Guía de la mejor práctica para los controles de la verificación y del destino de la despedida

Contenido

Introducción

La salida en grandes cantidades incontrolada del correo electrónico puede abrumar los dominios receptores. AsyncOS le da el control total de la entrega de mensajes definiendo el número de conexiones que su servicio de seguridad del correo electrónico se abrirá o el número de mensajes que envíen a cada dominio del destino.

En este documento, cubriremos:

1. Configurar la verificación de la despedida para proteger su organización contra los ataques de la despedida
2. Usando la tabla de control de destino para practicar las buenas directivas vecinas
3. La autenticación basada en DNS S TP que despliega Named Entities (DANÉS) a proporcionar asegura la salida de los mensajes

Verificación de la despedida

Habilitar la verificación de la despedida es una manera muy buena de combatir los ataques del retrodifusor/de la despedida. El concepto detrás de la verificación de la despedida es simple. Primero, marca encima de los mensajes que salen de su ESA. Busque ese margen de beneficio en cualquier mensaje de despedida, si el margen de beneficio está presente, él significa que ésta es una despedida de un mensaje que originó en su entorno. Si el margen de beneficio falta, la despedida es fraudulenta y puede ser rechazada o ser caída.

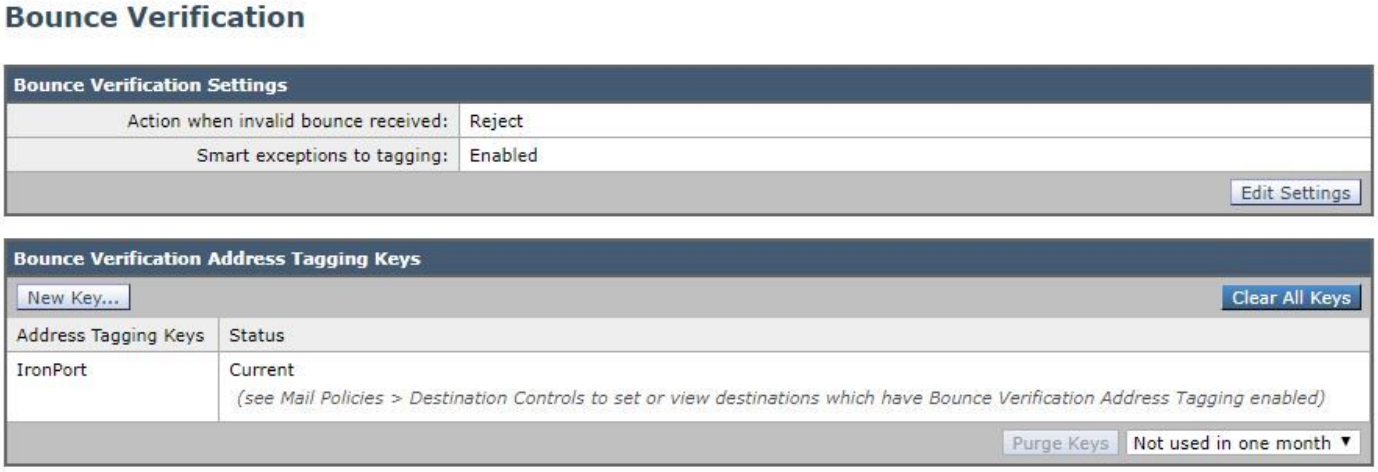
Por ejemplo, CORREO DE: joe@example.com se convierte en CORREO DE: prvs=joe=123ABCDEFG@example.com. … La cadena 123 en el ejemplo es la etiqueta de la verificación de la despedida que se agrega al remitente del sobre mientras que es enviado por su dispositivo ESA. Si el mensaje despide, el direccionamiento receptor del sobre en el mensaje despedido incluirá la etiqueta de la verificación de la despedida, que deja el ESA saber que es un mensaje despedido legítimo.

