Hoe stel ik de ESA in om anti-spam en/of anti-virus scannen naar mijn vertrouwde afzenders over te slaan?

Inhoud

vraag

Hoe stel ik de ESA in om anti-spam en/of anti-virus scannen naar mijn vertrouwde afzenders over te slaan?

Antwoord

AsyncOS biedt drie belangrijke gereedschappen die u kunt gebruiken om anti-spam of anti-viruscontrole over te slaan voor uw meest vertrouwde afzenders. Houd er rekening mee dat de ESA op geen enkel moment adviseert om antiviruscontroles te annuleren, zelfs niet voor uw meest vertrouwde zenders, vanwege de mogelijkheid van een onbedoelde virusinfectie. Hieronder vindt u een discussie over de drie manieren waarop u antispam-controles voor een deel van de berichtstroom kunt overslaan.

Het eerste gereedschap dat u beschikbaar is, is het beleid voor Mail Flow Line van Host Access Tabel (HAT). Met het beleid van Mail Flow kunt u zenders door IP-adres identificeren (met behulp van numerieke IP-adressen of PTR DNS-namen), door SenderBase-score of door een lokale DNS-lijst of een blocklist. Zodra u afzender als vertrouwd binnen een Groep van het Sender in HAT hebt geïdentificeerd, kunt u die sendergroep dan merken om anti-spam scannen te overslaan.

Stel dat je bijvoorbeeld een specifieke zakelijke partner, BIJVOORBEELD.COM, wilde identificeren die geen anti-spam controle op hun post zou moeten hebben. U moet de IP-adressen van de mailserver van SCU.COM (of DNS-muisrecords) bekijken. In dit geval moeten we ervan uitgaan dat EXAMPLE.COM mailservers heeft die IP-adressen hebben met DNS PTR-records van "smtp1.mail.scu.com" via "smtp4.mail.scu.com". Denk er in dit geval aan dat we kijken naar de PTR-record (soms omgekeerde DNS genoemd) voor de mail servers; Dit heeft niets te maken met de domeinnaam die mensen op SCU.COM gebruiken voor uitgaande post.

U kunt een nieuwe verzendgroep maken (of een bestaande sendergroep gebruiken, zoals ALLOWLIST) met Mail-beleid>Overzicht>Add Sender Group. Laten we er een maken, genaamd "NotSpammers". Nadat u deze pagina hebt verzonden, wordt u teruggestuurd naar het scherm Mail Policy>Overzicht, waar u de mogelijkheid krijgt om een nieuw beleid toe te voegen voor deze verzendende groep. Als u op "Toevoegen beleid" klikt, krijgt u de mogelijkheid om een nieuw beleid te maken. In dit geval willen we het standaardbeleid op één gebied alleen maar omzeilen: Spam-detectie. Geef het beleid een naam en stel het verbindingsgedrag in om "Accept" te zijn. scrollen vervolgens naar het vak Spam Detectie en stel dit beleid in om spamcontrole over te

slaan. Geef dat nieuwe beleid aan en vergeet niet om 'Wijzigingen te plegen'.

Een alternatieve benadering is het gebruik van inkomende e-mailbeleid om anti-spam-scannen te overslaan. Het verschil tussen het HAT- en het inkomende postbeleid is dat de HAT volledig gebaseerd is op de IP-informatie over de verzender: het juiste IP-adres, het IP-adres zoals weergegeven in de DNS, de SenderBase-score (die is gebaseerd op het IP-adres) of een DNS-alimiet of een blokkade-lijst op basis van het IP-adres. Inkomend postbeleid is gebaseerd op informatie over de berichtenenvelop: Het bericht is afkomstig van of naar wie het bericht is gericht. Dit betekent dat het bericht vatbaar is voor misleiding door iemand die een bericht verzenden. Maar als je simpelweg alle anti-spam controles voor inkomende post wilt overslaan van mensen die e-mailadressen hebben die eind in "@voorbeeld.com" houden zou je dat ook kunnen doen.

Om zo'n beleid te creëren, ga naar **Mail-beleid > Inkomend postbeleid > Toevoegen beleid**. Dit zal u een beleid laten toevoegen dat een reeks zenders (of ontvangers) definieert. Zodra u het inkomende e-mailbeleid hebt gedefinieerd, wordt dit weergegeven in het overzichtsscherm (Mail Policy>Inkomend-mailbeleid). U kunt vervolgens op de kolom "Anti-spam" klikken en de specifieke instellingen voor anti-spam voor deze specifieke gebruiker bewerken.

De anti-spam instellingen voor een bepaald beleid hebben veel opties, maar in dit geval willen we simpelweg anti-spam controles overslaan. Let hier op een ander verschil tussen op HAT gebaseerd beleid en inkomend postbeleid: Met HAT kunt u alleen antispamscan overslaan of niet overslaan, terwijl het beleid voor inkomende e-mail een veel grotere controle heeft. U kunt bijvoorbeeld kiezen om spam uit bepaalde zenders in quarantaine te plaatsen en spam uit andere zenders te verwijderen.

De derde optie voor het overslaan van een antispamscan is door een Berichtfilter te configureren en te gebruiken.

> Opmerking: Content Filters kunnen voor dit programma niet worden gebruikt, omdat contentfilters voorkomen nadat anti-spam-scannen al is uitgevoerd

Een van de acties in berichtfilters is "skip-spamcheck." Het onderstaande berichtfilter slaat de anti-spam controle over voor zenders die een bepaald IP adres hebben of die uit een bepaalde domeinnaam komen:

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')      )
   {
       skip-spamcheck();
   }
```

Lees de gebruikershandleiding voor meer informatie over het gebruik van Berichtfilters om de versie van AsyncOS te bekijken die wordt ingezet.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems