¿Cuáles son las prácticas recomendadas para utilizar SenderBase?

Contenido

Introducción

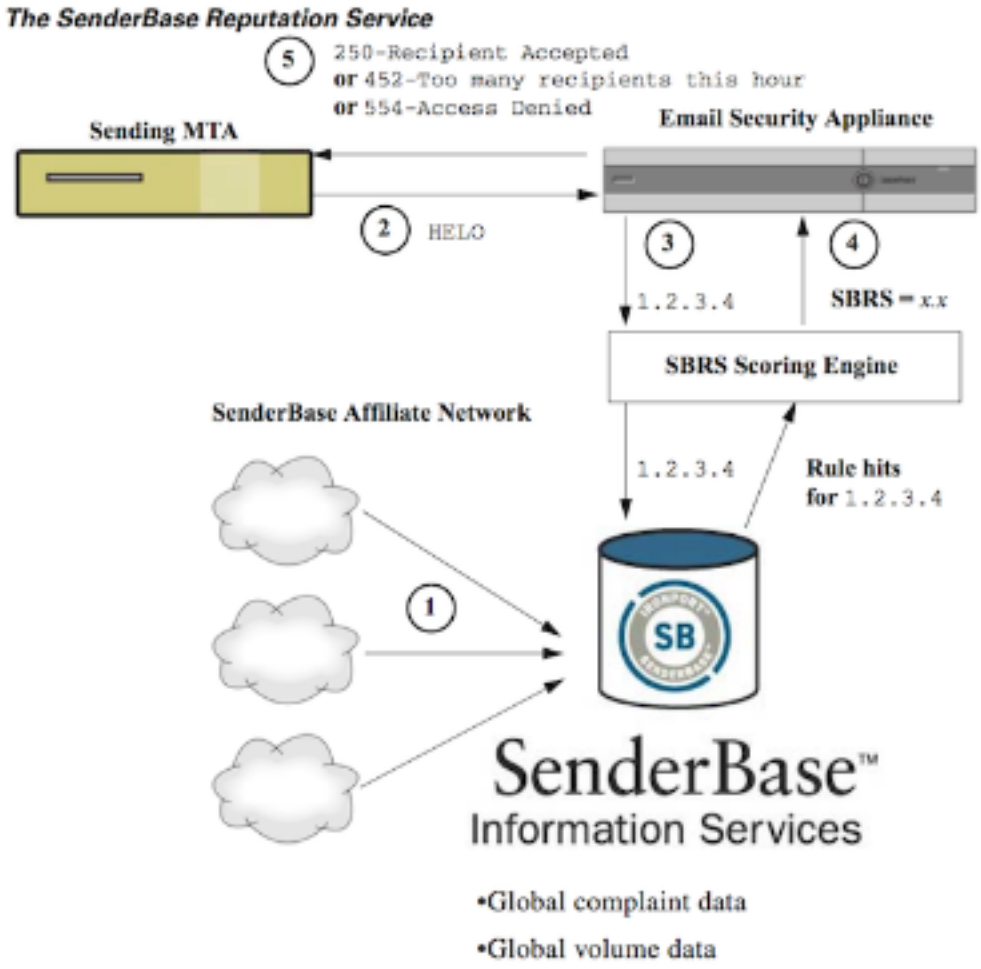
Este documento describe las prácticas recomendadas para utilizar SenderBase.

¿Cuáles son las prácticas recomendadas para utilizar SenderBase?

El servicio SenderBase Reputation Service (SBRS) proporciona una forma precisa y flexible de rechazar o limitar los sistemas sospechosos de transmitir spam basándose en la dirección IP de conexión del host remoto. El SBRS devuelve una puntuación basada en la probabilidad de que un mensaje de una fuente dada sea spam, que va desde -10 (seguro que es spam) hasta +10 (seguro que no es spam). Aunque SBRS se puede utilizar como una solución antispam independiente, es más eficaz cuando se combina con un analizador antispam basado en contenido.

Las puntuaciones de SenderBase se pueden utilizar en la tabla de acceso de host (HAT) de un receptor SMTP para asignar conexiones SMTP entrantes a diferentes grupos de remitentes. Cada grupo de remitentes tiene asociada una política que afecta a la forma en que se maneja el correo entrante. Lo más común con las puntuaciones de SenderBase es rechazar el correo por completo o limitar el remitente sospechoso de spam.

Puede utilizar puntuaciones SBRS en HAT para rechazar o limitar el correo electrónico. También puede crear filtros de mensajes para especificar "umbrales" para las puntuaciones SBRS para actuar en mayor medida en los mensajes procesados por el sistema. El siguiente diagrama proporciona un esquema aproximado de cómo se pueden utilizar las puntuaciones SBRS para bloquear o limitar los remitentes sospechosos:



1. Los afiliados de SenderBase envían datos globales en tiempo real.
2. El envío de MTA abre la conexión con el dispositivo.
3. El dispositivo verifica los datos globales para la dirección IP de conexión.
4. SenderBase Reputation Service calcula la probabilidad de que este mensaje sea spam y asigna una puntuación de reputación de SenderBase.
5. El dispositivo devuelve la respuesta (rechazando el correo electrónico o limitando el remitente) en función de la puntuación de reputación de SenderBase.

