Entender os parâmetros relacionados às políticas de fluxo de e-mail e aos controles de destino

Contents

Introduction

Este documento descreve alguns aspectos de configuração do Email Security Appliance (ESA) sobre como limitar/limitar a taxa de envio e envio. Os recursos que serão descritos no artigo são Políticas de fluxo de e-mail e Controles de destino.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica das políticas de fluxo de e-mail e dos controles de destino
- Familiaridade com o uso desses recursos na configuração do ESA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Vantagens das políticas de fluxo de e-mail e controles de destino

Há uma função muito importante que esses dois recursos têm, que é a limitação de taxa/limitação. Esse aspecto ajuda o administrador a ter controle sobre qual tráfego deve ser livre e qual deve ser permitido com restrições.

Políticas de fluxo de e-mail

Essas são as políticas que se aplicam aos grupos de remetentes do ESA, com base nas quais a modulação de tráfego de e-mail é feita.

As Políticas de fluxo de e-mail sempre se aplicam ao tráfego que é de entrada para o ESA, independentemente do e-mail ser de entrada ou de saída.

As Políticas de fluxo de e-mail funcionam no backend em relação ao comportamento de conexão selecionado para essa política. O comportamento de conexão diferente disponível nos ESAs é:

1. Aceitar
2. Reject
3. Retransmissão
4. Recusar TCP
5. Continuar

Aceitar: A conexão é aceita, e a aceitação do e-mail é restringida ainda mais pelas configurações do ouvinte, incluindo a Tabela de Acesso do Destinatário (para ouvintes públicos). Este comportamento de conexão trata um e-mail como entrada

Reject: O cliente que está tentando se conectar obtém um código de status SMTP 4XX ou 5XX. Nenhum e-mail é aceito. Isso é usado principalmente para remetentes da lista negra

Retransmissão: A conexão é aceita. O recebimento de qualquer destinatário é permitido e não é restringido pela tabela de acesso de destinatário. Isso trata um e-mail como uma mensagem de saída

Recusar TCP: A conexão é recusada no nível TCP.

Continuar: O mapeamento no HAT é ignorado e o processamento do HAT continua. Se a conexão de entrada corresponder a uma entrada posterior que não é CONTINUAR, essa entrada será usada. A regra CONTINUAR é usada para facilitar a edição do HAT na GUI.

Componentes de uma política de fluxo de e-mail

Max. Mensagens por conexão: O número máximo de mensagens que podem ser enviadas através deste ouvinte por conexão de um host remoto. Cada ICID representa uma conexão

Max. Destinatários por mensagem: O número máximo de destinatários por mensagem que serão aceitos deste host que é processado usando esta política de fluxo de e-mail

Max. Tamanho da mensagem: O tamanho máximo de uma mensagem que será aceita por esse ouvinte marcado na Política de fluxo de e-mail. O menor tamanho máximo possível de mensagem é 1 kilobyte.

Max. Conexões simultâneas de um único IP: O número máximo de conexões simultâneas permitidas para se conectar a esse ouvinte a partir de um único endereço IP.

Código de banner SMTP personalizado: O código SMTP retornado quando uma conexão é estabelecida com esse ouvinte.

Texto do banner SMTP personalizado: O texto do banner SMTP retornado quando uma conexão é estabelecida com esse ouvinte. Você pode usar algumas variáveis neste campo.

Substituir nome de host de banner SMTP: por padrão, o dispositivo incluirá o nome de host associado à interface do ouvinte ao exibir o banner SMTP para hosts remotos (por exemplo, 220-hostname ESMTP). Você pode optar por substituir esse banner inserindo um nome de host diferente aqui. Além disso, você pode deixar o campo hostname em branco para escolher *não* exibir um hostname no banner.

Limites de fluxo de e-mail

Max. Destinatários por hora: O número máximo de destinatários por hora que este ouvinte receberá de um host remoto. O número de destinatários por endereço IP do remetente é rastreado globalmente. Cada ouvinte rastreia seu próprio limite de taxa, entretanto, como todos os ouvintes validam em um único contador, é mais provável que o limite de taxa seja excedido se o mesmo endereço IP (remetente) estiver se conectando a vários ouvintes. Você pode usar algumas variáveis neste campo.

Max. Destinatários por código de hora: O código SMTP retornado quando um host excede o número máximo de destinatários por hora definido para esse ouvinte.

Max. Destinatários por texto de hora: O texto do banner SMTP retornado quando um host excede o número máximo de destinatários por hora definido para esse ouvinte.

Limite de taxa para remetentes de envelope

Max. Destinatários por intervalo de tempo: O número máximo de destinatários durante um período de tempo especificado que esse ouvinte receberá de um remetente de envelope exclusivo, com base no endereço de email de. O número de destinatários é rastreado globalmente. Cada ouvinte rastreia seu próprio limite de taxa; no entanto, como todos os ouvintes validam em um único contador, é mais provável que o limite de taxa seja excedido se as mensagens do mesmo endereço de email de forem recebidas por vários ouvintes.