Usted puede habilitar o inhabilitar marcar con etiqueta de la verificación de la despedida sistema-ancho como valor por defecto. Usted puede también habilitar o inhabilitar la verificación de la

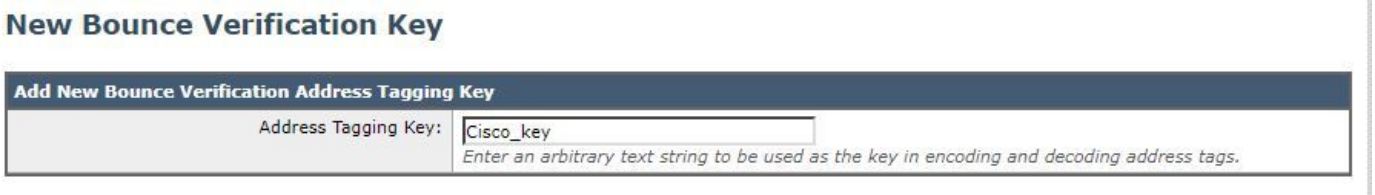
despedida que marca con etiqueta para los dominios específicos. En la mayoría de las implementaciones, se habilita por abandono para todos los dominios.

Configuración ESA

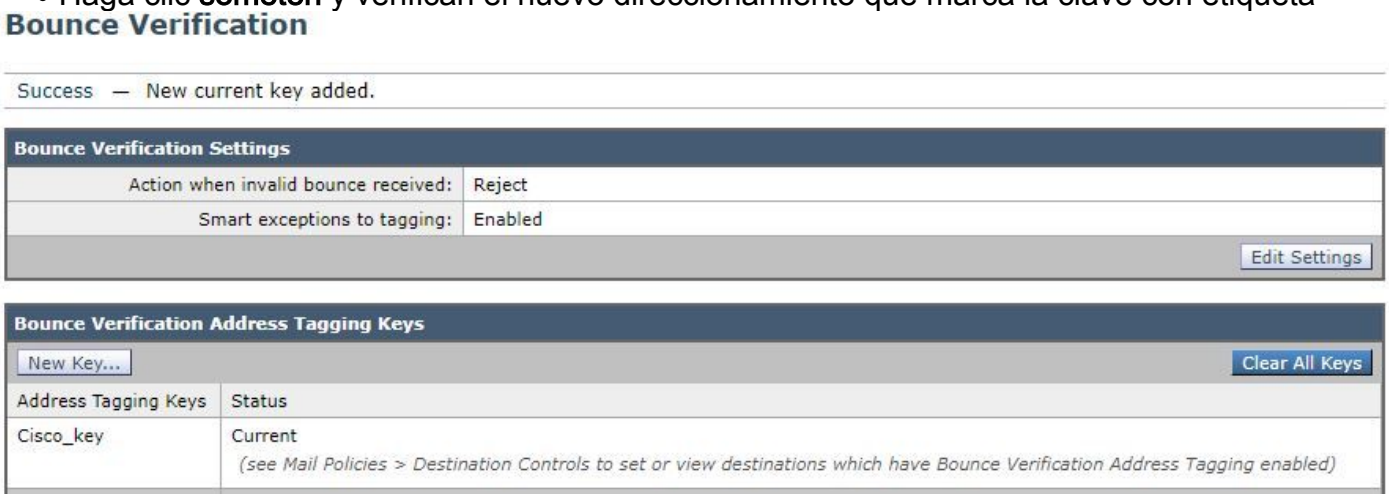
- Navegue **para enviar las directivas > la verificación de la despedida** y para hacer clic la **nueva clave**



- Ingrese cualquier texto arbitrario que se utilizará como la clave en la codificación y las etiquetas del direccionamiento el decodificar. Por ejemplo, “Cisco_key”.

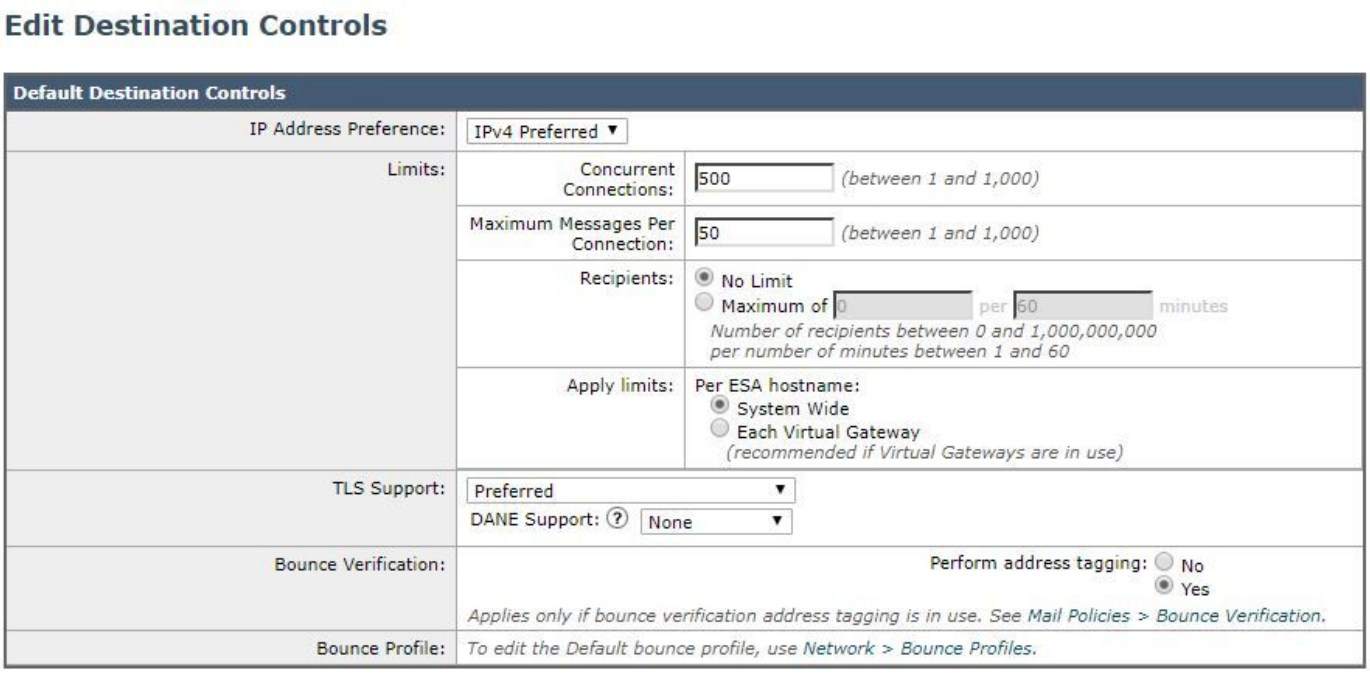


- Haga clic **someten** y verifican el nuevo direccionamiento que marca la clave con etiqueta

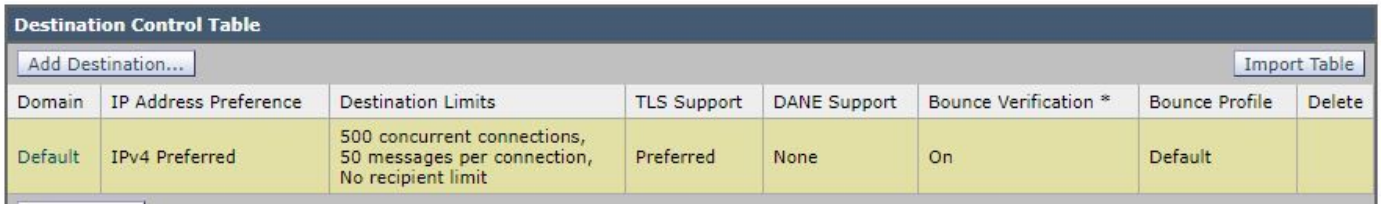


Ahora, habilitemos la verificación de la despedida para nuestro dominio “predeterminado”:

- Navegue **para enviar las directivas > los controles del destino** y para hacer clic en el **valor por defecto.**
- Configure la **verificación de la despedida: Realice marcar con etiqueta del direccionamiento: Yes**



- El tecleo **somete** y **confía los cambios.** Observe que la verificación de la despedida ahora está encendido para el Default Domain.



Usando la tabla de control de destino

La salida incontrolada del correo electrónico puede abrumar los dominios receptores. El ESA le da el control total de la entrega de mensajes definiendo el número de conexiones que su dispositivo se abrirá o el número de mensajes su dispositivo enviará a cada dominio del destino. La tabla de controles de destino proporciona las configuraciones para las tarifas de la conexión y del mensaje cuando el ESA está entregando a los destinos remotos. También proporciona las configuraciones para intentar o aplicar el uso de TLS a estos destinos. El ESA se configura con una configuración predeterminada para la tabla de control de destino.

