Filtro per gestire i messaggi che hanno ignorato la verifica DMARC

Sommario

Introduzione

In questo documento viene descritto come creare un filtro per attivare e-mail che ignorano la verifica DMARC (Domain-based Message Authentication, Reporting And Conformance) in Email Security Appliance (ESA) e Cloud Email Security (CES).

Requisiti

Prerequisiti

- AsyncOS versione 11.1.2 e successive.
- Informazioni su DMARC (https://tools.ietf.org/html/rfc7489#page-56)
- ESA/CES con verifica DMARC abilitata.

Premesse

ESA/CES con verifica DMARC configurata sulle policy di flusso della posta, dove verifica messaggi/mail_logs stanno restituendo la riga di log: **DMARC: Verifica ignorata (impossibile determinare il dominio di invio)**".

Questa riga di log indica che ESA/CES ha rilevato più di un'identità di dominio nell'intestazione from e quando nell'intestazione sono presenti più indirizzi e-mail, questa intestazione verrà ignorata nella maggior parte delle implementazioni DMARC.Le intestazioni di elaborazione con più di un'identità di dominio sono esposte come fuori ambito nella specifica DMARC.

Filtro soluzione

Cisco AsyncOS versione 11.1.2 e successive versioni aggiunge una nuova funzione dove il dispositivo includerà una nuova x-header che acquisisce Risultati della verifica DMARC con un valore univoco basato sul risultato della verifica DMARC.

Sono disponibili quattro valori di intestazione da filtrare: validskip, invalidskip, temperror e

premerror.

> **Nota**: nei casi in cui non è stato possibile eseguire la verifica DMARC a causa della presenza di caratteri speciali o di intestazioni da in formato non corretto oppure perché il controllo DMARC non è riuscito a causa di un'altra omissione valida o non valida, l'intestazione x aggiunta sarà: **X-Ironport-Dmarc-Check-Result:** invalidskip o validskip.

> **Nota:** Questo filtro può essere distribuito sia nei filtri messaggi (con restrizioni CLI) che nei filtri contenuti.

Valori intestazione:

- **L'opzione Ignora valido** copre i casi in cui non è stato possibile eseguire la verifica DMARC quando è presente un'intestazione from o non è presente alcun record DMARC.
- **Ignora non valido** copre i casi in cui sono presenti caratteri non validi nell'intestazione da, più intestazioni da, più entità di dominio nell'intestazione da, l'indirizzo del mittente contiene caratteri non ASCII US e se si verifica un errore nell'analisi dei valori nel campo dell'intestazione da.
- **Permerror** copre i casi in cui si è verificato un errore permanente durante la valutazione DMARC, ad esempio quando si è verificato un record DMARC sintatticamente errato. È improbabile che un tentativo successivo produca un risultato finale.
- **Temperror** copre i casi in cui si è verificato un errore temporaneo durante la valutazione DMARC.Un tentativo successivo potrebbe produrre un risultato finale.

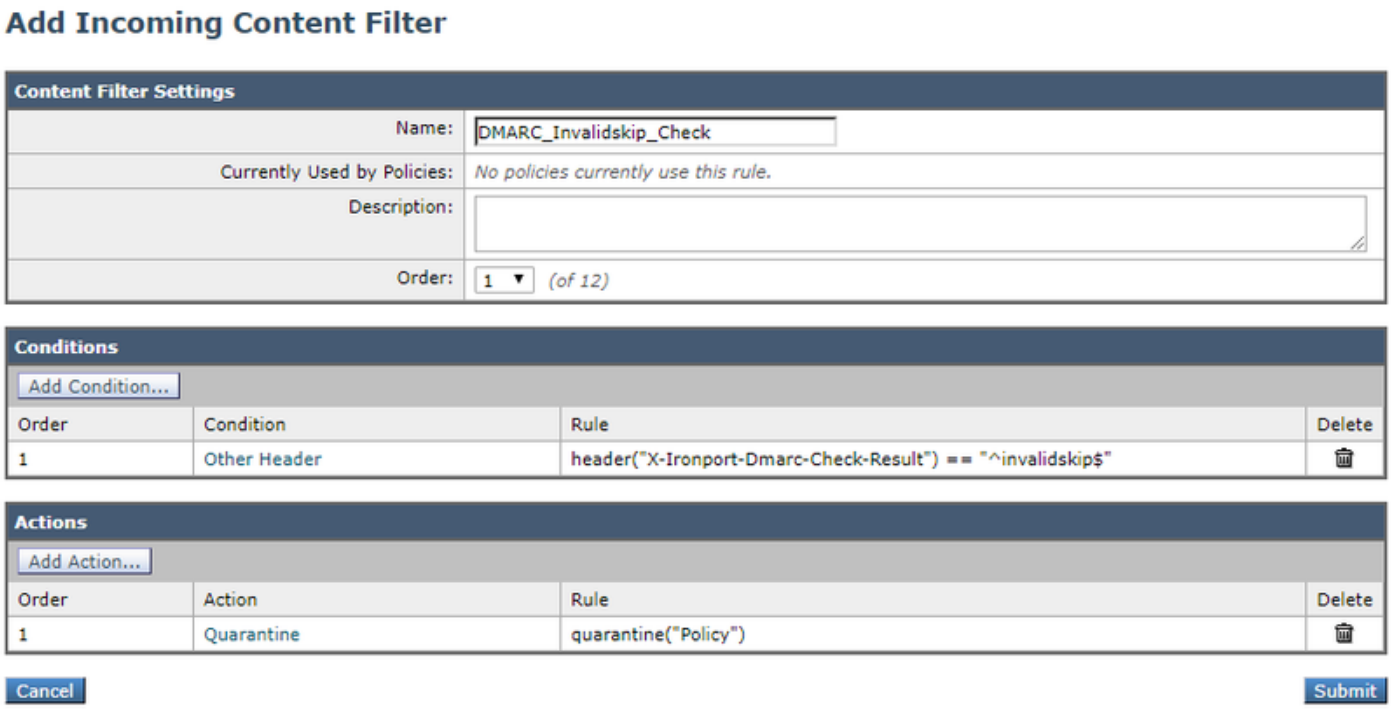
Di seguito viene riportato il filtro DMARC che controlla **"X-Ironport-Dmarc-Check-Result"** per individuare un **salto non valido** e procede alla quarantena.

Se necessario, l'azione può essere personalizzata in base ad altri requisiti.

Filtro messaggi

```
Quarantine_messages_DMARC_skip:
if header("X-Ironport-Dmarc-Check-Result") == "^invalidskip$"
{
quarantine("Policy");
}
```

Filtro contenuti



Informazioni correlate

- [Cisco Email Security Appliance - Guide per l'utente]
- [Documentazione e supporto tecnico – Cisco Systems]
- [Che cos'è DMARC?]