independiente SPF/System (SIDF) en la directiva predeterminada del mailflow:

1. **Directivas del correo del** tecleo **> directiva del flujo de correo**.
2. **Parámetros de la política predeterminada del** tecleo.
3. En los parámetros de la política predeterminada, vea la sección de las **funciones de seguridad**.
4. En la sección de la verificación SPF/SIDF, haga clic **sí**.
5. Fije el nivel de conformidad (el valor por defecto es SIDF-compatible). Esta opción permite que usted determine que estándar de la verificación SPF o SIDF a utilizar. Además de la conformidad SIDF, usted puede elegir SIDF-compatible, que combina el SPF y SIDF.
6. Si usted elige una conformidad llana de SIDF-compatible, configuración si la verificación retrocede un resultado del **paso de la** identidad del PRA a **ningunos** si hay Volver a enviar-remitente: o Volver a enviar-de: encabezados presentes en el mensaje. Usted puede ser que elija los propósitos de esta opción de seguridad.
7. Si usted elige una conformidad llana del SPF, configure si realizar una prueba contra la identidad HELO. Usted puede ser que utilice esta opción para mejorar el funcionamiento inhabilitando el control HELO. Esto puede ser útil, porque la regla para filtros SPF-pasajera marca el PRA o el CORREO de las identidades primero. El dispositivo realiza solamente la comprobación para HELO el nivel de la conformidad SPF.

Para tomar medidas en los resultados de la verificación SPF, agregue por favor los filtros contentos:

1. Cree un filtro del contenido del SPF-estatus para cada tipo de verificación SPF/SIDF. Utilice a una convención para nombres para indicar el tipo de verificación. Por ejemplo, utilice SPF-**pasado** para los mensajes que pasan la verificación SPF/SIDF, o el **SPF-TempErr** para los mensajes que no fueron pasados debido a un error transitorio durante la verificación. Para la información sobre crear un filtro del contenido del SPF-estatus, vea la regla para filtros contenta del SPF-estatus en el GUI.

2. Después de que usted procese varios mensajes SPF/SIDF-verified, haga clic los **filtros del monitor > del contenido** para ver cuántos mensajes accionaron cada uno de los filtros del contenido SPF/SIDF-verified.

¿Qué la “prueba del helicóptero” por intervalos significa? ¿Qué sucederá si la prueba del helicóptero falla de cierto dominio?

Si usted elige una conformidad llana del SPF, configure si realizar una prueba contra la identidad HELO. Usted puede ser que utilice esta opción para mejorar el funcionamiento inhabilitando el control HELO. Esto puede ser útil porque la regla para filtros SPF-pasajera marca el PRA o el CORREO de las identidades primero. El dispositivo realiza solamente la comprobación para HELO el nivel de la conformidad SPF.

Expedientes válidos SPF

Para pasar el control SPF HELO, asegúrese de que usted incluye un expediente SPF para cada MTA de envío (a parte del dominio). Si usted no incluye este expediente, el control HELO dará lugar probablemente a un **ninguno** veredicto para la identidad HELO. Si usted nota que los remitentes SPF a su dominio vuelven un número alto de **ningunos los** veredictos, estos remitentes pudieron no haber incluido un expediente SPF para cada MTA de envío.

El mensaje será entregado si no hay filtros del mensaje/del contenido configurados. Una vez más usted puede tomar ciertas medidas usando los filtros del mensaje/del contenido para cada veredicto SPF/SIDF.

¿Cuál es la mejor manera de habilitarla para solamente un dominio externo?

Para habilitar el dominio SPF con certeza, usted puede ser que necesite definir un nuevo sendergroup con una directiva del flujo de correo que tiene SPF habilitado; entonces cree los filtros según lo mencionado previamente.

¿Puede usted habilitar una comprobación para SPF el Spam sospechoso?

El Anti-Spam de Cisco considera el bastantes de los factores mientras que calcula las calificaciones de spam. Tener récord comprobable SPF puede reducir la calificación de spam pero todavía hay ocasión de conseguir esos mensajes cogidos como Spam sospechoso.

La solución mejor sería a la lista blanca la dirección IP del remitente O crearía un filtro del mensaje para saltar el spamcheck con las condiciones múltiples (encabezado del IP remoto, correo-de, de X-skipspamcheck, etc.). La encabezado se puede agregar por el servidor de envío para identificar un tipo de mensaje de otros.

Información Relacionada

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