ESR2000 MTP-verificatievoorwaarde om spoeling te voorkomen

Inhoud

Inleiding

Dit document beschrijft hoe u een filter kunt maken op basis van de MGN (Simple Mail Transfer Protocol) - geverifieerde gebruiker en log de gebruikersnaam in een X-header.

Voorwaarden

Cisco raadt u aan kennis te hebben van AsyncOS versie 6.5 en hoger.

Achtergrondinformatie

Met de MTP-verificatiefunctie kunnen klanten voor hun cliënten gebruik maken van een MTP-verificatie om verbinding te maken met e-mail security applicaties (ESA's) en deze te versturen. Aangezien deze functie de geauthentiseerde gebruiker toelaat om door te geven, is het mogelijk voor gebruikers om het veld "Van:" in e-mails te vervalsen die zij door het Cisco ESA verzenden. Om te voorkomen dat gebruikers zich vormgeven, bevat het ESR AsyncOS versie 6.5 en bevat het later een berichtfiltervoorwaarde die vergelijkingen met de geauthentiseerde gebruikersnaam en de **e-mail van** e-mailadres toestaat.

Een filter maken

De voorwaarde van het berichtfilter staat een beheerder toe om een filter te schrijven gelijkend op de voorbeeldregel in de volgende sectie die e-mails vergelijkt die uitgestoten worden via een MTP-authentificatiesessie. Als de MTP-referenties worden gecompromitteerd, genereert de machine die de e-mails verstuurt doorgaans verschillende adressen die als de post **Van** worden gebruikt**:** kopbal. Met de functie berichtfilter kunt u alleen e-mails verlaten als de gebruikersnaam en e-mail **van:** kopregels passen bij elkaar. Anders wordt de e-mail beschouwd als een gesmeerde mail **vanuit:** en wordt de actie van het bericht filter geactiveerd. De actie van het berichtfilter kan elke

definitieve actie zijn; de voorbeeldregel toont een quarantaineactie . Het filter heeft de volgende syntaxis:

```
smtp-auth-id-matches("<target>" [, "<sieve-char>"])
```

Het filter maakt een vergelijking met een van deze doelen mogelijk:

- **OmvangVan:** Vergelijk het adres dat in **Mail** is opgegeven**:** in het gesprek van de MTP.
- **VanAdres:** Vergelijk de adressen die uit de **Van zijn** ontleend**:** kopbal. Aangezien meerdere adressen in het **Van** zijn toegestaan**:** kopje, er moet maar één overeenkomen.
- **Afzender:** Vergelijk het adres in de **afzender:** kopbal.
- **Alle:** Overeenkomst berichten die tijdens een geauthentiseerde zitting (ongeacht de identiteit) werden gemaakt.
- **None:** Overeenkomstberichten die niet werden gemaakt tijdens een geauthentiseerde MTP-sessie (bijvoorbeeld wanneer MTP-verificatie de **voorkeur** krijgt).

TCP-ID	SIEVE CHAR	VERGELIJKBAAR ADRES	MATCHES?
jongeman		otheruser@example.com	Nee
jongeman		someuser@example.com	Ja
jongeman		someuser@face.localhost	Ja
Sommige gebruikers		someuser@example.com	Ja
jongeman		someuser+folder@example.com	Nee
jongeman	+	someuser+folder@example.com	Ja
someUser@example.com		someuser@forged.com	Nee
someUser@example.com		someuser@example.com	Ja
someUser@example.com		someuser@example.com	Ja

Deze variabele substitutie, **$SMTPAuthID**, werd gecreëerd om opname in kopregels van de oorspronkelijke authenticatie geloofsbrieven toe te staan die werden gebruikt om af te geven.

Voorbeelden

```
Msg_Authentication: if (smtp-auth-id-matches("*Any"))
{
   # Always include the original authentication credentials in a
   # special header.
   insert-header("X-SMTPAUTH", "$SMTPAuthID");

   if (smtp-auth-id-matches("*FromAddress", "+") and
       smtp-auth-id-matches("*EnvelopeFrom", "+"))
   {
       # Username matches.  Verify the domain
       if (header('from') != "(?i)@(?:example\.com|example\.com)" or mail-from !=
"(?i)@(?:example\.com|\.com)"
       {
           # User has specified a domain which cannot be authenticated
           quarantine("forged");
       }
   } else {
       # User claims to be an completely different user
       quarantine("forged");
   }
}
```

Opmerking: Deze filter veronderstelt dat je een quarantaine hebt die **vervalst** wordt

genoemd.

Gerelateerde informatie

- IJzeren poort asynchrone/synchrone geavanceerde gebruikershandleiding voor IronPort E-mail security applicaties
- Technische ondersteuning en documentatie – Cisco Systems