

¿SenderBase en Cisco Email Security Appliance (ESA) es otro DNS RBL?

Contenido

[Pregunta](#)

[Respuesta](#)

[Información Relacionada](#)

Pregunta

¿SenderBase en Cisco Email Security Appliance (ESA) es otra lista negra de DNS en tiempo real (RBL)?

Respuesta

SenderBase no es un DNS RBL normal. En la comunidad anti-spam, hay muchas listas de bloqueo basadas en DNS. Una técnica desarrollada a lo largo de los años, las listas de bloqueo basadas en DNS proporcionan una forma de agregar una API estandarizada (interfaz de programación de aplicaciones) a una base de datos ampliamente distribuida. Debido a que los dispositivos de red, como los servidores de correo, todos tienen una aplicación cliente DNS integrada (a veces denominada "resolución"), el uso del DNS para buscar información sobre las direcciones IP es una operación muy natural para la mayoría de los sistemas. La idea de una lista de bloqueo basada en DNS es proporcionar una manera fácil para una comunidad de usuarios ampliamente distribuida de consultar de manera eficiente una lista orientada a IP sin tener que preocuparse por la replicación de bases de datos, la autenticación o API más elaboradas.

La estrategia de la mayoría de las listas de bloqueo basadas en DNS es establecer alguna descripción de una lista de bloqueo (por ejemplo, "sistemas que se sabe que están abiertos") y luego permitir que cualquiera consulte la lista para ver si hay una dirección IP en la lista. Si aparece la dirección, el propietario de la lista afirma que la dirección IP cumple los requisitos para estar en la lista. En otras palabras, las listas de bloqueo basadas en DNS son respuestas "sí/no": o está en la lista o no lo está.

Por lo general, los voluntarios administran las listas de bloqueo basadas en DNS (aunque hay pocos disponibles sobre la base de una suscripción de pago). También tienden a ser muy idiosincrásicas en su funcionamiento. Como proyectos dirigidos por voluntarios, son manejados por individuos o grupos que se sienten muy fuertemente acerca del problema del spam y generalmente tienden a errar del lado del bloqueo de correo legítimo. Las empresas que han optado por utilizar listas de bloqueo basadas en DNS o bien las encuentran mínimamente eficaces para reducir el spam (es decir, es difícil aparecer en la lista y las actualizaciones de la lista no son oportunas) o bien descubren que estas listas generan una tasa muy alta de falsos positivos (es decir, es demasiado fácil aparecer en la lista).

SenderBase se creó para reducir el comportamiento idiosincrático en las listas de bloqueo basadas en DNS y permitir al administrador de red tomar sus propias decisiones sobre lo conservador o agresivamente que usarán la lista. Con el uso adecuado de SenderBase, junto con las capacidades de regulación de un ESA, la tasa de falsos positivos puede disminuir

drásticamente. Al mismo tiempo, una gran proporción del spam se mantiene fuera de la red corporativa.

Información Relacionada

- [¿Cómo actúa SenderBase?](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)