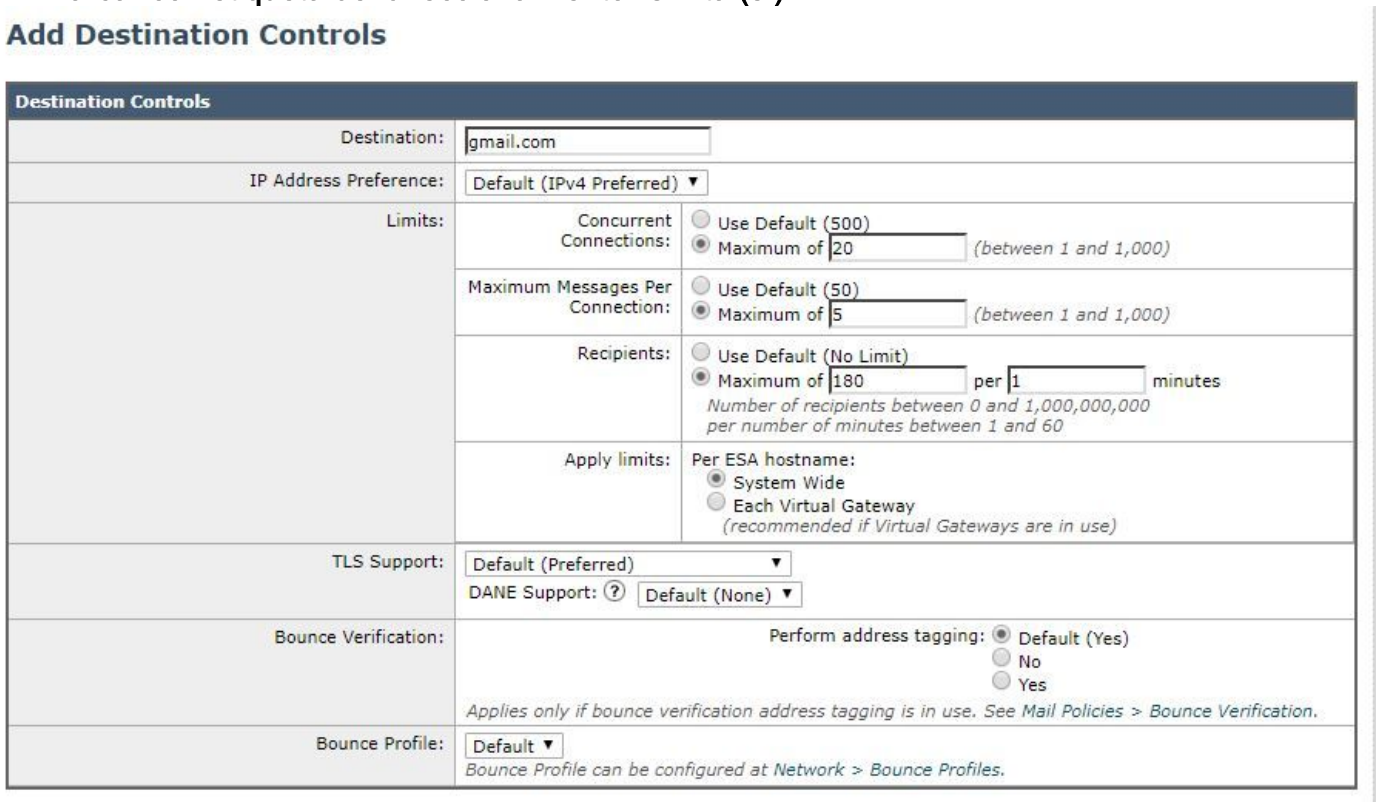
Qué cubriremos en este documento es cómo podemos manejar y configurar el control sobre los destinos donde no está un ajuste el valor por defecto. Por ejemplo, Google tiene un conjunto de recepción gobierna que los usuarios de Gmail deben seguir o arriesgan el enviar apoyan un código de la respuesta S TP 4XX y un mensaje que le dice está enviando demasiado rápidamente, o el buzón del beneficiario ha excedido su límite del almacenamiento. Agregaremos el dominio de Gmail a la tabla de control de destino que limita la cantidad de mensaje enviada a un beneficiario de Gmail abajo.