El modo en que utilice las puntuaciones SBRS dependerá de la agresividad con la que desee estar en el filtrado previo de correos electrónicos. El dispositivo de seguridad Email Security Appliance (ESA) ofrece tres estrategias diferentes para implementar SenderBase:

- **Conservador**: Un enfoque conservador es bloquear mensajes con una puntuación de reputación de SenderBase inferior a -7.0, limitar entre -7.0 y -2.0, aplicar la política predeterminada entre -2.0 y +6.0, y aplicar la política de confianza para los mensajes con una puntuación mayor que +6.0. El uso de este enfoque garantiza una tasa de falsos positivos cercana a cero al tiempo que se logra un mejor rendimiento del sistema.
- **Moderado:** Un enfoque moderado es bloquear mensajes con una puntuación de reputación de SenderBase inferior a -4.0, limitar entre -4.0 y 0, aplicar la política predeterminada entre 0 y +6.0 y aplicar la política de confianza para los mensajes con una puntuación mayor que +6.0. El uso de este enfoque garantiza una tasa de falsos positivos muy pequeña al tiempo que se logra un mejor rendimiento del sistema (ya que se elimina más correo del procesamiento antispam).
- **Agresivo:** Un enfoque agresivo es bloquear mensajes con una puntuación de reputación de SenderBase inferior a -1.0, limitar entre -1.0 y 0, aplicar la política predeterminada entre 0 y

+4.0 y aplicar la política de confianza para los mensajes con una puntuación mayor que +4.0. Con este enfoque, podría incurrir en falsos positivos; sin embargo, este enfoque maximiza el rendimiento del sistema al desviar la mayor parte del correo del procesamiento antispam.

La siguiente tabla resume estas tres políticas:

Enfoque	Características	Lista permitida	Lista de bloqueo	Lista de sospechosos	Lista desconocida
		Rango de puntuación de reputación de base del remitente:			
Conservador	Casi cero falsos positivos, mejor rendimiento	7 a 10	-10 a -4	-4 a -2	-2 a 7
Moderado (predeterminado)	Muy pocos falsos positivos, alto rendimiento	No se utilizan las puntuaciones de reputación de la base del remitente.	-10 a -3	-3 a -1	-1 a +10
Agresivo	Algunos falsos positivos, máximo rendimiento Esta opción evita que el correo se procese con más frecuencia.	4 a 10	-10 a -2	-2 a -1	-1 a 4
Todos los enfoques		Política de flujo de correo: De confianza	Bloqueado	Tramitado	Aceptado

Implementación de Regulación o Bloqueo de SenderBase

La mejor manera de utilizar las puntuaciones de SenderBase significa seguir una metodología simple de 2 partes. Primero, usted decide su política (por ejemplo, podría comenzar con la política "Conservadora" anterior) y mapear esa política a los Grupos de Enviadores. A continuación, asigne esos grupos de remitentes a la política que desee. El ESA ya ha creado una matriz de grupos de remitentes y políticas de flujo de correo que puede servir como plantilla para la implementación del SBRS.

Para implementar la regulación de SenderBase basada en la política predeterminada, editará los cuatro grupos de remitentes (lista de permitidos, lista de bloqueo, lista de sospechosos y lista desconocida) en Políticas de correo > Descripción general de tabla de acceso de host (HAT). Comience haciendo clic en el grupo de remitentes "Allowlist". A continuación, mediante el menú desplegable de la ficha Enviadores, haga clic en "Agregar remitente" con la opción "Puntuación de reputación de SenderBase (SBRS)" seleccionada. Esto agregará una línea SBRS a la lista de remitentes. Rellene su rango de puntuación SBRS (en este caso 6.0 a 10.0) y haga clic en el botón **Enviar**.

La política para el grupo de remitentes Allowlist es "Trusted". De forma predeterminada, esta política omitirá el procesamiento antispam, lo que aumentará el rendimiento del sistema. Debido a que es muy poco probable que los remitentes con puntuaciones SBRS muy altas envíen spam, este solo paso aumentará el rendimiento. Edite los tres grupos de remitentes restantes para agregar puntuaciones SBRS, según la tabla siguiente:

Grupo de remitentes	Rango	Resultado

Lista permitida	6 a 10	No se escanearán los remitentes de calidad conocidos
Lista desconocida	-2 a +6	Los remitentes con poca información serán escaneados normalmente
Lista de sospechosos	-7 a -2	Los remitentes con mala reputación se verán fuertemente limitados para reducir cantidad de spam que pueden enviar
Lista de bloqueo	-10 a -7	El correo de spammers conocidos será rechazado en el momento SMTP con una respuesta 5xx

Cuando haya terminado de agregar rangos de puntuación, no olvide hacer clic en "**Registrar cambios**". Cuando agregue reglas de puntuación SBRS a grupos de remitentes existentes, colóquelas en la parte inferior de la lista de remitentes de cualquier grupo. El orden importa al definir los grupos de remitentes en HAT de un receptor, ya que los grupos se evalúan de arriba hacia abajo y, dentro de cada grupo, cada regla se evalúa individualmente, de arriba hacia abajo. En una HAT, se utilizará la primera regla que coincida con un remitente para seleccionar una política. Si una conexión entrante de un dominio de envío tiene una puntuación SBRS definida y coincide con el rango en una regla de HAT del receptor, se aplicará la política de flujo de correo, incluso si otras reglas más abajo en la lista de grupos de remitentes también pueden coincidir.

Si su política para colocar remitentes en grupos de remitentes requiere que se evalúen todas las reglas que no son de SBRS antes de considerar las puntuaciones SBRS, simplemente puede agregar cuatro nuevos grupos de remitentes al final de la lista de grupos de remitentes existentes específicamente para la coincidencia de políticas SBRS junto con sus políticas relevantes.

Información Relacionada

- Preguntas frecuentes sobre SenderBase
- Soporte Técnico y Documentación - Cisco Systems