# Vérifier si une règle d'accès TCPREFUSE ou REJECT fonctionne sur un ESA

## Table des matières


Introduction

Conditions préalables

- Exigences

Vérifier si une règle d'accès TCPREFUSE ou REJECT fonctionne

- Problème
- Motif
- Résolution
- Conditions préalables et restrictions

Vérifier avec les journaux de messagerie

- Résultat attendu

Vérifier avec la capture de paquets

- Résultat attendu

Informations connexes

Récapitulatif de comparaison

Résumé


## Introduction

Ce document décrit comment vérifier si une règle d'accès du dispositif de sécurité de la messagerie Cisco (ESA) fonctionne en tant que TCPREFUSE ou REJECT.

## Conditions préalables

### Exigences

- Appliance de sécurisation de la messagerie Cisco (ESA)
- Toutes les versions d'AsyncOS

## Vérifier si une règle d'accès TCPREFUSE ou REJECT fonctionne

Utilisez les journaux de messagerie ou une capture de paquets pour confirmer le comportement.

REJECT renvoie une réponse SMTP (Simple Mail Transfer Protocol) 5XX au MTA (Message Transfer Agent) distant. TCPREFUSE réinitialise la connexion en envoyant un paquet RST, ACK.

### Problème

Une confirmation est requise pour déterminer si une règle d'accès de la stratégie de flux de messages BLOQUÉS fonctionne en tant que TCPREFUSE ou REJECT.

### Motif

TCPREFUSE et REJECT sont les deux comportements de connexion normalement associés à la stratégie de flux de messages BLOQUÉS. REJECT bloque les messages provenant d'un hôte distant avec une notification, également appelée rebondissement forcé. TCPREFUSE interrompt la connexion.

### Résolution

Utilisez l'une des méthodes de vérification suivantes :

- Vérifiez les journaux de messagerie pour confirmer que la règle a été déclenchée. Les journaux de messagerie contiennent des entrées pour TCPREFUSE uniquement lorsque la consignation détaillée des connexions est activée.
- Utilisez un analyseur de protocole, tel que tcpdump, pour surveiller la conversation au niveau du paquet.

### Conditions préalables et restrictions

- La journalisation des connexions détaillées doit être activée pour enregistrer les entrées TCPREFUSE dans les journaux de messagerie.
- La capture de paquets vérifie la conversation réseau, mais elle ne remplace pas la vérification du journal des messages.

## Vérifier avec les journaux de messagerie

1. Vérifiez les journaux de messagerie pour la tentative de connexion de l'agent de transfert de messages (MTA) distant.
2. Vérifiez si l'entrée de journal affiche TCPREFUSE ou REJECT.

### Résultat attendu

Les entrées du journal de messagerie confirment que la règle d'accès a été appliquée. Pour TCPREFUSE, les entrées apparaissent uniquement lorsque la consignation détaillée des connexions est activée.

## Vérifier avec la capture de paquets

1. Exécutez la commande tcpdump afin de capturer la conversation SMTP (Simple Mail Transfer Protocol).
2. Examinez le flux de paquets et comparez le résultat avec le comportement attendu pour REJECT et TCPREFUSE.

### Résultat attendu

REJECT renvoie une réponse SMTP 5XX. TCPREFUSE réinitialise la connexion en envoyant un paquet RST, ACK.

## Informations connexes

Reportez-vous à .

---



Remarque : Un renvoi ferme est un rejet SMTP permanent renvoyé au système émetteur. La consignation détaillée des connexions enregistre des détails de connexion supplémentaires dans les journaux de messagerie.

---

## Récapitulatif de comparaison

REJETER le flux de paquets entre l'ESA et l'agent de transfert de messages (MTA) distant :

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

TCPREFUSE flux de paquets entre l'ESA et le MTA distant :

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

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

# Résumé

- REJETER : Retourne une réponse SMTP 5XX et ferme la session.
- TCPREFUSE : Réinitialise la connexion en envoyant un paquet RST, ACK.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.