

Come evitare il controllo DMARC su Email Security Appliance

Sommario

[Introduzione](#)

[Verifica DMARC](#)

[Configura bypass DMARC](#)

[Differenza in Mail Logs](#)

[Log di posta per controllo DMARC ignorato](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come evitare il controllo DMARC (Domain-based Message Authentication, Reporting and Conformance) su Email Security Appliance (ESA). Fare riferimento all'[introduzione sull'autenticazione e-mail](#).

Verifica DMARC

DMARC è una specifica tecnica creata per ridurre il rischio di abusi basati su e-mail. DMARC standardizza il modo in cui i destinatari di posta elettronica eseguono l'autenticazione tramite posta elettronica utilizzando il framework SPF (Sender Policy Framework) e i meccanismi DKIM (DomainKeys Identified Mail). Per superare la verifica DMARC, un messaggio di posta elettronica deve superare almeno uno di questi meccanismi di autenticazione e gli identificatori di autenticazione devono essere conformi alla RFC 5322.

L'accessorio consente di:

- Verificare i messaggi e-mail in arrivo utilizzando DMARC.
- Definire i profili per ignorare (accettare, mettere in quarantena o rifiutare) i criteri dei proprietari di dominio.
- Inviare rapporti di feedback ai proprietari dei domini, per rafforzare le distribuzioni di autenticazione.
- Invia rapporti sugli errori di recapito ai proprietari del dominio se le dimensioni del rapporto aggregato DMARC superano 10 MB o le dimensioni specificate nel tag RUA (Aggregated Reports) del record DMARC.

AsyncOS è in grado di gestire e-mail conformi alle specifiche DMARC inviate alla Internet Engineering Task Force (IETF) il 31 marzo 2013. Per ulteriori informazioni, vedere <http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02>.

Nota: L'accessorio non eseguirà la verifica DMARC dei messaggi provenienti da domini con record DMARC in formato non valido. Tuttavia, l'accessorio può ricevere ed elaborare tali messaggi.

Configura bypass DMARC

Se come amministratore il tuo requisito è quello di ignorare la verifica DMARC dei messaggi da mittenti specifici, dovrai seguire alcuni passaggi per raggiungere il bypass con successo. Di seguito è riportata una panoramica dei passaggi:

Nota: Gli elenchi di indirizzi creati solo con l'utilizzo di indirizzi di posta elettronica completi o domini possono essere utilizzati per ignorare la verifica DMARC. È possibile utilizzare un **elenco indirizzi** con l'opzione **Tutti i precedenti**. Tuttavia, le voci con solo dominio/indirizzo di posta elettronica completo o indirizzo di dominio parziale funzioneranno per un'eccezione. È necessario utilizzare il **dominio/indirizzo e-mail completo** indicato nell'intestazione **From**.

1. Verificare che **Verifica DMARC** sia attivata per il criterio flusso di posta associato.
2. Selezionare **Mail Policies > Address List** (Policy di posta > Elenco indirizzi).
3. Fare clic su **Aggiungi elenco indirizzi**.
4. Creare un **elenco indirizzi** immettendo i dettagli.
5. Fare clic su **Submit (Invia)**.
6. Una volta creato l'**elenco indirizzi**, sarà necessario richiamarlo per **ignorare l'elenco indirizzi di mittenti specifici DMARC**.

Di seguito è riportato un esempio di come è possibile configurare la configurazione di bypass e come verrà eseguita la registrazione:

L'elenco indirizzi viene creato con "**Solo domini**" come esempio e aggiunto nei dettagli dell'intestazione **From**.

Edit Address List Details	
Address List Name:	<input type="text" value="Bypass_test"/>
Description:	<input type="text" value="bypass DMARC"/>
List Type:	<input type="radio"/> Full Email Addresses only <input checked="" type="radio"/> Domains only <input type="radio"/> IP Addresses only <input type="radio"/> All of the above
Addresses:	<input type="text" value="@whitelist.com"/> e.g.: @example.com, @.example.com

Dopo aver creato l'elenco indirizzi con tutte le voci desiderate, sarà necessario chiamare l'**elenco indirizzi** in **Mittenti specifici DMARC Ignora elenco indirizzi**. Passare a **Mail Policies > DMARC > Edit Global Settings** (Policy di posta > DMARC > Modifica impostazioni globali) e chiamare l'**elenco indirizzi** appena creato facendo clic sull'elenco a discesa, come mostrato di seguito:

DMARC Global Settings	
Specific senders bypass address list:	<div style="border: 1px solid gray; padding: 2px;"> None <input checked="" type="checkbox"/> Bypass_test <input type="checkbox"/> SMARC_bypass </div>
Bypass verification for messages with headers:	<input type="text"/> <small>(e.g. List-ID, List-Subscribe)</small>
Schedule for report generation:	<input type="text" value="12"/> <input type="text" value="00"/> <input type="text" value="AM"/>
Entity generating reports:	<input type="text"/>
Additional contact information for reports:	<input type="text"/>
Send copy of all aggregate reports to:	<input type="text"/>
Error Reports:	<input type="checkbox"/> Enable sending of delivery error reports

Differenza in Mail_Logs

Qui viene presentata una rappresentazione dei log di posta che aiuta a comprendere la differenza tra la registrazione, quando il DMARC di un dominio viene convalidato e quando è configurato per ignorare.

Registri di posta quando DMARC è selezionato:

```
Sat Mar 20 21:14:22 2021 Info: ICID 57 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable
```

```
Sat Mar 20 21:14:22 2021 Info: Start MID 76571 ICID 57
```

```
Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 From:
```

```
Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 RID 0 To:
```

```
Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC: Verification skipped (No record found for the
sending domain)
```

```
Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC:
```

```
Sat Mar 20 21:14:23 2021 Info: MID 76571 Message-ID '<613a1e1b-998a-6375-8887-
ab2c6d430256@whitelist.com>'
```

```
Sat Mar 20 21:14:23 2021 Info: MID 76571 Subject 'Test 4'
```

Nota: Non è stato pubblicato alcun record per il dominio @whitelist.com, motivo per cui viene visualizzato "Nessun record trovato per il dominio di invio".

Log di posta per controllo DMARC ignorato

```
Sat Mar 20 21:15:36 2021 Info: ICID 58 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable
```

```
Sat Mar 20 21:15:37 2021 Info: Start MID 76572 ICID 58
```

```
Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 From:
```

```
Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 RID 0 To:
```

Sat Mar 20 21:15:37 2021 Info: MID 76572 **DMARC: Verification skipped (Local bypass configuration)**

Sat Mar 20 21:15:37 2021 Info: MID 76572 Message-ID '<2ba742a2-f8ba-9ff0-7dc9-362421f5177e@whitelist.com>'

Sat Mar 20 21:15:37 2021 Info: MID 76572 Subject 'Test Bypass DMARC'

Informazioni correlate

- [Informazioni sul flusso di lavoro DMARC](#)
- [Verifica dei messaggi in arrivo tramite DMARC](#)
- [Filtro per gestire i messaggi che hanno ignorato la verifica DMARC](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)