Comprender los parámetros relacionados con las políticas de flujo de correo y los controles de destino

Contenido

Introducción

Este documento describe un par de aspectos de configuración de Email Security Appliance (ESA) sobre cómo acelerar/limitar velocidad de envío y envío de remitentes. Las funciones que se describirán en el artículo son Políticas de flujo de correo y Controles de destino.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de las políticas de flujo de correo y los controles de destino
- Familiaridad con el uso de estas funciones en la configuración del ESA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Ventajas de las políticas de flujo de correo y los controles de destino

Hay una función muy importante que ambas funciones tienen, a saber, limitación/aceleración de velocidad. Este aspecto ayuda al administrador a tener control sobre qué tráfico debe fluir libremente y a cuál debe permitirse con restricciones.

Políticas de flujo de correo

Estas son las políticas que se aplican a los grupos de remitentes del ESA, en función de las cuales se realiza la modulación del tráfico de correo electrónico.

Las políticas de flujo de correo siempre se aplican al tráfico entrante en el ESA independientemente de que el correo electrónico sea entrante o saliente.

Las políticas de flujo de correo funcionan en el motor con respecto al comportamiento de conexión seleccionado para esa política. Los diferentes comportamientos de conexión disponibles en los ESA son:

1. Aceptar
2. Rechazar
3. Relay
4. Rechazo de TCP
5. Continúe

Aceptar: Se acepta la conexión y, a continuación, la aceptación del correo electrónico se ve restringida por la configuración del receptor, incluida la Tabla de acceso de destinatarios (para los receptores públicos). Este comportamiento de conexión trata un correo electrónico como entrante

Rechazar: El cliente que intenta conectarse obtiene un código de estado SMTP 4XX o 5XX. No se acepta ningún correo electrónico. Esto se utiliza principalmente para remitentes de listas negras

Relay: Se acepta la conexión. La recepción para cualquier destinatario está permitida y no está limitada por la Tabla de Acceso de Destinatarios. Esto trata un correo electrónico como un correo saliente

Rechazo TCP: La conexión se rechaza en el nivel TCP.

Continúe: El mapeo en HAT es ignorado, y el procesamiento de HAT continúa. Si la conexión entrante coincide con una entrada posterior que no es CONTINUE, se utiliza esa entrada en su lugar. La regla CONTINUE se utiliza para facilitar la edición de HAT en la GUI.

Componentes de una política de flujo de correo

Max. Mensajes por conexión: El número máximo de mensajes que se pueden enviar a través de este receptor por conexión desde un host remoto. Cada ICID representa una conexión

Max. Destinatarios por mensaje: El número máximo de destinatarios por mensaje que serán aceptados desde este host que se procesan usando esta política de flujo de correo

Max. Tamaño del mensaje: El tamaño máximo de un mensaje que aceptará este receptor etiquetado a la política de flujo de correo. El tamaño máximo más pequeño posible del mensaje es de 1 kilobyte.

Max. Conexiones Concurrentes desde una IP Única: El número máximo de conexiones simultáneas permitidas para conectarse a este receptor desde una sola dirección IP.

Código de banner SMTP personalizado: El código SMTP devuelto cuando se establece una conexión con este receptor.

Texto del banner SMTP personalizado: El texto del banner SMTP devuelto cuando se establece una conexión con este listener. Puede utilizar algunas variables en este campo.

Anular nombre de host de banner SMTP: de forma predeterminada, el dispositivo incluirá el nombre de host asociado a la interfaz del receptor cuando muestre el banner SMTP a hosts remotos (por ejemplo, 220-hostname ESMTP). Puede optar por anular este banner introduciendo aquí un nombre de host diferente. Además, puede dejar el campo hostname en blanco para elegir *no* mostrar un nombre de host en el banner.

Límites de flujo de correo

Max. Destinatarios por hora: El número máximo de destinatarios por hora que este receptor recibirá de un host remoto. El número de destinatarios por dirección IP del remitente se realiza un seguimiento global. Sin embargo, cada receptor realiza un seguimiento de su propio umbral de límite de velocidad, ya que todos los receptores se validan en un único contador, es más probable que se supere el límite de velocidad si la misma dirección IP (remitente) se conecta a varios receptores. Puede utilizar algunas variables en este campo.

Max. Código de Destinatarios por Hora: El código SMTP devuelto cuando un host supera el número máximo de destinatarios por hora definido para este receptor.

Max. Texto de Destinatarios por Hora: El texto del banner SMTP devuelto cuando un host excede el número máximo de destinatarios por hora definido para este listener.

Límite de velocidad para remitentes de sobres

Max. Destinatarios por intervalo de tiempo: El número máximo de destinatarios durante un período de tiempo especificado que este receptor recibirá de un remitente de sobre único, en función de la dirección de correo electrónico de origen. El número de destinatarios se realiza un seguimiento global. Cada receptor realiza un seguimiento de su propio umbral de límite de velocidad; sin embargo, dado que todos los receptores se validan en un único contador, es más probable que se exceda el límite de velocidad si varios receptores reciben mensajes de la misma dirección de correo electrónico de.

