

# Guida alle best practice per la verifica dei rimbalzi e i controlli di destinazione

## Sommario

[Introduzione](#)

[Verifica Rimbalzo](#)

[Configurazione ESA](#)

[Utilizzo della tabella di controllo della destinazione](#)

[Aggiunta di un nuovo dominio alla tabella di controllo di destinazione](#)

[Distribuzione dell'autenticazione DNS SMTP di entità denominate \(DANE\)](#)

[Configurazione ESA](#)

## Introduzione

Il recapito di grandi volumi di e-mail non controllato può sovraccaricare i domini dei destinatari. AsyncOS offre il controllo completo sul recapito dei messaggi definendo il numero di connessioni che il servizio Email Security aprirà o il numero di messaggi che invierà a ciascun dominio di destinazione.

In questo documento, tratteremo:

1. Impostazione della verifica dei rimbalzi per proteggere l'organizzazione dagli attacchi di rimbalzo
2. Utilizzo della tabella di controllo della destinazione per applicare criteri appropriati per le risorse adiacenti
3. Distribuzione dell'autenticazione DANE (Named Entities) basata su DNS SMTP per il recapito sicuro dei messaggi

## Verifica Rimbalzo

Abilitare la verifica dei rimbalzi è un ottimo modo per combattere gli attacchi di tipo backscatter/bounce. Il concetto alla base della verifica dei rimbalzi è semplice. Anzitutto, contrassegnare i messaggi che lasciano il ESA. Cercare tale markup in tutti i messaggi di bounce, se il markup è presente, significa che si tratta di un rimbalzo di un messaggio originato nel proprio ambiente. Se il markup è mancante, il rimbalzo è fraudolento e può essere rifiutato o scartato.

Ad esempio, MAIL FROM: joe@example.com diventa MAIL FROM:

prvs=joe=123ABCDEFGFG@example.com. La stringa 123... nell'esempio è il rimbalzo il tag di verifica che viene aggiunto al mittente della busta al momento dell'invio da parte dell'appliance ESA. Se il messaggio salta, l'indirizzo Envelope Recipient nel messaggio rimbalzato includerà il tag per la verifica del rimbalzo, che indica all'ESA che si tratta di un rimbalzo legittimo messaggio.

Potete abilitare o disabilitare l'applicazione di tag di verifica del rimbalzo a livello di sistema come impostazione predefinita. È possibile abilitare o disabilitare anche i tag di verifica del rimbalzo per domini specifici. Nella maggior parte distribuzioni, è abilitata per impostazione predefinita per tutti i

domini.

## Configurazione ESA

- Passare a **Mail Policies > Bounce Verification (Policy di posta > Verifica rimbalzo)** e fare clic su **New Key (Nuova chiave)**

### Bounce Verification

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
<a href="#">Edit Settings</a>	

Bounce Verification Address Tagging Keys	
<a href="#">New Key...</a> <span style="float: right;"><a href="#">Clear All Keys</a></span>	
Address Tagging Keys	Status
IronPort	Current <small>(see Mail Policies &gt; Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>
<a href="#">Purge Keys</a> <a href="#">Not used in one month ▾</a>	

- Immettere il testo arbitrario da utilizzare come chiave nei tag degli indirizzi di codifica e decodifica. Ad esempio, "Cisco\_key".

### New Bounce Verification Key

Add New Bounce Verification Address Tagging Key	
Address Tagging Key:	<input type="text" value="Cisco_key"/> <small>Enter an arbitrary text string to be used as the key in encoding and decoding address tags.</small>

- Fare clic su **Invia** e verificare la nuova chiave di tag dell'indirizzo

### Bounce Verification

Success — New current key added.

