

Best Practice Guide for Bounce Verification and Desturement Controles

Inhoud

[Inleiding](#)

[Stapelverificatie](#)

[ESA-configuratie](#)

[Tabel voor doelcontrole gebruiken](#)

[Een nieuw domein aan de tabel met doelcontrole toevoegen](#)

[Hiermee implementeert u DNS-gebaseerde verificatie van benoemde entiteiten \(DANE\)](#)

[ESA-configuratie](#)

Inleiding

Ongecontroleerde levering van hoge aantallen e-mail kan overweldigend gebied zijn. AsyncOS geeft u volledige controle over het leveren van berichten door het aantal verbindingen te bepalen die uw e-mail security service zal openen of het aantal berichten dat naar elk doeldomein zal verzenden.

In dit document zullen wij het volgende behandelen:

1. Oprichtingscontrole instellen om uw organisatie te beschermen tegen aanvallen op de kade
2. Doelcontroletabel gebruiken om goed buurbeleid uit te voeren
3. Het implementeren van DNS-gebaseerde verificatie van benoemde entiteiten (DANE) om veilige levering van berichten te waarborgen

Stapelverificatie

Het toestaan van controle op de bounces is een zeer goede manier om aanvallen te bestrijden met terugkrabbels en stuiters. Het concept achter deze verificatie is eenvoudig. Eerst de berichten die je achterlaten ESA. Als de markup aanwezig is, betekent dat dat, als de markup aanwezig is, dit is een weerkaatsing van een boodschap die in uw omgeving is ontstaan . Als de markering ontbreekt, de aanval is frauduleus en kan worden geweigerd of ingetrokken .

Bijvoorbeeld MAIL VAN: joe@example.com E-MAIL VANUIT:

prvs=joe=123ABCDEFGH@example.com. De 123... string in het voorbeeld is de bounce verificatietag die aan de Envelope Sender wordt toegevoegd zoals deze door uw ESA-apparaat wordt verzonden. Indien Het bericht in de vorm van de Bounces bevat het adres van de ontvanger van de envelop in het aangekondigde bericht de controle-tag bounce, die de ESA laat weten dat het een rechtmatig uitgesproken is bericht.

U kunt verificatie-tagging systeem in- of uitschakelen als standaard. U kunt schakelt u verificatie-tagging voor specifieke domeinen ook in of uit. In de meeste implementaties, wordt deze standaard voor alle domeinen ingeschakeld.

ESA-configuratie

- Navigeren in op **postbeleid > Verificatie** afblazen en op **Nieuwe sleutel** klikken

Bounce Verification

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
Edit Settings	

Bounce Verification Address Tagging Keys	
New Key... Clear All Keys	
Address Tagging Keys	Status
IronPort	Current <small>(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>
Purge Keys Not used in one month ▾	

- Voer een willekeurige tekst in die als de sleutel voor het coderen en decoderen van adrestags moet worden gebruikt. Bijvoorbeeld, "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>

- Klik op **Indienen** en controleer de nieuwe adrestoewijzing-toets

Bounce Verification

Success — New current key added.

Bounce Verification Settings	
Action when invalid bounce received:	Reject
Smart exceptions to tagging:	Enabled
Edit Settings	

Bounce Verification Address Tagging Keys	
New Key... Clear All Keys	
Address Tagging Keys	Status
Cisco_key	Current <small>(see Mail Policies > Destination Controls to set or view destinations which have Bounce Verification Address Tagging enabled)</small>

Schakel deze optie in als u verificatie voor het "standaard"-domein wilt inschakelen:

- Navigeer naar **Mail-beleid > Destination Control** en klik op de **Default**.
- **Bounce verificatie** configureren: **Adres taggen uitvoeren**: Ja

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: <ul style="list-style-type: none"> <input checked="" type="radio"/> No Limit <input type="radio"/> Maximum of <input type="text" value="0"/> per <input type="text" value="50"/> minutes <small>Number of recipients between 0 and 1,000,000,000 per number of minutes between 1 and 60</small>
	Apply limits: <ul style="list-style-type: none"> Per ESA hostname: <ul style="list-style-type: none"> <input checked="" type="radio"/> System Wide <input type="radio"/> Each Virtual Gateway <small>(recommended if Virtual Gateways are in use)</small>
TLS Support:	Preferred ▼ DANE Support: <input type="text" value="None"/> ▼
Bounce Verification:	Perform address tagging: <input type="radio"/> No <input checked="" type="radio"/> Yes <small>Applies only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.</small>
Bounce Profile:	<small>To edit the Default bounce profile, use Network > Bounce Profiles.</small>

- Klik op **Inzenden** en **Commit-wijzigingen**. Merk op dat de Bounce Verificatie nu is ingeschakeld voor het standaarddomein.

