ESA FAQ: Wat is een poststroombeleid?

Inhoud

Inleiding

In dit document wordt beschreven wat een poststroombeleid is op de e-mail security applicatie (ESA) en welke acties er zijn gekoppeld aan een poststroombeleid.

Wat is een poststroombeleid?

Een poststroombeleid staat u toe om de stroom e-mailberichten van een afzender aan de luisteraar tijdens het gesprek te controleren of te beperken. U beheerst gesprekken in TCP door de volgende typen parameters te definiëren in het poststroombeleid:

- Verbindingsparameters, zoals maximum aantal berichten per verbinding.
- Snelheidsbeperkende parameters, zoals het maximale aantal ontvangers per uur.
- Wijzig aangepaste codes en antwoorden die tijdens het gesprek worden gecommuniceerd.
- Spamdetectie inschakelen.
- virusbescherming inschakelen.
- Versleuteling, zoals het gebruik van TLS om de TCP-verbinding te versleutelen.
- Verificatieparameters, zoals het gebruik van DKIM om inkomende mail te controleren.

Het beleid van de poststroom voert een van de volgende acties op verbindingen van verre gastheren uit:

- ACCEPTEREN. De verbinding wordt geaccepteerd en e-mailacceptatie wordt vervolgens verder beperkt door luisteraarinstellingen, inclusief de Content Access Table (RAT) (voor openbare luisteraars).
- AFSCHAFFEN. De verbinding wordt aanvankelijk geaccepteerd, maar de client die probeert verbinding te maken krijgt een 4XX of 5XX status code met een MTP-status. Een e-mail is niet geaccepteerd.

  Opmerking: U kunt ook AsyncOS configureren om deze afstoting uit te voeren op het niveau van de berichtontvanger (RCPT TO), in plaats van aan het begin van het gesprek mtp. Het afwijzen van berichten vertraagt op deze manier de berichtafstoting en baseert het bericht op, wat AsyncOS in staat stelt om gedetailleerdere informatie over de verworpen berichten te bewaren. Deze instelling wordt ingesteld in de CLI **listenerfig > Setup-**opdracht.

- TCPFANUSSEN. Verbinding wordt geweigerd op het TCP-niveau.
- RELAY. Verbinding wordt geaccepteerd. Ontvangst voor elke ontvanger is toegestaan en wordt door de RAT niet beperkt.
- DOORGAAN. De afbeelding in de Host Access Tabel (HAT) wordt genegeerd en de verwerking van de HAT wordt voortgezet. Als de inkomende verbinding overeenkomt met een latere ingang die niet VERDER is, dan wordt die ingang gebruikt. De CONTINUE-regel wordt gebruikt om het bewerken van de HAT in de GUI te vergemakkelijken.

Houd in gedachten, het beleid van de poststroom is aan het begin van de e-mailleiding, dus deze parameters worden toegepast als verafgelegen hosts probeert verbinding te maken met het ESA.

Het beleid van de Mail-flow verschilt van het beleid van de Inkomend en Uitgaande Mail, dat anti-spam, anti-virus, virus uitbraak en content filter definieert, dat toegepast wordt op e-mail die ontvangen wordt van of bestemd is voor bepaalde domeinen, groepen e-mailadressen of specifieke e-mailadressen.

Het beleid van de standaard poststroom kan worden aangepast en het nieuwe beleid van de mailflow kan worden gedefinieerd.

Er zijn vier standaardinstellingen voor de poststroom die worden gedefinieerd door luisteraars:

- AANVAARD
- GEBLOKKEERD
- VERDWENEN
- VERTROUWD

Private luisteraars gebruiken het volgende beleid voor de poststroom:

- AANVAARD
- GEBLOKKEERD
- VERLAAGD

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems