

وأ TCVoruse لوصو ةدعاق تناك اذا امم ققحتلا ESA ىلع لمعت REJECT

تايوتحمل

[قمدملا](#)

[قيساسالا تابلطتملا](#)

[تابلطتملا](#)

[الما لمعت REJECT وأ TCVoruse لوصولا ةدعاق تناك اذا امم ققحتلا](#)

[ةلكشملا](#)

[ببسملا](#)

[بلاق](#)

[دويقلاو قيساسالا تابلطتملا](#)

[ديربلا تالچس مادختساب ققحتلا](#)

[ةعقوتملا ةجيتنلا](#)

[قمزحلا طاقتملا مادختساب ققحتلا](#)

[ةعقوتملا ةجيتنلا](#)

[قلىص تاذ تامولعم](#)

[قنراقملا صخلم](#)

[صخلم](#)

ةمدملا

ينورتكلال ديربلا نامأ زاهج لوصو ةدعاق تناك اذا امم ققحتلا ةيفيك دنتسملا اذه حضوي
ضوفرملك مأ فدارملك لمعت Cisco (ESA) نم

قيساسالا تابلطتملا

تابلطتملا

- Cisco Email Security Appliance (ESA) ينورتكلال ديربلا نامأ ةزهجأ
- AsyncOS تارادصا عيجم

REJECT وأ TCVoruse لوصولا ةدعاق تناك اذا امم ققحتلا
الما لمعت

لوكونوربل ةباجتسا ضفرلا عجري . كولسلا ديكأتل ةمزح طاقنلا وأ ديربل تالچس مدختسا موقى . (MTA) ديعلال لئاسرلا لقن لماع ىلإ 5XX ب صاخلا (SMTP) طيسبل ديربل لقن ACK. و RST ةمزح لاسرا قيرط نع لاصتالا طبض ةداعإ CiscoPrefuse

ةلكشملا

لمعت روظملا ديربل قفدت جهن ىلإ لوصول ةدعاق تناك اذا ام دىحتل بولطم ديكأتل REJECT. أو TCPREFUSE

ببسل

روظملا ديربل قفدت جهن ب ةداع نانرتقملا لاصتالا كولس امه REJECT و CstOperationUse موقى . تباثلا دادترالا اضيأ ىمسي ،مالعإ عم دىعب فيضم نم لئاسرلا رطح ضفر لاصتالا طاقساب

زارق

هذه ققحتلا بيلاسا دحأ مادختسا:

- ل تالاخدا ىلع ديربل تالچس يوتحت . ةدعاقلا ليغشت نم دكأتل ديربل تالچس عجار لوظملا لاصتالا ليچست نيكم ت دنع طقف TCVoruse
- . ةمزحلا يوتسم ىلع ةثداحملا ةبقارمل ،tcpdump لثم ، لكونوربل للحم مدختسا

دويقلالو ةيساسال تابلطتملا

- . ديربل تالچس يف TCVoruse تالاخدا ليچستل Verbose لاصتالا ليچست نيكم ت بچي
- . ديربل لچس ةعجارم لدبتسي ال هنكلو ، ةكبشلا ةثداحم نم ةمزحلا طاقنلا ققحتي

ديربل تالچس مادختساب ققحتلا

- 1.(MTA) "دع نع لئاسرلا لقن لماع" نم لاصتالا ةلواحملا ديربل تالچس عجار
- 2.REJECT أو TCVericeUse ضرعي لچسلا لاخدا ناك اذا ام ديكأتب مق

ةعقوتملا ةجيتنلا

تالاخدالا رهظت ،TCVoruse ل ةبسنلاب . لوصول ةدعاق قيبطت ديربل لچس تالاخدا دكؤت انكمم لوظملا لاصتالا ليچست نوكي ام دنع طقف

ةمزحلا طاقنلا مادختساب ققحتلا

- 1.طيسبل لكونوربلاب ةصاخلا ةثداحملا طاقنلا لچأ نم tcpdump رمألا ليغشتب مق (SMTP) ديربل لئاسر لقنل
- 2.TCPREFUSE و ضفر ل عقوتملا كولسلاب ةجيتنلا نراقو ةمزحلا قفدت عجار

ةعقوتملا ةجيتنلا

قي رط نع لاصتال طبض ةداعإ CiscoPrefuse موقي. SMTP 5XX ةباجتسإ REJECT عجرت
ACK و RST ةمزح لاسرا

قلص تاذا تمامولعم

عجـار .



لجسي. لاسرالماظن إلى هتداع| تمت مئاد SMTP ضفريه قبلصلال عزفقا: عطحالم
ديربال تالجس في فة فاضا| لاصلتا لي صافت لوطمالم لاصلتال لي جست

ةنراقم لاصخلم

(MTA) دع ب نع لئاسرلا لقن لماعو ESA ني ب ةمزال قفدت ضفر

```

Remote MTA -----> SYN  

                      SYN, ACK  

ESA -----> Remote MTA  

                      ACK  

Remote MTA -----> ESA  

                      5XX Code  

ESA -----> Remote MTA  

                      FIN, ACK  

ESA -----> Remote MTA  

                      ACK  

Remote MTA -----> ESA  

                      FIN, ACK  

Remote MTA -----> ESA  

                      ACK  

ESA -----> Remote MTA
```

دې پل MTA و ESA نې CiscoPrefuse ؤ مزح قفدت

```

Remote MTA -----> SYN
                      SYN, ACK
ESA -----> Remote MTA
                      ACK
Remote MTA -----> ESA
                      RST, ACK
ESA -----> Remote MTA

```

صخلم

- لم عمل السجل قالغ او SMTP 5XX ة باج ت سا عا ج را : ض فر
- ACK و RST ة مزح ل اس را ق ي ر ط ن ع ل اص ت ال ا ط ب ض ة دا ع : TC Voruse

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا