Guia do melhor prática para controles da verificação e do destino do salto

Índice

Introdução

A entrega descontrolada do email do volume alto pode oprimir domínios destinatários. AsyncOS dá-lhe o controle total da entrega de mensagem definindo o número de conexões que seu serviço de segurança do email abrirá ou o número de mensagens que enviarão a cada domínio do destino.

Neste documento, nós cobriremos:

1. Estabelecendo a verificação do salto para proteger sua organização dos ataques do salto
2. Usando a tabela de controle do destino para praticar boas políticas vizinhas
3. O S TP de distribuição DNS-baseou a autenticação Named Entidade (DINAMARQUÊS) para fornecer fixa a entrega das mensagens

Verificação do salto

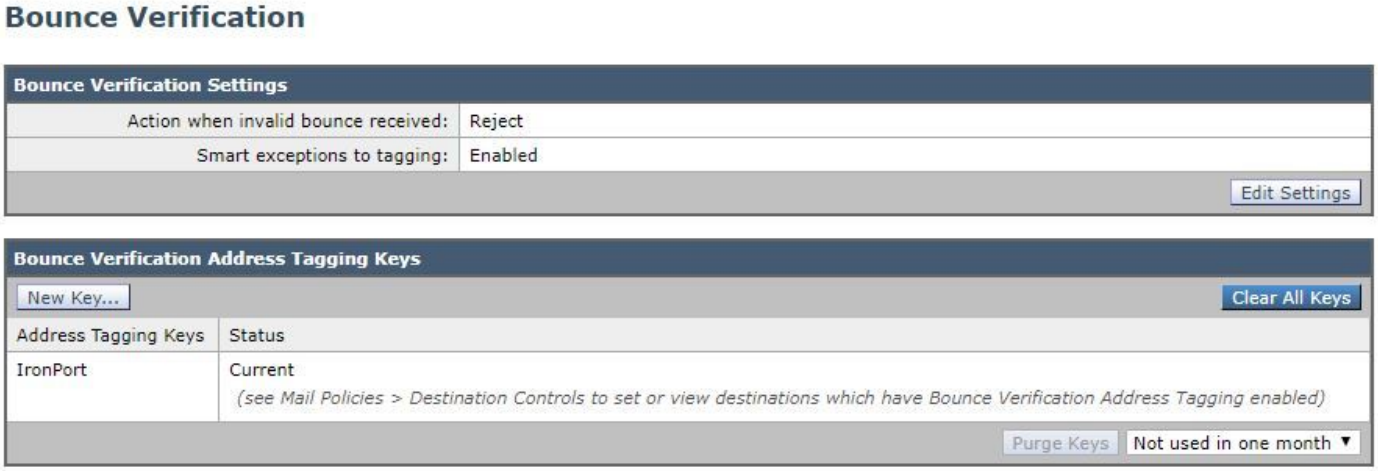
Permitir a verificação do salto é uma maneira muito boa de combater ataques do backscatter/salto. O conceito atrás da verificação do salto é simples. Primeiramente, marca acima das mensagens que saem de seu ESA. Procure essa margem de benefício em todas as mensagens de salto, se a margem de benefício esta presente, ele significa que este é um salto de uma mensagem que origine em seu ambiente. Se a margem de benefício falta, o salto é fraudulento e pode ser rejeitado ou deixado cair.

Por exemplo, CORREIO DE: joe@example.com transforma-se CORREIO DE: prvs=joe=123ABCDEFG@example.com. … A corda 123 no exemplo é a etiqueta da verificação do salto que está adicionada ao remetente do envelope enquanto é enviado por seu dispositivo ESA. Se a mensagem salta, o endereço destinatário do envelope na mensagem saltada incluirá a etiqueta da verificação do salto, que deixa o ESA saber que é uma mensagem saltada legítima.

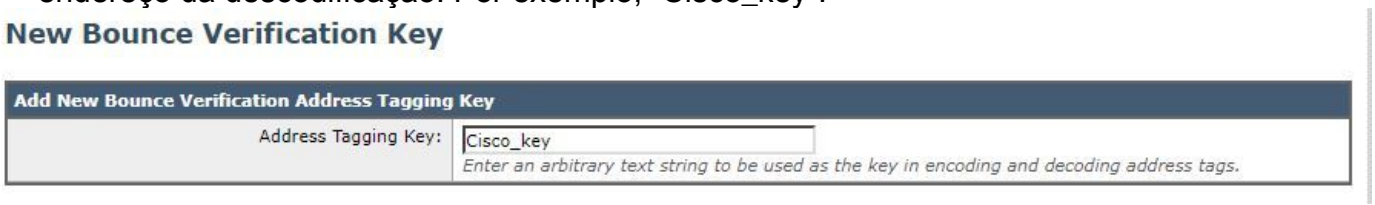
Você pode permitir ou desabilitar a colocação de etiquetas da verificação do salto sistema-larga como um padrão. Você pode igualmente permitir ou desabilitar a verificação do salto que etiqueta para domínios específicos. Na maioria de disposições, é permitida à revelia para todos os domínios.

Configuração ESA

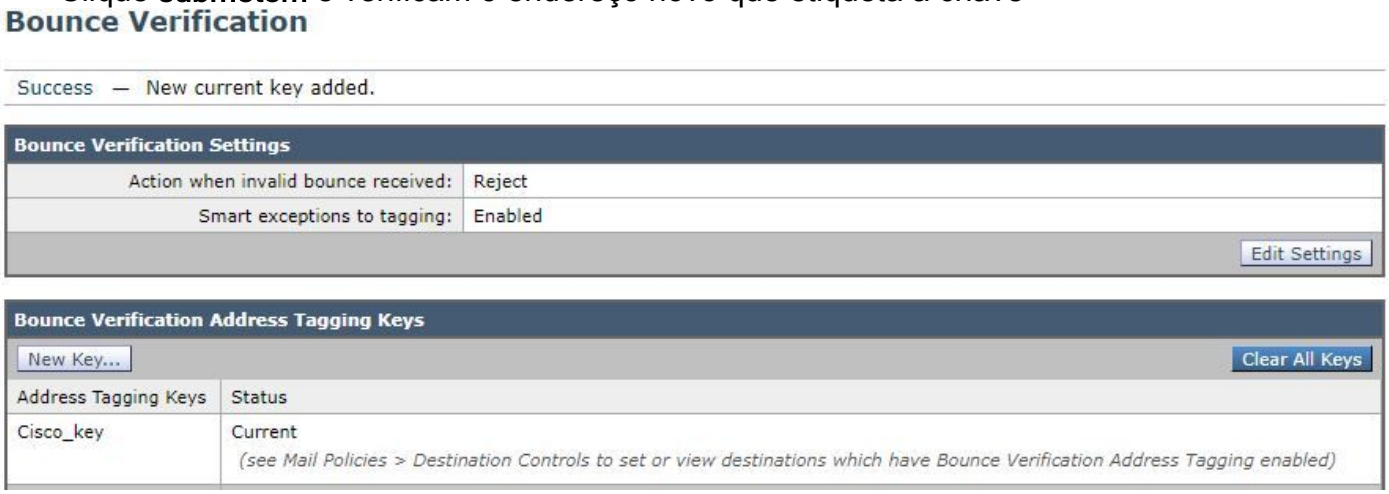
- Navegue **para enviar políticas > verificação do salto** e para clicar a **chave nova**



- Incorpore todo o texto arbitrário a ser usado como a chave à codificação e etiquetas do endereço da descodificação. Por exemplo, “Cisco_key”.

