Filtern zur Behandlung von Nachrichten, die die DMARC-Überprüfung übersprungen haben

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Filter für Aktionsemail erstellen, der die domänenbasierte Überprüfung von Authentifizierung, Reporting und Konformität (DMARC) in der E-Mail-Security-Appliance (ESA) und Cloud E-Mail Security (CES) übersprungen hat.

Anforderungen

Voraussetzungen

- AsyncOS 11.1.2 und höher
- Verständnis von DMARC (https://tools.ietf.org/html/rfc7489#page-56)
- ESA/CES mit aktivierter DMARC-Überprüfung.

Hintergrundinformationen

ESA/CES mit DMARC-Verifizierung, die auf den Mail-Flow-Richtlinien konfiguriert ist, bei denen die Protokollzeile durch Nachrichtenverfolgung/Mail_Protokolle generiert wird: **DMARC: Übersprungene Überprüfung (sendende Domäne konnte nicht bestimmt werden)**".

Diese Protokollzeile bedeutet, dass die ESA/CES mehr als eine Domänen-Identität im Header "From" erkannt hat und wenn mehr als eine E-Mail-Adresse im Header vorhanden ist, wird dieser Header in den meisten DMARC-Implementierungen übersprungen.Verarbeitende Header mit mehr als einer Domänen-Identität werden in der DMARC-Spezifikation als Out-of-Scope verfügbar gemacht.

Workaround-Filter

Die Cisco AsyncOS 11.1.2-Version und die folgenden Versionen fügen eine neue Funktion hinzu, bei der das Gerät einen neuen x-Header enthält, der verschiedene Die Ergebnisse der DMARC-Verifizierung werden mit einem eindeutigen Wert auf Basis des DMARC-Verifizierungsergebnisses ermittelt.

Es gibt vier Headerwerte, die gefiltert werden können: "validskip", "invalidskip", "temperror" und "permerror".

> **Hinweis**: In den Fällen, in denen die DMARC-Überprüfung nicht durchgeführt werden konnte, weil Sonderzeichen vorhanden waren oder die von-Headern fehlerhaft sind oder die DMARC-Prüfung fehlschlug, weil eine andere ungültige SKP-Nichtübereinstimmung besteht oder ungültiges Überspringen nicht möglich ist, wird folgender X-Header hinzugefügt: **X-Ironport-Dmarc-Check-Result:** ungültigSkip oder validskip.

> **Hinweis**: Dieser Filter kann sowohl auf den Nachrichtenfiltern (CLI eingeschränkt) als auch auf den Content-Filtern bereitgestellt werden.

Headerwerte:

- **Gültige Übersprungen** decken die Fälle ab, in denen die DMARC-Überprüfung nicht durchgeführt werden konnte, wenn es einen from-Header oder keinen DMARC-Datensatz gibt.
- **Ungültiges Überspringen** deckt die Fälle ab, in denen der from-Header ungültige Zeichen, mehrere from-Header, mehrere Domänen-Entitäten im from-Header enthält, die Absenderadresse nicht-US-ASCII-Zeichen hat und bei denen ein Fehler beim Analysieren von Werten im from-Headerfeld aufgetreten ist.
- **Permerror** deckt Fälle ab, in denen während der DMARC-Evaluierung ein permanenter Fehler aufgetreten ist, z. B. wenn ein syntaktisch inkorrekter DMARC-Datensatz gefunden wurde. Ein späterer Versuch ist unwahrscheinlich, ein Endergebnis zu erzielen.
- **Temperror** deckt Fälle ab, in denen während der DMARC-Evaluierung ein vorübergehender Fehler aufgetreten ist.Ein späterer Versuch kann zu einem Endergebnis führen.

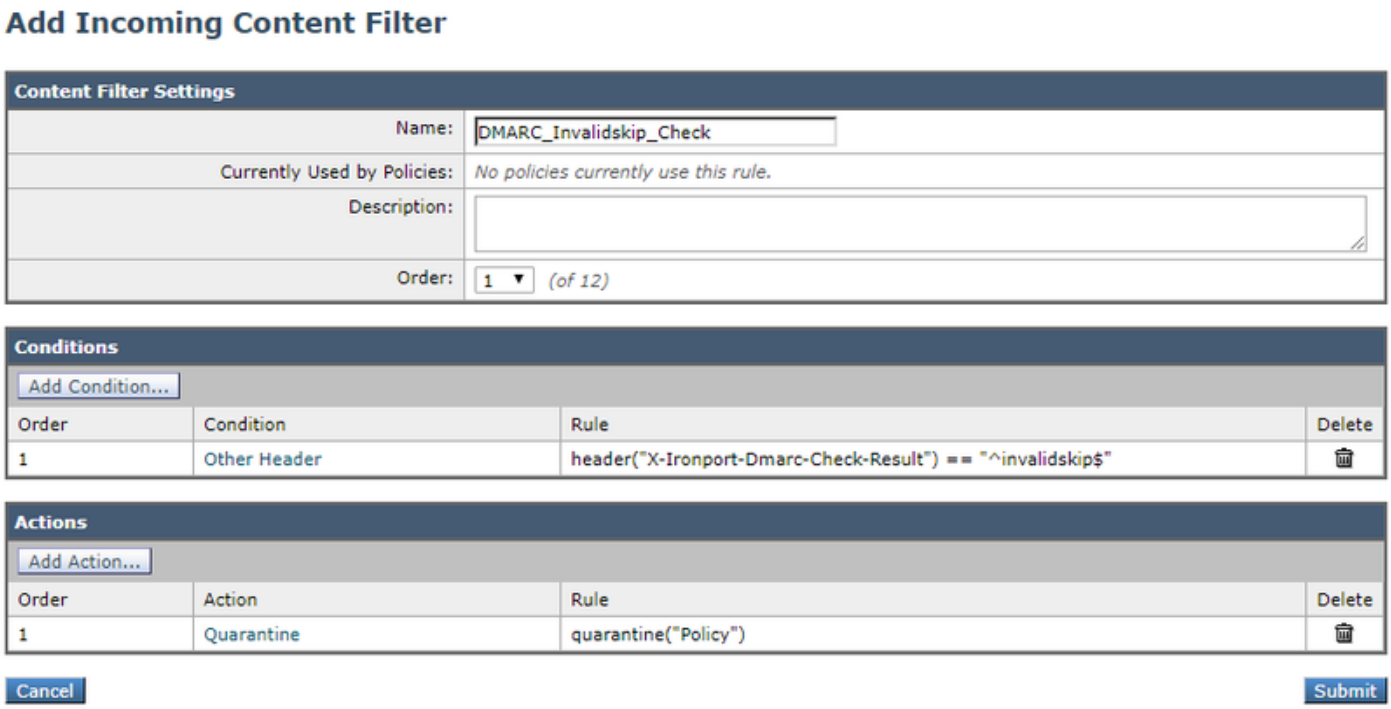
Im Folgenden sehen Sie den DMARC-Filter, der das **"X-Ironport-Dmarc-Check-Result"** auf einen **ungültigenSKP** überprüft und diesen unter Quarantäne stellt.

Die Aktion kann bei Bedarf an andere Anforderungen angepasst werden.

Nachrichtenfilter

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

Content-Filter



Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems
- Was ist DMARC?