Código de erro de limite de taxa de remetente: O código SMTP retornado quando um envelope excede o número máximo de destinatários para o intervalo de tempo definido para esse ouvinte.

Texto de erro de limite de taxa de remetente: O texto do banner SMTP retornado quando um remetente de envelope excede o número máximo de destinatários para o intervalo de tempo

definido para esse ouvinte.

Exceções: Se desejar que determinados remetentes de envelope fiquem isentos do limite de taxa definido, selecione uma lista de endereços que contenha os remetentes de envelope.

A lista de endereços é definida em Políticas de e-mail à Lista de endereços (Endereços de e-mail completos, Domínios, Endereços IP podem ser usados para isenções)

Usar SenderBase para Controle de Fluxo: Ative "pesquisas" no Serviço de reputação SenderBase para este ouvinte.

Agrupar por semelhança de endereços IP: Usado para rastrear e limitar a taxa de mensagens recebidas em uma base de endereço IP ao gerenciar entradas na HAT (Host Access Table, tabela de acesso de host) de um ouvinte em grandes blocos CIDR. Você define um intervalo de bits significativos (de 0 a 32) pelos quais agrupar endereços IP semelhantes para fins de limitação de taxa, enquanto mantém um contador individual para cada endereço IP dentro desse intervalo.

NOTE: Requer que "Usar SenderBase" seja desabilitado.

Prevenção de ataque de coleta de diretório (DHAP)

Max. Destinatários inválidos por hora: O número máximo de destinatários inválidos por hora que este ouvinte receberá de um host remoto. Esse limite representa o número total de rejeições de RAT e rejeições de servidor de chamadas antecipadas de SMTP combinadas com o número total de mensagens para destinatários LDAP inválidos descartados na conversação SMTP ou devolvidos na fila de trabalho (conforme configurado nas configurações de aceitação de LDAP no ouvinte associado).

Descartar conexão se o limite de DHAP for alcançado em uma conversação SMTP:

O aplicativo descartará uma conexão com um host se o limite de destinatários inválidos for atingido.

Max. Destinatários inválidos por código de hora: Especifique o código a ser usado ao descartar conexões. O código padrão é 550.

Max. Destinatários inválidos por texto de hora: Especifique o texto a ser usado para conexões descartadas. O texto padrão é "Muitos destinatários inválidos.

Recursos de segurança

Spam / AMP / Virus / Sender Domain Reputation Verification / Outbreak Filters / Advanced Phishing Protection / Graymail / Content & Message Filters : Os mecanismos de segurança/verificação e a verificação relacionada aos filtros podem ser ativados ou desativados aqui

Criptografia e autenticação: Podemos modificar as configurações como Desativado, Preferencial ou Exigir TLS (Transport Layer Security) em conversas SMTP para esse ouvinte.

A opção Verificar certificado do cliente direciona o Email Security Appliance para estabelecer uma conexão TLS com o aplicativo de e-mail do usuário, se o certificado do cliente for válido.

Para TLS preferencial, o aplicativo ainda permite uma conexão não TLS se o usuário não tiver um certificado, mas rejeita uma conexão se o usuário tiver um certificado inválido.

Para a configuração TLS necessário, selecionar essa opção exige que o usuário tenha um certificado válido para que o dispositivo permita a conexão.

Autenticação SMTP: Permite, não permite ou exige autenticação SMTP de hosts remotos conectando-se ao ouvinte

Se a autenticação TLS e SMTP estiver habilitada: Requer TLS para oferecer autenticação SMTP

Assinatura DKIM/Chave de domínio: Habilitar chaves de domínio ou assinatura DKIM neste ouvinte

Verificação DKIM: Habilitar verificação DKIM.

Descriptografia/verificação S/MIME: Habilite a descriptografia ou verificação de S/MIME.

Assinatura após processamento: Escolha se deseja reter ou remover a assinatura digital das mensagens após a verificação S/MIME.

Coleta de chaves públicas S/MIME: Habilitar coleta de chave pública S/MIME.

Coletar certificados em falha de verificação: Escolha se deseja coletar chaves públicas se a verificação das mensagens assinadas recebidas falhar.

Armazenar certificado atualizado: Escolha se deseja coletar chaves públicas atualizadas

Verificação SPF/SIDF: Ative a assinatura SPF/SIDF neste ouvinte.

Nível de conformidade: Defina o nível de conformidade SPF/SIDF. Você pode escolher entre SPF, SIDF ou compatível com SIDF

Desatualizar o resultado da verificação PRA se 'Resent-Sender:' ou 'Resent-From:' forem usados: Se você escolher um nível de conformidade compatível com o SIDF, configure se deseja fazer o downgrade do resultado da verificação de identidade do PRA para Nenhum se houver remetente: ou Reenviado de: cabeçalhos presentes na mensagem

Teste HELO: Configurar se você deseja executar um teste contra a identidade HELO (Use isso para níveis de conformidade compatíveis com SPF e SIDF)

Verificação DMARC: Ativar verificação de DMARC neste ouvinte

Usar perfil de verificação DMARC: Selecione o perfil de verificação DMARC que deseja usar neste ouvinte. O mesmo é criado a partir das Políticas de e-mail —> DMARC —> Add Profile

Relatórios de comentários do DMARC: Habilitar o envio de relatórios de comentários agregados de DMARC.