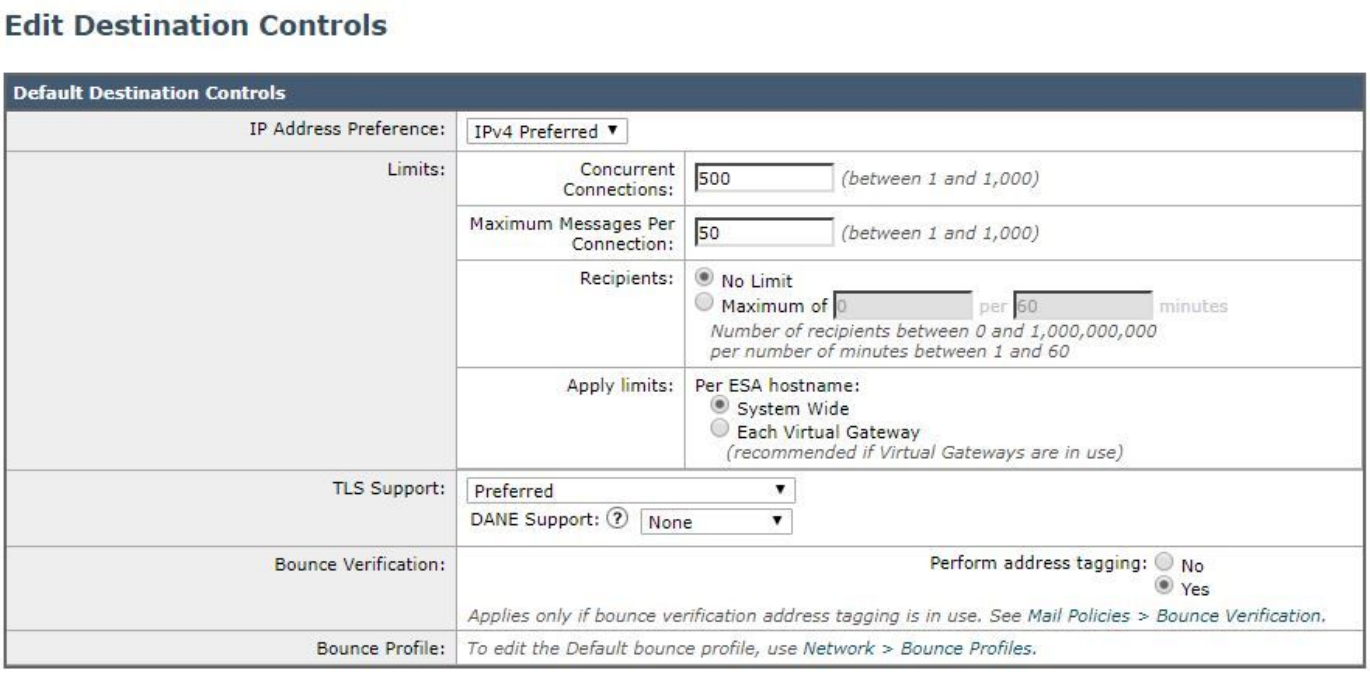


- Clique **submetem** e verificam o endereço novo que etiqueta a chave

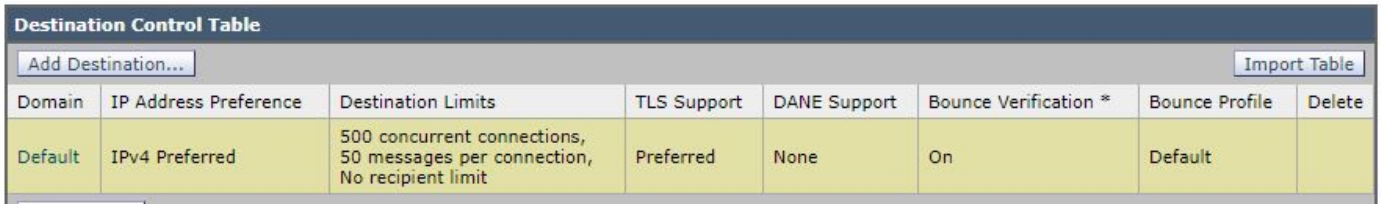


Agora, deixe-nos permitem a verificação do salto para nosso domínio do “padrão”:

- Navegue **para enviar políticas > controles do destino** e para clicar sobre o **padrão.**
- Configurar a **verificação do salto: Execute a colocação de etiquetas do endereço: Yes**



- Clique **submetem** e **comprometem mudanças.** Note que a verificação do salto é agora sobre para o domínio padrão.



Usando a tabela de controle do destino

A entrega descontrolada do email pode oprimir domínios destinatários. O ESA dá-lhe o controle total da entrega de mensagem definindo o número de conexões que seu dispositivo abrirá ou o número de mensagens seu dispositivo enviará a cada domínio do destino. A tabela de controles do destino fornece ajustes para taxas da conexão e da mensagem quando o ESA está entregando aos destinos remotos. Igualmente fornece ajustes tentando ou reforçando o uso do TLS a estes destinos. O ESA é configurado com uma configuração padrão para a tabela de controle do destino.

O que nós cobriremos neste documento é como nós podemos controlar e configurar o controle sobre os destinos onde o padrão não é um ajuste. Por exemplo, Google tem um grupo de recepção ordena que os usuários de Gmail devem seguir ou arriscam enviar suportam um código da resposta S TP 4XX e uma mensagem que diz o está enviando demasiado rapidamente, ou a caixa postal do receptor excedeu seu limite do armazenamento. Nós adicionaremos o domínio de Gmail à tabela de controle do destino que limita a quantidade de mensagem enviada a um receptor de Gmail abaixo.