Agregar un nuevo dominio a la tabla de control de destino

Según lo mencionado, Google tiene limitaciones para los remitentes que envían a Gmail. La recepción de los límites puede ser verificada mirando el remitente aquí - https://support.google.com/a/answer/1366776?hl=en publicado las limitaciones de Gmail

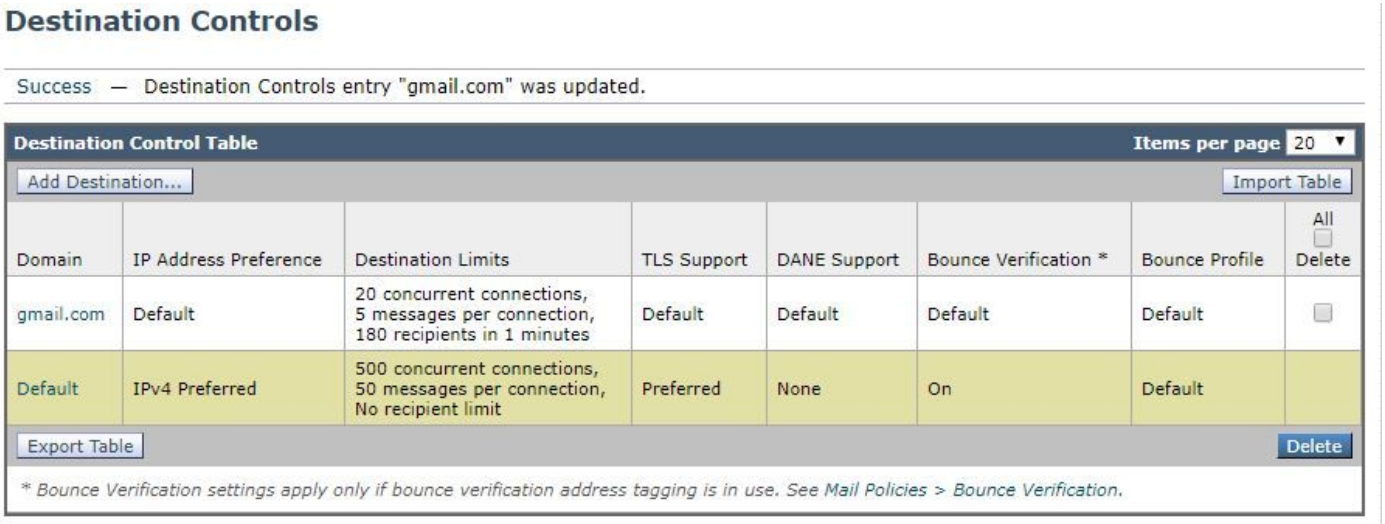
Configuremos el dominio del destino para Gmail como ejemplo de las buenas directivas vecinas.

- Navegue **para enviar las directivas > los controles del destino** y el tecleo **agrega el destino** y crea un nuevo perfil usando los parámetros siguientes: Destino: gmail.com**Preferencia de la dirección IP: IPv4 preferidoConexiones concurrentes: Máximo de 20Mensajes máximos por la conexión: 5Beneficiarios: Máximo de 180 por 1 minutoVerificación de la despedida: Realice marcar con etiqueta del direccionamiento: Omita (sí)**



- El tecleo **somete** y **confía los cambios.** Esto es lo que parece nuestra tabla de control de destino después de la adición del dominio.

Observe el “destino limita” y la “verificación de la despedida” cambia en la imagen abajo:



Autenticación basada en DNS S TP que despliega de Entities Nombrada (DANÉS)

La autenticación basada en DNS S TP del protocolo Named Entities (DANÉS) valida sus Certificados X.509 con los nombres DNS usando una extensión de la Seguridad del Sistema de

nombres de dominio (DNS) (DNSSEC) configurada en su servidor DNS y un registro de recursos DNS, también conocido como expediente TLSA.

El expediente TLSA se agrega en el certificado que contiene los detalles sobre el Certificate Authority (CA), el certificado de la fin-entidad, o el ancla de la confianza usada para el nombre DNS descrito en el RFC 6698. Las Extensiones de la Seguridad del Sistema de nombres de dominio (DNS) (DNSSEC) proporcionan la Seguridad agregada en el DNS dirigiendo las vulnerabilidades en la Seguridad DNS. DNSSEC usando las claves cifradas y las firmas digitales se asegura de que los datos de la búsqueda estén correctos y conecta para legitimar los servidores.