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
<a href="#">Edit Settings</a>	

Bounce Verification Address Tagging Keys	
<a href="#">New Key...</a> <span style="float: right;"><a href="#">Clear All Keys</a></span>	
Address Tagging Keys	Status
Cisco_key	Current <small>(see Mail Policies &gt; Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>

Abilitiamo ora la verifica dei rimbalzi per il nostro dominio "predefinito":

- Selezionare **Mail Policies > Destination Controls (Policy di posta > Controlli di destinazione)**, quindi fare clic su **Default**.
- Configura **verifica rimbalzo: Esegue l'assegnazione di tag agli indirizzi: Sì**

## Edit Destination Controls

Default Destination Controls	
IP Address Preference:	IPv4 Preferred ▾
Limits:	Concurrent Connections: <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> No Limit <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="50"/> minutes <i>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</i>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <i>(recommended if Virtual Gateways are in use)</i>
TLS Support:	Preferred ▾ DANE Support: <input type="text" value="None"/> ▾
Bounce Verification:	Perform address tagging: <input type="radio"/> No <input checked="" type="radio"/> Yes <i>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</i>
Bounce Profile:	<i>To edit the Default bounce profile, use Network &gt; Bounce Profiles.</i>

- Fare clic su **Invia e conferma modifiche**. Notare che la verifica dei rimbalzi è ora attiva per il dominio predefinito.

Destination Control Table							
<input type="button" value="Add Destination..."/>							<input type="button" value="Import Table"/>
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support	Bounce Verification *	Bounce Profile	Delete
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	On	Default	

## Utilizzo della tabella di controllo della destinazione

Il recapito non controllato dei messaggi di posta elettronica può sovraccaricare i domini dei destinatari. L'ESA offre il pieno controllo recapito dei messaggi definendo il numero di connessioni che l'accessorio aprirà o il numero di connessioni messaggi che l'accessorio invierà a ogni dominio di destinazione. La tabella dei controlli di destinazione fornisce le impostazioni per la velocità di connessione e di trasmissione dei messaggi quando l'ESA è recapitare a destinazioni remote. Fornisce inoltre le impostazioni per tentare di imporre l'uso di TLS a queste destinazioni. L'ESA è configurata con una configurazione predefinita per la tabella di controllo della destinazione.

In questo documento verrà illustrato come gestire e configurare il controllo sulle destinazioni in cui l'impostazione predefinita non è adatta. Google, ad esempio, dispone di un set di regole di ricezione che gli utenti di Gmail dovrebbero seguire o rischiano di inviare un codice di risposta SMTP 4XX e un messaggio che dice che si sta inviando troppo velocemente, o la cassetta postale del destinatario ha superato il suo limite di archiviazione. Il dominio Gmail verrà aggiunto alla tabella di controllo di destinazione limitando la quantità di messaggi inviati a un destinatario Gmail.

### Aggiunta di un nuovo dominio alla tabella di controllo di destinazione

Come accennato, Google ha delle limitazioni per i mittenti che inviano a Gmail. I limiti di ricezione possono essere verificati osservando le limitazioni del mittente Gmail pubblicate qui - <https://support.google.com/a/answer/1366776?hl=en>

Configuriamo il dominio di destinazione per Gmail come esempio di buone politiche per i vicini.

- Passare a **Mail Policies > Destination Controls** e fare clic su **Add Destination** per creare un nuovo profilo utilizzando i seguenti parametri: **Destinazione: gmail.com** **Preferenza indirizzo IP: IPv4 preferito** **Connessioni simultanee: Massimo 20** **Numero massimo messaggi per connessione: 5** **Destinatari: Max. 180 per 1 minuto** **Verifica Rimbalzo: Esegue l'assegnazione di tag agli indirizzi: Predefinito (Si)**

### Add Destination Controls

Destination Controls	
Destination:	<input type="text" value="gmail.com"/>
IP Address Preference:	Default (IPv4 Preferred) ▼
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="20"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="5"/> (between 1 and 1,000)
	Recipients: <input type="radio"/> Use Default (No Limit) <input checked="" type="radio"/> Maximum of <input type="text" value="180"/> per <input type="text" value="1"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	Default (Preferred) ▼
	DANE Support: <input type="text" value="?"/> Default (None) ▼
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (Yes) <input type="radio"/> No <input type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</small>
Bounce Profile:	Default ▼ <small>Bounce Profile can be configured at Network &gt; Bounce Profiles.</small>

- Fare clic su **Invia e conferma modifiche**. Questo è l'aspetto della tabella di controllo di destinazione dopo l'aggiunta del dominio.