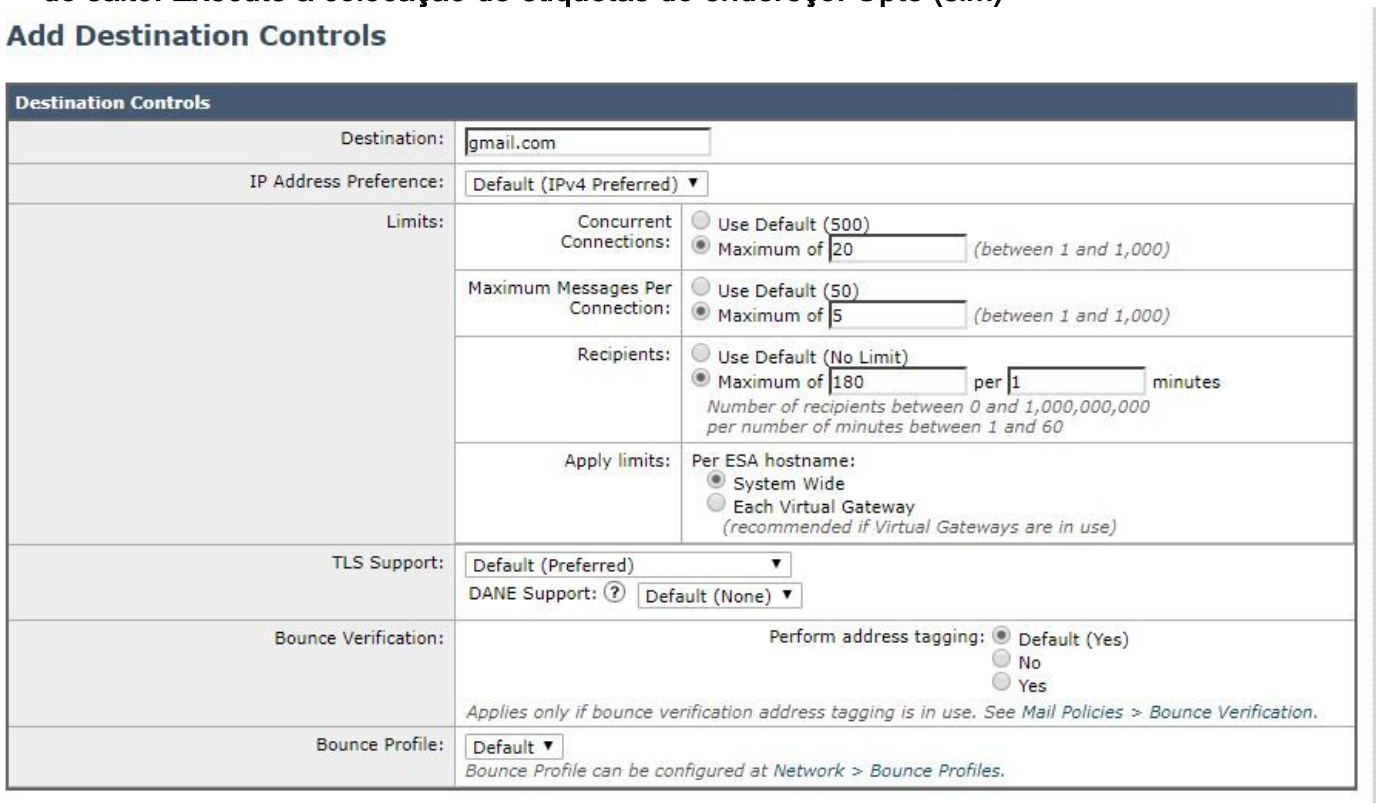
Adicionando um domínio novo à tabela de controle do destino

Como mencionado, Google tem limitações para os remetentes que enviam a Gmail. Receber limites pode ser verificada olhando o remetente - https://support.google.com/a/answer/1366776?hl=en aqui publicado limitações de Gmail

Deixe-nos estabelecer o domínio do destino para Gmail como exemplo das boas políticas