Código de error de límite de velocidad del remitente: El código SMTP devuelto cuando un sobre

supera el número máximo de destinatarios para el intervalo de tiempo definido para este receptor.

Texto de Error de Límite de Velocidad de Remitente: El texto del banner SMTP devuelto cuando un remitente del sobre excede el número máximo de destinatarios para el intervalo de tiempo definido para este receptor.

Exceptions: Si desea que ciertos remitentes de sobre estén exentos del límite de velocidad definido, seleccione una lista de direcciones que contenga los remitentes de sobre.

La lista de direcciones se define en Políticas de correo à Lista de direcciones (se pueden utilizar direcciones de correo electrónico completas, dominios y direcciones IP para las exenciones)

Utilizar SenderBase para Control de Flujo: Habilite "búsquedas" en el servicio de reputación de SenderBase para este receptor.

Agrupar por similitud de direcciones IP: Se utiliza para realizar un seguimiento y limitar la velocidad del correo entrante por dirección IP mientras se administran las entradas de la tabla de acceso de host (HAT) de un receptor en grandes bloques CIDR. Usted define un rango de bits significativos (de 0 a 32) por el cual agrupar direcciones IP similares con fines de limitación de velocidad, mientras mantiene un contador individual para cada dirección IP dentro de ese rango.

NOTE: Requiere que se deshabilite "Use SenderBase".

Prevención de ataques de recolección de directorios (DHAP)

Max. Destinatarios Por Hora No Válidos: El número máximo de destinatarios no válidos por hora que este receptor recibirá de un host remoto. Este umbral representa el número total de rechazos de RAT y de rechazos de servidor de llamadas SMTP combinados con el número total de mensajes a destinatarios LDAP no válidos descartados en la conversación SMTP o rebotados en la cola de trabajo (como se configuró en la configuración de aceptación LDAP en el receptor asociado).

Eliminar conexión si se alcanza el umbral DHAP dentro de una conversación SMTP:

El dispositivo descartará una conexión a un host si se alcanza el umbral de destinatarios no válidos.

Max. Código de Destinatarios por Hora No Válido: Especifique el código que se utilizará al descartar conexiones. El código predeterminado es 550.

Max. Texto de destinatarios por hora no válido: Especifique el texto que se utilizará para las conexiones caídas. El texto predeterminado es "Demasiados destinatarios no válidos.

Funciones de seguridad

Spam / AMP / Virus / Verificación de reputación de dominio de remitente / Filtros de brote / Protección avanzada de phishing / Graymail / Contenido y filtros de mensajes : Los motores de seguridad/escaneo y el escaneo relacionado con los filtros se pueden activar o desactivar desde aquí

Cifrado y autenticación: Podemos modificar la configuración como Off (Desactivado), Prefer

(Preferir) o Require Transport Layer Security (TLS) en conversaciones SMTP para este receptor.

La opción Verificar certificado de cliente indica al dispositivo de seguridad de correo electrónico que establezca una conexión TLS con la aplicación de correo del usuario si el certificado de cliente es válido.

Para el TLS preferido, el dispositivo todavía permite una conexión que no sea TLS si el usuario no tiene un certificado, pero rechaza una conexión si el usuario tiene un certificado no válido.

Para la configuración TLS requerida, seleccionar esta opción requiere que el usuario tenga un certificado válido para que el dispositivo permita la conexión.

Autenticación SMTP: Permite, no permite o requiere autenticación SMTP de hosts remotos que se conectan al receptor

Si TLS y autenticación SMTP están habilitados: Requerir TLS para ofrecer autenticación SMTP

Firma de clave de dominio/DKIM: Habilitar claves de dominio o firmas DKIM en este receptor

Verificación DKIM: Habilite la verificación DKIM.

Verificación/descifrado S/MIME: Habilite el descifrado S/MIME o la verificación.

Firma después del procesamiento: Elija si desea conservar o quitar la firma digital de los mensajes después de la verificación S/MIME.

Recolección de clave pública S/MIME: Habilite la obtención de claves públicas S/MIME.

Recolectar certificados en caso de fallo de verificación: Elija si desea recopilar claves públicas si falla la verificación de los mensajes entrantes firmados.

Almacenar certificado actualizado: Elija si desea recopilar claves públicas actualizadas

Verificación SPF/SIDF: Habilite la firma SPF/SIDF en este receptor.

Nivel de conformidad: Establezca el nivel de conformidad SPF/SIDF. Puede elegir entre SPF, SIDF o SIDF Compatible

Reducir el resultado de la verificación PRA si se utilizó 'Resent-Sender:' o 'Resent-From:': Si elige un nivel de conformidad compatible con SIDF, configure si desea degradar el resultado de la verificación de identidad PRA a Ninguno si hay remitente de reenvío: o de reenvío: encabezados presentes en el mensaje

Prueba HELO: Configure si desea realizar una prueba con la identidad HELO (utilice esta opción para los niveles de conformidad compatibles con SPF y SIDF)

Verificación de DMARC: Habilitar la verificación de DMARC en este receptor

Usar perfil de verificación de DMARC: Seleccione el perfil de verificación de DMARC que desea utilizar en este receptor. Lo mismo se crea a partir de Políticas de correo —> DMARC —> Agregar perfil

Informes de comentarios de DMARC: Habilite el envío de informes de comentarios agregados de DMARC.