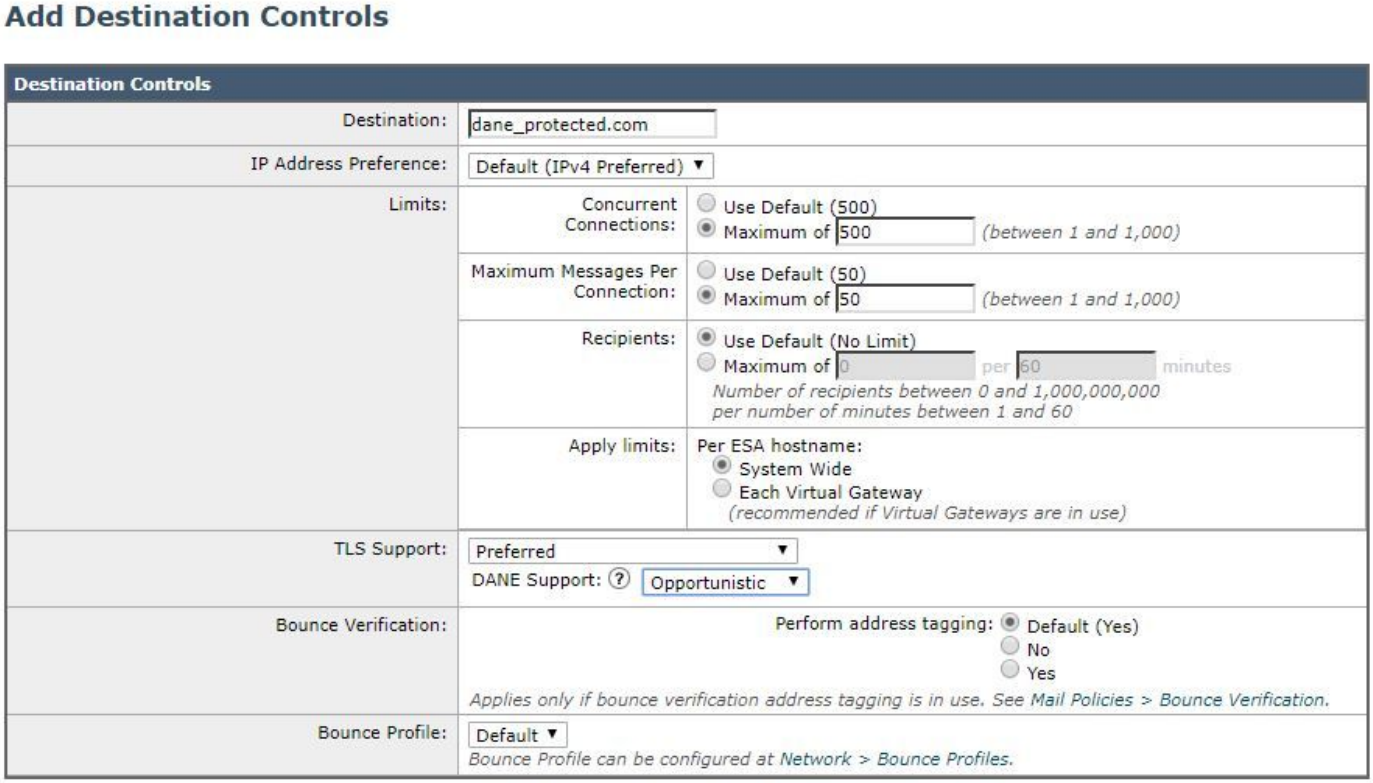
Los siguientes son las ventajas de usar al DANÉS S TP para las conexiones TLS salientes:

- Proporciona la salida segura de los mensajes previniendo los ataques del envenenamiento los ataques del downgrade (MITM), escuchar detras de las puertas y del caché Hombre-en--medios DNS.
- Proporciona la autenticidad de los Certificados y de la información DNS de TLS, cuando es asegurado por DNSSEC.

Configuración ESA

Antes de que usted comience a configurar al DANÉS en el ESA, asegúrese por favor de que el remitente del sobre y el registro de recursos TLSA DNSSEC esté verificado y de que el dominio de recepción es DANÉS protegido. Usted puede hacer esto en el ESA usando el comando CLI **daneverify**.

- Navegue **para enviar las directivas > los controles del destino** y el tecleo **agrega el destino** y crea un nuevo perfil usando los parámetros siguientes: **Destino:** dane_protected.com**Soporte de TLS:** Preferido**Soporte del DANÉS:** Oportunista



- El tecleo **somete** y **confía los cambios.**