Verificação de devolução

Considere os devoluções não marcados válidos: Aplica-se somente se a marcação de verificação de devolução estiver ativada. Por padrão, o dispositivo considera os devoluções não marcados inválidos e rejeita a devolução ou adiciona um cabeçalho personalizado, dependendo das configurações de Verificação de devolução. Se você optar por considerar válidos os devoluções não marcados, o aplicativo aceitará a mensagem de devolução.

Verificação do remetente

Verificação DNS do remetente do envelope:

Os remetentes podem não ser verificados por motivos diferentes. Os remetentes não verificados são classificados nas seguintes categorias:

- O registro PTR do host de conexão não existe no DNS.
- Falha na pesquisa de registro PTR do host de conexão devido a uma falha temporária de DNS.
- A pesquisa de DNS reverso (PTR) do host de conexão não corresponde à pesquisa de DNS avançado (A).

Podemos ativar ou desativar o recurso de verificação de remetente.

Usar tabela de exceção de verificação de remetente: Podemos usar a tabela de exceção de domínio de verificação de remetente para permitir isenções. Podemos ter apenas uma tabela de exceção, mas pode ser habilitada por política de fluxo de e-mail.

A tabela de exceções pode ser criada a partir de Políticas de e-mail —> Tabela de exceções de verificação de remetente —> Adicionar exceção de verificação de remetente

Controles de destino

Este é um recurso que controla as entregas de e-mail. Todos os e-mails que terminam o processamento via ESAs e estão prestes a sair dos ESAs para outras entregas podem ser controlados pelo recurso Controles de destino.

O perfil de controles de destino **padrão** se aplica a todas as entregas. Caso haja necessidade de controles de entrega específicos do domínio, temos que criar um perfil de controles de destino personalizado.

Componentes de um perfil de controles de destino

Limites

Conexões simultâneas: Número de conexões simultâneas (DCIDs) para hosts remotos que o dispositivo tentará abrir para concluir a entrega.

Máximo de mensagens por conexão: Número de mensagens que o ESA enviará a um domínio de destino por uma conexão (DCID) antes que o dispositivo inicie uma nova conexão.

Destinatários: Número de destinatários que o dispositivo enviará a um determinado host remoto em um determinado período de tempo.

Aplicar limites: Esses aspectos ajudam a decidir como aplicar os limites especificados por destino e por nome de host MGA.

Suporte TLS

Isso ajuda a decidir se as conexões TLS aos hosts remotos serão definidas como Nenhum / Preferencial / Obrigatório

Suporte DANE: Se você configurar o DANE como 'Oportunista' e o host remoto não suportar DANE, o TLS oportunista é preferido para criptografar conversações SMTP.

Se você configurar o DANE como "obrigatório" e o host remoto não suportar o DANE, nenhuma conexão será estabelecida para o host de destino.

Se você configurar o DANE como "obrigatório" ou "oportunista" e o host remoto suportar o DANE, ele será preferido para criptografar conversações SMTP.

NOTE: O DANE não será imposto para domínios com rotas SMTP configuradas.

Verificação de devolução

Isso ajuda a decidir se deve ou não executar a marcação de endereço do remetente de envelope (prvs-xxxxx-xxxx) através da verificação de devolução.

A verificação de devolução pode ser configurada em Políticas de e-mail —> Verificação de devolução —> Adicionar nova chave

Perfil de devolução

O perfil de devolução pode ser usado pelo dispositivo para um determinado host remoto. Ele decide por quanto tempo um e-mail será mantido na Fila de entrega do ESA se houver problemas de entrega, antes do lançamento de um e-mail em modo de contorno

O perfil de devolução é definido através da Rede —> Perfis de devolução

Configurações globais

Certificado: Esse é o aspecto em que definimos os certificados a serem usados ao estabelecer conexões SSL/TLS ao iniciar entregas de e-mail para o próximo salto. É sempre recomendado utilizar um certificado assinado pela Autoridade de Certificação (AC) neste aspecto.

Enviar um alerta quando uma conexão TLS necessária falhar: Podemos especificar se o dispositivo envia um alerta se a negociação TLS falhar ao entregar mensagens para um domínio que requer uma conexão TLS. A mensagem de alerta contém o nome do domínio de destino para a negociação TLS com falha. O aplicativo envia a mensagem de alerta a todos os destinatários definidos para receber alertas de nível de gravidade de **aviso** para tipos de **alerta do sistema**.

Podemos gerenciar os destinatários de alertas através da Administração do sistema —> Alertas