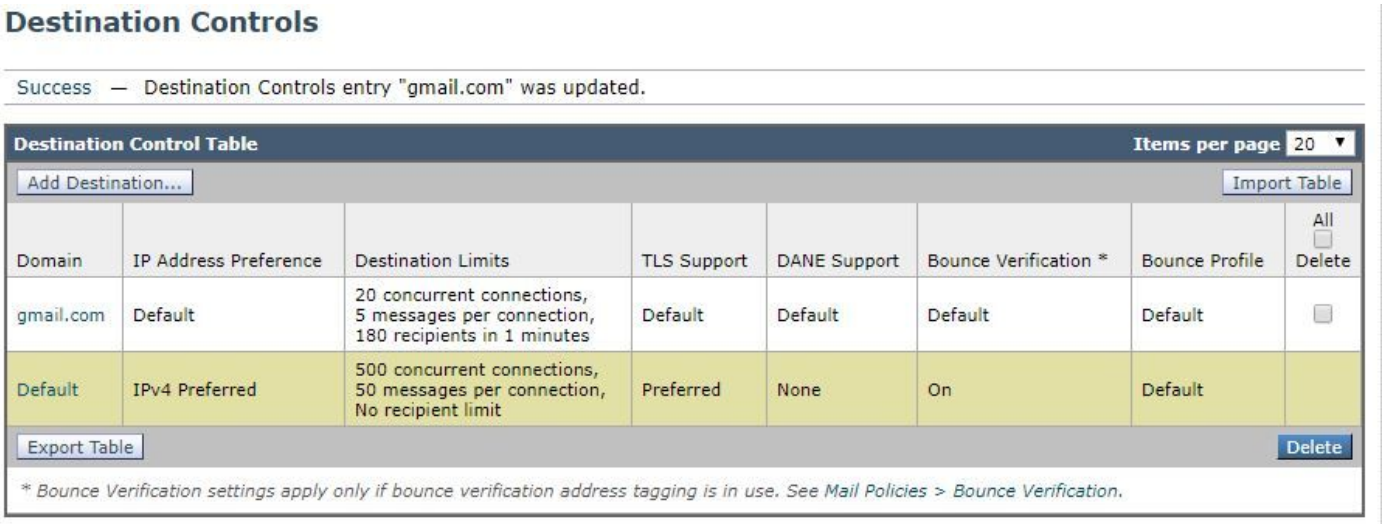
vizinhas.

- Navegue **para enviar políticas > controles do destino** e o clique **adiciona o destino** e cria um perfil novo usando os seguintes parâmetros: Destino: gmail.com**Preferência do endereço IP de Um ou Mais Servidores Cisco ICM NT: IPv4 preferidoConexões simultâneas: Máximo de 20Mensagens máximas pela conexão: 5Receptores: Máximo de 180 por 1 minutoVerificação do salto: Execute a colocação de etiquetas do endereço: Opte (sim)**



- O clique **submete** e **compromete mudanças.** Este é o que nossa tabela de controle do destino olha como após a adição do domínio.

Note o “destino limita” e do “a verificação salto” muda na imagem abaixo:



O S TP de distribuição DNS-baseou a autenticação Named Entidade (o DINAMARQUÊS)

A autenticação DNS-baseada S TP do protocolo Named Entidade (DINAMARQUÊS) valida seus Certificados X.509 com nomes de DNS usando uma extensão da Segurança do Domain Name System (DNSSEC) configurada em seu servidor DNS e em um registro de recurso DNS, igualmente conhecido como um registro TLSA.

O registro TLSA é adicionado no certificado que contém detalhes sobre o Certificate Authority (CA), o certificado da fim-entidade, ou a âncora da confiança usada para o nome de DNS descrito no RFC 6698. Os Ramais da Segurança do Domain Name System (DNSSEC) fornecem a Segurança adicionada no DNS endereçando vulnerabilidades na Segurança DNS. DNSSEC usando chaves criptográficas e assinaturas digital assegura-se de que os dados da consulta estejam corretos e conecta-se para legitimar server.

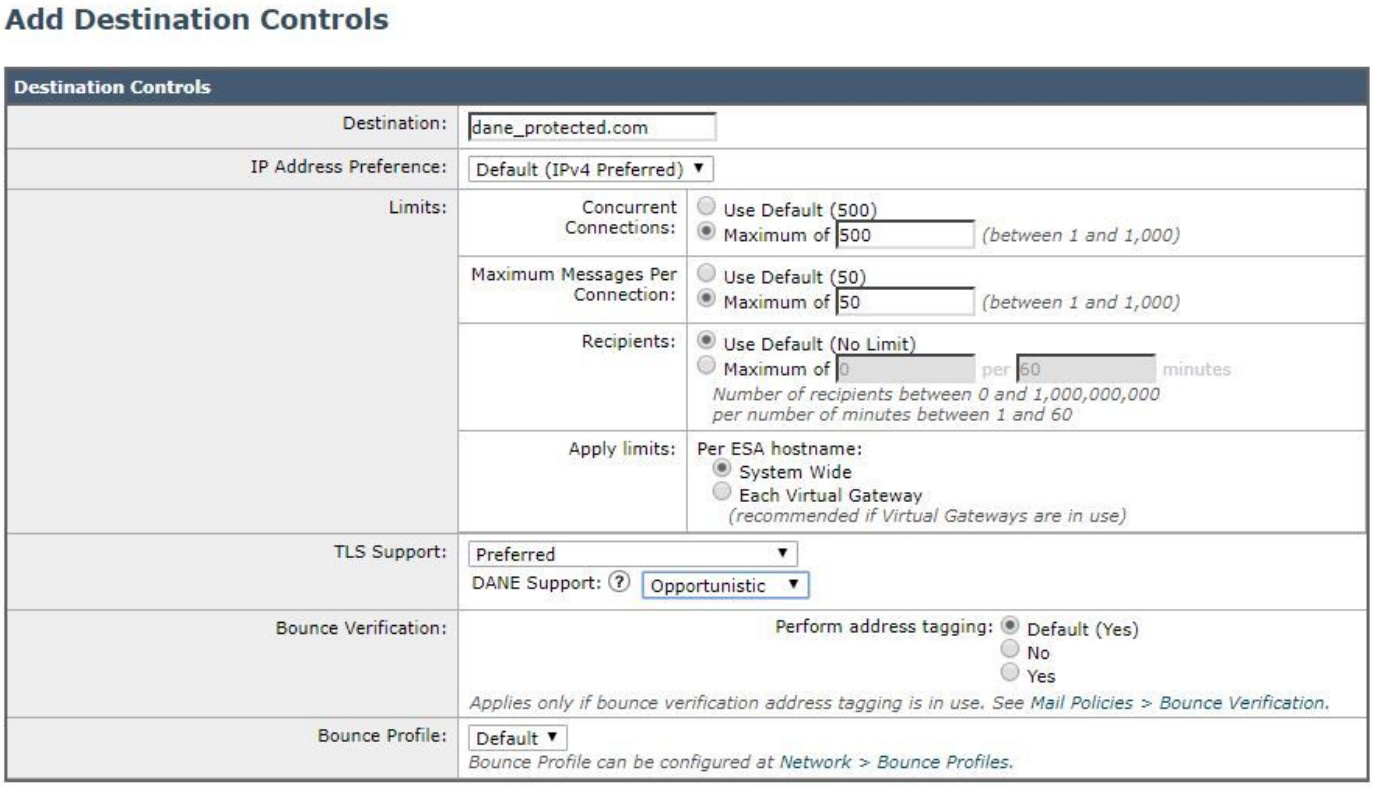
Os seguintes são os benefícios de usar o DINAMARQUÊS S TP para conexões TLS que parte:

- Fornece a entrega segura das mensagens pelo impedimento de ataques Homem-em--médios do downgrade (MITM), bisbilhotar e pelo esconderijo DNS ataques do envenenamento.
- Fornece a autenticidade de Certificados e de informação de DNS TLS, quando fixado por DNSSEC.

Configuração ESA

Antes que você comece estabelecer o DINAMARQUÊS no ESA, assegure-se de por favor que o remetente do envelope e o registro de recurso TLSA sejam DNSSEC verificados e que o domínio de recepção é DINAMARQUÊS protegido. Você pode fazer este no ESA que usa o comando CLI **daneverify**.

- Navegue **para enviar políticas > controles do destino** e o clique **adiciona o destino** e cria um perfil novo usando os seguintes parâmetros: **Destino:** dane_protected.com**Apoio TLS:** Preferido**Apoio do DINAMARQUÊS:** Oportunista



- Clique **submetem** e **comprometem mudanças.**