Nota "Limiti di destinazione" e "Verifica rimbalzo" cambiano nell'immagine seguente:

### Destination Controls

Success — Destination Controls entry "gmail.com" was updated.

Destination Control Table							Items per page 20 ▼
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support	Bounce Verification *	Bounce Profile	All <input type="checkbox"/> Delete
gmail.com	Default	20 concurrent connections, 5 messages per connection, 180 recipients in 1 minutes	Default	Default	Default	Default	<input type="checkbox"/>
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	On	Default	

\* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.

## Distribuzione dell'autenticazione DNS SMTP di entità denominate (DANE)

Il protocollo DANE (Authentication of Named Entities) basato su DNS SMTP convalida i certificati X.509 con nomi DNS utilizzando un'estensione DNSSEC (Domain Name System Security)



configurata nel server DNS e un record di risorse DNS, noto anche come record TLSA.

Il record TLSA viene aggiunto nel certificato che contiene i dettagli relativi all'Autorità di certificazione (CA), al certificato dell'entità finale o al trust anchor utilizzato per il nome DNS descritto nella RFC 6698. Le estensioni DNSSEC (Domain Name System Security) offrono una maggiore sicurezza nel DNS risolvendo le vulnerabilità nella sicurezza DNS. DNSSEC utilizza chiavi crittografiche e firme digitali per garantire la correttezza dei dati di ricerca e la connessione a server legittimi.

Di seguito sono elencati i vantaggi dell'utilizzo di DANE SMTP per le connessioni TLS in uscita:

- Fornisce il recapito sicuro dei messaggi impedendo attacchi MITM (Man-in-the-Middle), intercettazioni e avvelenamenti della cache DNS.
- Fornisce l'autenticità dei certificati TLS e delle informazioni DNS, se protetti da DNSSEC.

## Configurazione ESA

Prima di iniziare a configurare DANE sull'ESA, accertarsi che il mittente della busta e il record di risorse TLSA siano verificati per DNSSEC e che il dominio ricevente sia protetto da DANE. È possibile farlo sull'ESA usando il comando **daneverify** della CLI.

- Passare a **Mail Policies > Destination Controls** e fare clic su **Add Destination** per creare un nuovo profilo utilizzando i seguenti parametri: **Destinazione: dane\_protected.com** **Supporto TLS: Preferred (Preferito)** **Supporto DANE: Opportunistico**

### Add Destination Controls

Destination Controls	
Destination:	<input type="text" value="dane_protected.com"/>
IP Address Preference:	<input type="text" value="Default (IPv4 Preferred)"/>
Limits:	Concurrent Connections: <input type="radio"/> Use Default (500) <input checked="" type="radio"/> Maximum of <input type="text" value="500"/> (between 1 and 1,000)
	Maximum Messages Per Connection: <input type="radio"/> Use Default (50) <input checked="" type="radio"/> Maximum of <input type="text" value="50"/> (between 1 and 1,000)
	Recipients: <input checked="" type="radio"/> Use Default (No Limit) <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="60"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: Per ESA hostname: <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	<input type="text" value="Preferred"/> DANE Support: <input type="text" value="Opportunistic"/>
Bounce Verification:	Perform address tagging: <input checked="" type="radio"/> Default (Yes) <input type="radio"/> No <input type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies &gt; Bounce Verification.</small>
Bounce Profile:	<input type="text" value="Default"/> <small>Bounce Profile can be configured at Network &gt; Bounce Profiles.</small>

- Fare clic su **Invia** e conferma modifiche.