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	

Tabel voor doelcontrole gebruiken

Ongecontroleerde e-maillevering kan overweldigend gebied zijn. De ESA geeft u volledige controle bericht-levering door het aantal verbindingen te bepalen dat uw apparaat zal openen of het aantal berichten die uw apparaat naar elk doeldomein stuurt. De tabel met doelbesturingselementen voorziet in instellingen voor de aansluitings- en berichttarieven wanneer de ESA is levering aan afgelegene bestemmingen. Het biedt ook instellingen voor het trachten of afdwingen van het gebruik van TLS op deze bestemmingen. De ESA is ingesteld met een standaardconfiguratie voor de tabel Besturing.

Wat we in dit document zullen behandelen is hoe we controle kunnen uitoefenen en configureren over bestemmingen waar de standaard niet past. Zo heeft Google bijvoorbeeld een reeks regels die Gmail-gebruikers zouden moeten volgen of die het risico lopen een bericht terug te sturen dat u te snel stuurt, of dat de brievenbus van de ontvanger de opslaglimiet heeft overschreden. We voegen het Gmail-domein toe aan de bestemmingstafel. Deze beperkt de hoeveelheid berichten die naar een Gmail-ontvanger wordt gestuurd.

Een nieuw domein aan de tabel met doelcontrole toevoegen

Zoals al is gezegd, heeft Google beperkingen voor het verzenden van berichten naar Gmail. Ontvangende limieten kunnen worden geverifieerd door naar de hier gepubliceerde beperkingen van de Gmail-zender te kijken - <https://support.google.com/a/answer/1366776?hl=en>

Laten we het bestemmingsdomein voor Gmail instellen als voorbeeld van goed buurbeleid.

- Navigeer naar **Mail-beleid > Bestemmingscontroles** en klik op **Bestanden toevoegen** en maak een nieuw profiel met de volgende parameters: **Bestemming: gmail.com****IP-adresvoorkeur: IPv4-voorkeur****Gelijktijdige verbindingen: Max. 20****Max. berichten per verbinding: 5****Ontvangers: Max. 180 per minuut****Bounce verificatie: Adres taggen uitvoeren: Standaard (Ja)**

Add Destination Controls

Destination Controls	
Destination:	<input type="text" value="gmail.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="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:	<input type="text" value="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 > Bounce Verification.</small>
Bounce Profile:	<input type="text" value="Default"/>
	<small>Bounce Profile can be configured at Network > Bounce Profiles.</small>

- Klik op **Inzenden** en **wijzigingen** toezeggen. Zo ziet onze tabel met doelcontrole er uit na de toevoeging van het domein.

In de onderstaande afbeelding worden wijzigingen aangebracht in "Doelbeperingen" en "Bounce Verification":

Destination Controls

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

Destination Control Table							Items per page 20
<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	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.

Hiermee implementeert u DNS-gebaseerde verificatie van benoemde entiteiten (DANE)

Het DNS-gebaseerde Verificatie van Benoemde Entiteiten (DANE)-protocol valideert uw X.509-certificaten met DNS-namen met een DNSSEC-uitbreiding (Domain Name System Security) die op uw DNS-server is geconfigureerd en een DNS-resource record, ook bekend als een TLSA-

record.

De TLSA-record wordt toegevoegd aan het certificaat dat gegevens bevat over de certificaatinstantie (CA), het certificaat van de eindentiteit of het vertrouwensanker dat wordt gebruikt voor de DNS-naam die in RFC 6698 is beschreven. De DNSSEC-uitbreidingen (Domain Name System Security) bieden extra beveiliging op de DNS-beveiliging door kwetsbaarheden in DNS-beveiliging aan te pakken. DNSSEC met cryptografische toetsen en digitale handtekeningen zorgt ervoor dat de "lookup"-gegevens correct zijn en op legitieme servers worden aangesloten.

De volgende voordelen zijn het gebruik van MTP DANE voor uitgaande TLS-verbindingen:

- Verleent veilige levering van berichten door te voorkomen dat aanvallen met een Man-in-the-Middle (MITM) worden gedowngrade, e-mailing en DNS cache vergiftiging.
- Verstrekt de authenticiteit van TLS-certificaten en DNS-informatie, indien beveiligd door DNSSEC.

ESA-configuratie

Voordat u start met het instellen van een DANE op de ESA, zorg er dan voor dat de omslagzender en de TLSA-brongegevens DNSSEC zijn gecontroleerd en dat het ontvangende domein DANE-beschermd is. U kunt dit op de ESA doen met behulp van de CLI-opdracht **daneverify**.

- Navigeer naar **Mail-beleid > Bestemmingscontroles** en klik op **Bestanden toevoegen** en maak een nieuw profiel met de volgende parameters: **Bestemming: dane_protection.com** **TLS-ondersteuning: voorbestemd** **DANE-ondersteuning: opportunistisch**

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 > Bounce Verification.</small>
Bounce Profile:	<input type="text" value="Default"/> <small>Bounce Profile can be configured at Network > Bounce Profiles.</small>

- Klik op **Inzenden** en **Commit-wijzigingen**.