Verificación de rebote

Considere los rebotes no etiquetados como válidos: Sólo se aplica si el etiquetado de verificación de rebote está habilitado. De forma predeterminada, el dispositivo considera que los rebotes sin etiqueta no son válidos y rechaza el rebote o agrega un encabezado personalizado, según la configuración de verificación de rebote. Si decide considerar los rebotes sin etiqueta como válidos, el dispositivo acepta el mensaje de rebote.

Verificación de remitente

Verificación de DNS del remitente del sobre:

Los remitentes pueden no ser verificados por diferentes razones. Los remitentes no verificados se clasifican en las siguientes categorías:

- El registro PTR del host de conexión no existe en el DNS.
- La conexión de la búsqueda del registro PTR del host falla debido a una falla temporal de DNS.
- La búsqueda de DNS inverso (PTR) del host de conexión no coincide con la búsqueda de DNS de reenvío (A).

Podemos activar o desactivar la función de verificación de remitente.

Usar tabla de excepción de verificación de remitente: Podemos utilizar la tabla de excepciones de dominio de verificación del remitente para permitir exenciones. Solo podemos tener una tabla de excepciones, pero se puede habilitar por política de flujo de correo.

La tabla Excepción se puede crear a partir de Políticas de correo —> Tabla de excepciones de verificación de remitente —> Agregar excepción de verificación de remitente

Controles de destino

Esta es una función que controla las entregas por correo electrónico. Todos los correos electrónicos que terminan de procesarse a través de los ESA y que están a punto de salir de los ESA para futuras entregas pueden ser controlados por la función Controles de destino.

El perfil **Default** Destination Controls se aplica a todas las entregas. Por si acaso, se necesitan controles de entrega específicos del dominio, por lo que tenemos que crear un perfil de controles de destino personalizado.

Componentes de un perfil de controles de destino

Limits

Conexiones simultáneas: Número de conexiones simultáneas (DCID) a hosts remotos que el dispositivo intentará abrir para completar la entrega.

Máximo de mensajes por conexión: Número de mensajes que el ESA enviará a un dominio de destino a través de una conexión (DCID) antes de que el dispositivo inicie una nueva conexión.

Destinatarios: Número de destinatarios que el dispositivo enviará a un host remoto determinado en un período de tiempo determinado.

Aplicar límites: Estos aspectos ayudan a decidir cómo aplicar los límites que hemos especificado por destino y por nombre de host MGA.

Soporte de TLS

Esto ayuda a decidir si las conexiones TLS a los hosts remotos se establecerán en Ninguno / Preferido / Obligatorio

Soporte de DANE: Si configura DANE como 'Oportunista' y el host remoto no soporta DANE, se prefiere TLS oportunista para cifrar conversaciones SMTP.

Si configura DANE como 'Obligatorio' y el host remoto no soporta DANE, no se establece ninguna conexión con el host de destino.

Si configura DANE como 'Obligatorio' o 'Oportunista' y el host remoto soporta DANE, se prefiere para cifrar conversaciones SMTP.

NOTE: No se aplicará DANE para los dominios que tienen configuradas las rutas SMTP.

Verificación de rebote

Esto ayuda a decidir si realizar o no el etiquetado de la dirección del remitente del sobre (prvs-xxxxxx-xxxx) a través de la verificación de rebote.

La verificación de rebote se puede configurar desde Políticas de correo —> Verificación de rebote —> Agregar nueva clave

Perfil de rebote

El dispositivo puede utilizar el perfil de rebote para un host remoto determinado. Decide cuánto tiempo se retendrá un correo electrónico en la cola de entrega del ESA si hay problemas de entrega, antes de rebotar un correo electrónico

El perfil de rebote se establece a través de la red —> Perfiles de rebote

Configuración global

Certificado: Este es el aspecto en el que definimos los certificados que se utilizarán al establecer conexiones SSL/TLS al iniciar envíos de correo electrónico al salto siguiente. Siempre se recomienda utilizar un certificado firmado por la Autoridad de Certificación (CA) en este aspecto.

Enviar una alerta cuando falla una conexión TLS requerida: Podemos especificar si el dispositivo envía una alerta si la negociación TLS falla al enviar mensajes a un dominio que requiere una

conexión TLS. El mensaje de alerta contiene el nombre del dominio de destino para la negociación TLS fallida. El dispositivo envía el mensaje de alerta a todos los destinatarios configurados para recibir alertas de nivel de gravedad **de advertencia para los** tipos de **alerta del sistema**.

Podemos administrar destinatarios de alertas a través de Administración del sistema —> Alertas