

ةسايس يه ام :ESA لوح ةل وادتم لا ةلئس أا ؟دي ربل ا ق ف دت

المحتويات

[المقدمة](#)

[ما هي سياسة تدفق البريد؟](#)

[معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند ما هي سياسة تدفق البريد الموجودة على جهاز أمان البريد الإلكتروني (ESA)، والإجراءات المقترنة بنهج تدفق البريد.

ما هي سياسة تدفق البريد؟

يسمح لك نهج تدفق البريد بالتحكم في تدفق رسائل البريد الإلكتروني من المرسل إلى موزع الرسائل أثناء محادثة SMTP أو الحد من تدفقها. يمكنك التحكم في محادثات SMTP عن طريق تحديد الأنواع التالية من المعلمات في نهج تدفق البريد:

- معلمات الاتصال، مثل الحد الأقصى لعدد الرسائل لكل اتصال.
 - معلمات تحديد المعدل، مثل الحد الأقصى لعدد المستلمين في الساعة.
 - تعديل رموز SMTP المخصصة والاستجابات التي تم الاتصال بها أثناء محادثة SMTP.
 - تمكين الكشف عن البريد العشوائي.
 - تمكين الحماية من الفيروسات.
 - التشفير، مثل استخدام TLS لتشفير اتصال SMTP.
 - معلمات المصادقة، مثل استخدام DKIM للتحقق من البريد الوارد.
- تقوم سياسات تدفق البريد بتنفيذ أحد الإجراءات التالية على الاتصالات من الأجهزة المضيفة البعيدة:
- قبول. تم قبول الاتصال، ثم تم تقييد قبول البريد الإلكتروني أكثر من قبل إعدادات المصغي، بما في ذلك جدول وصول المستلم (RAT) (للمستمعين العاميين).
 - رفض. تم قبول الاتصال في البداية، ولكن العميل الذي يحاول الاتصال يحصل على رمز حالة SMTP 4XX أو 5XX. لم يتم قبول أي بريد إلكتروني.

ملاحظة: يمكنك أيضا تكوين AsyncOS لإجراء هذا الرفض على مستوى مستلم الرسالة (RCPT إلى)، بدلا من بداية محادثة SMTP. يؤدي رفض الرسائل بهذه الطريقة إلى تأخير رفض الرسالة وقلب الرسالة، مما يسمح ل AsyncOS بالاحتفاظ بمعلومات أكثر تفصيلا حول الرسائل المرفوضة. تم تكوين هذا الإعداد من أمر `CLI listEnergyConfig > setup`.

- Tcprefuse. تم رفض الاتصال على مستوى TCP.
- ترحيل. تم قبول الاتصال. يسمح بالاستلام لأي مستلم ولا يقيد الجرذ.

• متابعة. يتم تجاهل التخطيط في جدول الوصول إلى المضيف (HAT)، وتستمر معالجة HAT. في حالة تطابق الاتصال الوارد مع إدخال لاحق غير "متابعة"، يتم استخدام هذا الإدخال بدلا من ذلك. تستخدم قاعدة "المتابعة" لتسهيل تحرير HAT في واجهة المستخدم الرسومية (GUI).
تذكر أن سياسات تدفق البريد هي في بداية تدفق البريد الإلكتروني، لذلك يتم تطبيق هذه المعلمات كمضيفين عن بعد يحاولون إنشاء اتصالات مع ESA.

تختلف سياسات تدفق البريد عن سياسات البريد الصادر والوارد، التي تحدد معلمات مكافحة البريد العشوائي ومكافحة الفيروسات وتفشي الفيروسات وتصفية المحتوى التي سيتم تطبيقها على البريد المستلم من المجالات المحددة أو الموجهة إليها أو مجموعات عناوين البريد الإلكتروني أو عناوين بريد إلكتروني محددة.

يمكن تعديل السياسات الافتراضية لتدفق البريد وتحديد سياسات جديدة لتدفق البريد.

هناك أربع سياسات افتراضية لتدفق البريد تم تعريفها على المستمعين العاميين:

- مقبول
- محصور
- خنق
- أئمتن

يستخدم المستمعون الخاصون سياسات تدفق البريد التالية:

- مقبول
- محصور
- مرحلن

معلومات ذات صلة

- [جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل