¿Cuáles son las mejores prácticas para usar SenderBase?

Contenido

Introducción

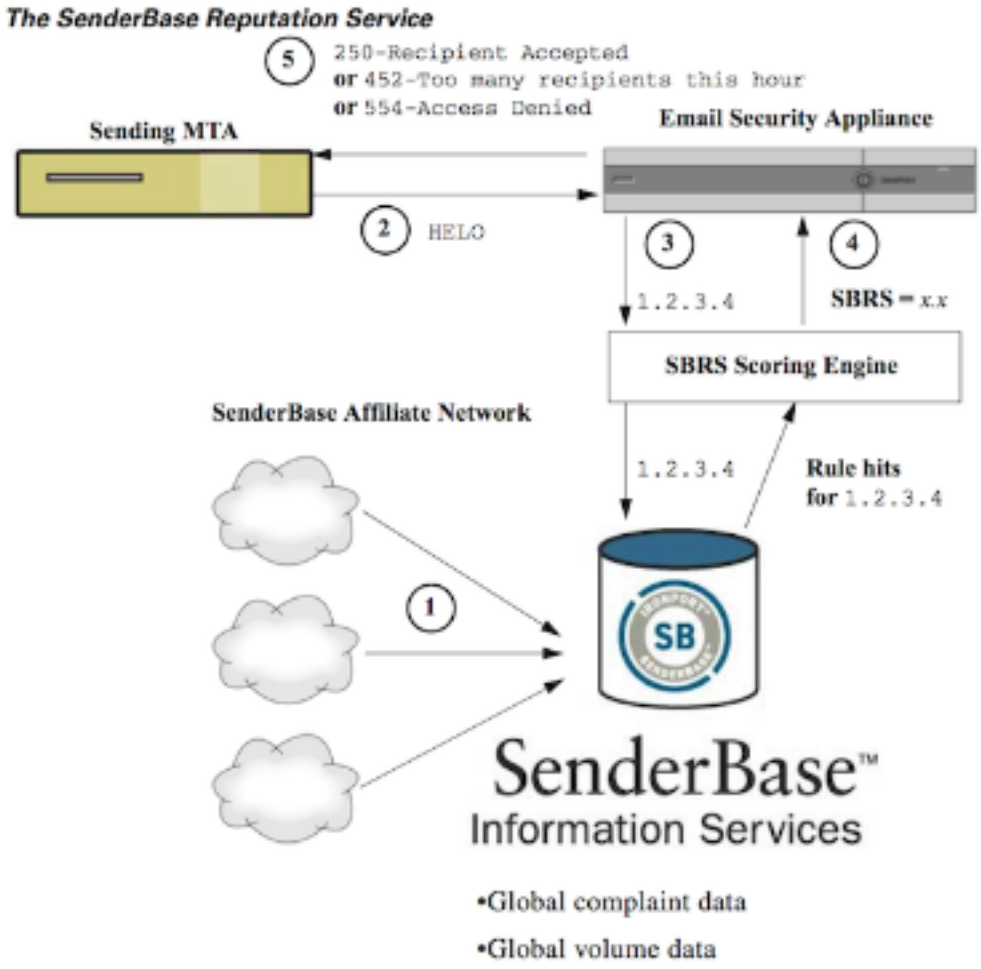
Este documento describe las mejores prácticas para usar SenderBase.

¿Cuáles son las mejores prácticas para usar SenderBase?

El servicio de la reputación de SenderBase (SBR) proporciona un exacto, la manera flexible para que usted rechace o estrangule los sistemas sospechosos para transmitir el Spam basado en la dirección IP de conexión del host remoto. Los SBR vuelven una calificación basada en la probabilidad que un mensaje de una fuente dada es Spam, extendiéndose a partir de la -10 (seguro de ser Spam) con 0 a +10 (seguro de no ser Spam). Aunque los SBR se puedan utilizar como solución independiente del anti-Spam, es la más eficaz cuando está combinada con un escáner contenido-basado del anti-Spam.

Las calificaciones de SenderBase se pueden utilizar en la tabla del acceso del host (SOMBRERO) en un módulo de escucha S TP para asociar las conexiones SMTP entrantes a diversos grupos del remitente. Cada grupo del remitente ha asociado a él una directiva que afecta a cómo se maneja el correo electrónico entrante. Las cosas mas comunes a hacer con las calificaciones de SenderBase están al correo del rechazo totalmente, o para estrangular el remitente sospechoso del Spam.

Usted puede utilizar las calificaciones SBR en el SOMBRERO para rechazar o para estrangular el correo electrónico. Usted puede también crear los filtros del mensaje para especificar los “umbrales” para que las calificaciones SBR actúen más lejos sobre los mensajes procesados por el sistema. El diagrama a continuación proporciona un áspero delinea de cómo las cuentas SBR se pueden utilizar para bloquear o para estrangular los remitentes sospechosos:



1. Los afiliados de SenderBase envían los datos en tiempo real, globales.
2. El envío del MTA abre la conexión con el dispositivo.
3. El dispositivo marca los datos globales para la dirección IP de conexión.
4. El servicio de la reputación de SenderBase calcula la probabilidad que este mensaje es Spam y asigna una calificación de las reputaciones de SenderBase.
5. El dispositivo vuelve la respuesta (rechazando el correo electrónico o estrangulando el remitente) basada en la calificación de la reputación de SenderBase.

Cómo usted utiliza las calificaciones SBR dependerán de cómo es agresivo usted quiere estar en el correo electrónico de PRE-filtración. El dispositivo de seguridad del email (ESA) ofrece tres diversas estrategias para implementar SenderBase:

- **Conservador**: Un enfoque conservador es bloquear los mensajes con una calificación de la reputación de SenderBase más bajo de -7.0, estrangular entre -7.0 y -2.0, aplicar la política predeterminada entre -2.0 y +6.0, y aplicar la directiva de confianza para los mensajes con una calificación mayor de +6.0. Usando este acercamiento asegura una tarifa cero cercana del falso positivo mientras que alcanza un mejor rendimiento del sistema.
- **Moderado:** Un acercamiento moderado es bloquear los mensajes con una calificación de la reputación de SenderBase más bajo de -4.0, estrangular entre -4.0 y 0, aplicar la política predeterminada entre 0 y +6.0, y aplicar la directiva de confianza para los mensajes con una calificación mayor de +6.0. Usando este acercamiento asegura una tarifa muy pequeña del falso positivo mientras que alcanza un mejor rendimiento del sistema (porque más correo se desvía lejos del Anti-Spam que procesa).
- **Agresivo:** Un acercamiento agresivo es bloquear los mensajes con una calificación de la reputación de SenderBase más bajo de -1.0, estrangular entre -1.0 y 0, aplicar la política

predeterminada entre 0 y +4.0, y aplicar la directiva de confianza para los mensajes con una calificación mayor de +4.0. Usando este acercamiento, usted puede ser que incurra en algunos falsos positivos; sin embargo, este acercamiento maximiza el rendimiento del sistema desviando la mayoría del correo lejos del proceso del Anti-Spam.

El gráfico y la tabla abajo resume estas tres directivas:

Approach	Characteristics	Whitelist	Blacklist	Suspectlist	Unknownlist
		Sender Base Reputation Score range:			
Conservative	Near zero false positives, better performance	7 to 10	-10 to -4	-4 to -2	-2 to 7
Moderate (Installation default)	Very few false positives, high performance	Sender Base Reputation Scores are not used.	-10 to -3	-3 to -1	-1 to +10
Aggressive	Some false positives, maximum performance. This option shunts the most mail away from Anti-Spam processing.	4 to 10	-10 to -2	-2 to -1	-1 to 4
		Mail Flow Policy:			
All approaches		Trusted	Blocked	Throttled	Accepted

Implementar SenderBase que estrangula o bloqueo

La mejor manera de utilizar las calificaciones de SenderBase significa el siguiente de una metodología simple, en dos partes. Primero, usted decide sobre su directiva (por ejemplo, usted podría comenzar con la directiva “conservadora” antedicha) y asocia esa directiva a los grupos del remitente. Entonces, usted asocia esos grupos del remitente a la directiva que usted quiere. El ESA ha creado ya una matriz de los grupos del remitente y de las directivas del flujo de correo que pueden servir como plantilla para su implementación de los SBR.

Para implementar estrangular de SenderBase basado en la política predeterminada, usted editará los cuatro grupos del remitente (Whitelist, lista negra, Suspectlist, y Unknownlist) en las directivas del correo > la descripción de la tabla del acceso del host (SOMBRERO). Comience haciendo clic en el grupo del remitente de “Whitelist”. Entonces, usando el menú desplegable en la lengueta de los remitentes, haga clic en “agregan el remitente” con “la cuenta de la reputación de SenderBase (SBR)” seleccionada. Esto agregará los SBR alinea a la lista de remitentes. Complete su rango de la calificación SBR (en este caso 6.0 a 10.0) y haga clic el **botón Submit Button**.

La directiva para el grupo del remitente de la lista blanca es “de confianza. ” Por abandono, esta directiva saltará el anti-Spam que procesa, que aumentará el rendimiento del sistema. Porque los remitentes con las calificaciones muy altas SBR son muy poco probable enviar el Spam, este paso solamente aumentará la producción. Edite los tres grupos restantes del remitente para agregar las calificaciones SBR, según la tabla abajo:

Grupo del remitente	Rango de la calificación	Resultado
Lista blanca	6 a 10	Los buenos remitentes sabidos no serán analizados
Unknownlist	-2 a +6	Los remitentes con poca información serán analizados normalmente
Suspectlist	-7 a -2	Los remitentes con la reputación pobre serán estrangulados pesadamente p reducir la cantidad de Spam que pueden enviar
Lista negra	-10 a -7	El correo de los spammeres sabidos será rechazado en el tiempo S TP con respuesta 5xx

Cuando le hacen que agrega los rangos de la calificación, no olvide hacer clic los “**cambios del cometer**.” Cuando usted está agregando los SBR que anotan las reglas a los grupos existentes del remitente, póngalos en la parte inferior de la lista de remitentes en cualquier grupo. Pida las materias al definir los grupos del remitente en el SOMBRERO de un módulo de escucha, como los grupos se evalúan de arriba a abajo, y dentro de cada grupo, cada regla se evalúa individualmente, de arriba a abajo. En un SOMBRERO, la primera regla que corresponde con un remitente será utilizada para seleccionar una directiva. Si una conexión entrante de un dominio de envío tiene los SBR definidos anota y hace juego el rango en una regla en el SOMBRERO del módulo de escucha, la directiva del flujo de correo será aplicado, incluso si el otro otro plumón de las reglas en la lista de grupos del remitente pudo también hacer juego.

Si su directiva para poner los remitentes en los grupos del remitente requiere que todas las reglas NON-SBR estén evaluadas antes de que se consideren las calificaciones SBR, después usted puede agregar simplemente cuatro nuevos grupos del remitente en el extremo de la lista de grupos existentes del remitente específicamente para la directiva SBR que corresponde con junto con sus directivas relevantes.

Información Relacionada

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