

Como posso eu verificar que a regra do meu acesso TCPREFUSE ou de REJEIÇÃO está trabalhando?

Índice

[Como posso eu verificar que a regra do meu acesso TCPREFUSE ou de REJEIÇÃO está trabalhando?](#)

Como posso eu verificar que a regra do meu acesso TCPREFUSE ou de REJEIÇÃO está trabalhando?

Ambiente: Cisco envia por correio eletrônico a ferramenta de segurança (ESA), todas as versões de AsyncOS

TCPREFUSE e a REJEIÇÃO são os dois comportamentos da conexão que são associados normalmente com a política OBSTRUÍDA do fluxo de correio. Estas regras do acesso permitem que você escolha se obstruir mensagens de um host remoto com uma notificação (salto duro) ou deixar cair simplesmente a conexão. Veja [o que é a diferença entre a REJEIÇÃO e o TCPREFUSE?](#)

Se você gostaria de determinar se um host remoto está sendo deixado cair devido a TCPREFUSE ou a REJEIÇÃO, você pode ver entradas nos logs do correio. Os logs do correio conterão somente entradas para TCPREFUSE se o registro verboso da conexão é permitido. Adicionalmente você pode usar um analisador de protocolo, tal como o `tcpdump`, para monitorar as conversações a nível do pacote. Ao usar um analisador de protocolo, você observará conversações diferentes para TCPREFUSE contra a REJEIÇÃO.

O fluxo da conexão de TCP entre o ESA e o agente de transferência de mensagem remoto (MTA) para a conexão da rejeição é como este:

```

Remote MTA -----> ESA
                        SYN
ESA -----> Remote MTA
                        SYN, ACK
Remote MTA -----> ESA
                        ACK
Remote MTA -----> ESA
                        5XX Code
ESA -----> Remote MTA
                        FIN, ACK
Remote MTA -----> Remote MTA
                        ACK
Remote MTA -----> ESA
                        FIN, ACK
Remote MTA -----> ESA
                        ACK
```

ESA -----> Remote MTA

O fluxo da conexão de TCP entre o ESA e o MTA remoto para a conexão da recusa TCP é como este:

```

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