Configuración de SPF y Prácticas Recomendadas

Contenido

Introducción

Este documento describe diferentes escenarios con el marco de políticas de remitente (SPF) en Cisco Email Security Appliance (ESA).

Prerequisites

Cisco recomienda conocer estos temas:

- ESA de Cisco
- Todas las versiones de AsyncOS

¿Qué es SPF?

Sender Policy Framework (SPF) es un sencillo sistema de validación de correo electrónico diseñado para detectar la suplantación de correo electrónico al proporcionar un mecanismo que permita a los intercambiadores de correo recibir correo comprobar que el correo entrante de un dominio se envía desde un host autorizado por los administradores de ese dominio. La lista de hosts de envío autorizados para un dominio se publica en los registros del Sistema de nombres de dominio (DNS) de ese dominio en forma de un registro TXT con formato especial. El correo electrónico no deseado y la suplantación de identidad a menudo utilizan direcciones de remitentes falsificadas, por lo que publicar y comprobar registros SPF se puede considerar como técnicas antispam.

¿Habrá un gran impacto en el rendimiento de los ESA?

Desde el punto de vista de la CPU, no habrá un impacto enorme en el rendimiento. Sin embargo,

al activar la verificación SPF, aumentará el número de consultas DNS y el tráfico DNS. Para cada mensaje, el ESA puede tener que iniciar consultas de 1-3 SPF DNS y esto dará como resultado que la memoria caché DNS caduque antes que antes. Por lo tanto, la ESA también generará más consultas para los demás procesos.

Además de la información anterior, el registro SPF será un registro TXT que puede ser mayor que los registros DNS normales y podría causar tráfico DNS adicional.

¿Cómo habilita el SPF?

Estas instrucciones provienen de la guía del usuario avanzada sobre la configuración de la verificación SPF:

Para habilitar SPF/System Independent Data Format (SIDF) en la política de flujo de correo predeterminada:

1. Haga clic en **Políticas de correo > Política de flujo de correo**.
2. Haga clic en **Parámetros de política predeterminados**.
3. En los parámetros de política predeterminados, vea la sección **Funciones de seguridad**.
4. En la sección Verificación SPF/SIDF, haga clic en **Sí**.
5. Establezca el nivel de conformidad (el valor predeterminado es compatible con SIDF). Esta opción le permite determinar qué estándar de verificación SPF o SIDF debe utilizar. Además de la conformidad con el SIDF, puede elegir SIDF compatible, que combina SPF y SIDF. Los detalles de los niveles de conformidad están disponibles en la *guía del usuario final.*
6. Si elige un nivel de conformidad compatible con SIDF, configure si la verificación resta un resultado **Pass** de la identidad PRA a **None** si hay Resent-Sender: o de reenvío: encabezados presentes en el mensaje. Puede elegir esta opción por motivos de seguridad.
7. Si elige un nivel de conformidad de SPF, configure si realizar una prueba con la identidad HELO. Puede utilizar esta opción para mejorar el rendimiento desactivando la comprobación HELO. Esto puede ser útil porque la regla de filtro aprobada por spf verifica primero el PRA o las identidades MAIL FROM. El dispositivo sólo realiza la verificación HELO para el nivel de conformidad SPF.

Para tomar medidas sobre los resultados de la verificación SPF, agregue filtros de contenido:

1. Cree un filtro de contenido spf-status para cada tipo de verificación SPF/SIDF. Utilice una convención de nomenclatura para indicar el tipo de verificación. Por ejemplo, utilice **SPF-Passed** para los mensajes que pasan la verificación SPF/SIDF, o **SPF-TempErr** para los mensajes que no se pasaron debido a un error transitorio durante la verificación. Para obtener información sobre cómo crear un filtro de contenido de estado de spf, vea la regla de filtro de contenido de estado de spf en la GUI.
2. Después de procesar algunos mensajes verificados por SPF/SIDF, haga clic en **Monitor > Content Filters** para ver cuántos mensajes desencadenaron cada uno de los filtros de contenido verificados por SPF/SIDF.

¿Qué significa "Helo Test" activado y desactivado? ¿Qué ocurrirá si la prueba de Helo falla desde un dominio determinado?

Si elige un nivel de conformidad de SPF, configure si realizar una prueba con la identidad HELO. Puede utilizar esta opción para mejorar el rendimiento desactivando la comprobación HELO. Esto puede ser útil porque la regla de filtro aprobada por spf verifica primero el PRA o las identidades MAIL FROM. El dispositivo sólo realiza la verificación HELO para el nivel de conformidad SPF.

Registros SPF válidos

Para pasar la verificación HELO SPF, asegúrese de incluir un registro SPF para cada MTA de envío (separado del dominio). Si no incluye este registro, la verificación HELO probablemente dará lugar a un veredicto **None** para la identidad HELO. Si observa que los remitentes SPF a su dominio devuelven un número elevado de veredictos **None**, es posible que estos remitentes no hayan incluido un registro SPF para cada MTA de envío.

El mensaje se entregará si no hay ningún filtro de contenido/mensaje configurado. Una vez más, puede realizar ciertas acciones utilizando filtros de mensajes/contenido para cada veredicto SPF/SIDF.

¿Cuál es la mejor manera de habilitarlo para un solo dominio externo?

Para habilitar el SPF para un dominio determinado, es posible que necesite definir un nuevo grupo de remitentes con una política de flujo de correo que tenga SPF habilitado; a continuación, cree filtros como se mencionó anteriormente.

¿Puede activar una verificación SPF para detectar spam sospechoso?

Cisco Anti-Spam tiene en cuenta muchos factores al calcular las puntuaciones de spam. Tener un registro SPF verificable puede reducir la puntuación de spam, pero todavía existe la posibilidad de que los mensajes sean capturados como spam sospechoso.

La mejor solución posible sería permitir la lista de direcciones IP del remitente O crear un filtro de mensajes para saltar la comprobación de spam con varias condiciones (dirección IP remota, correo electrónico de, encabezado X-skipspamcheck, etc.). El servidor de envío puede agregar el encabezado para identificar un tipo de mensajes de otros.

Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance - Guías de usuario final
- Prácticas recomendadas de autenticación de correo electrónico: implementación de SPF/DKIM/DMARC
- Soporte Técnico y Documentación - Cisco Systems