

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Protocoles IP nécessaires pour expédier par un Pare-feu](#)

[Ports UDP/TCP nécessaires pour expédier par un Pare-feu](#)

[Informations connexes](#)

Introduction

La transmission du trafic VPN par un Pare-feu dépend quel logiciel client de systèmes compatibles IntraPort vous utilisez, de quel type transformé sont spécifiés, et/ou le type de tunnel entre réseaux locaux qui est utilisé. Des protocoles IP et les ports TCP/UDP doivent être ouverts dans le Pare-feu.

Remarque: Tous les Routeurs de Cisco doivent avoir un système d'exploitation de version 11.3 ou ultérieures afin de conduire le trafic d'IPsec. Les versions antérieures ne conduisent pas des protocoles IPsecs.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Protocoles IP nécessaires pour expédier par un Pare-feu

Les protocoles IP nécessaires pour expédier par un Pare-feu sont :

- **47 GRE (le Général Router Encapsulation) ?** Ceci affecte tous les tunnels entre réseaux locaux d'ÉTAPE sans authentification ou cryptage. Ce type de tunnel entre réseaux locaux est compatible avec des tunnels de non-IPsec offerts dans des Routeurs de Cisco.
- **L'ESP 50 (encapsulant la charge utile de Sécurité) ?** Tous les clients de l'IKE 3.x si le cryptage est spécifié dans le groupe transformé. Tous les clients 2.x si le cryptage est spécifié au groupe VPN. tunnels entre réseaux locaux d'ÉTAPE de systèmes compatibles de support de clients du MAC 3.x et 2.x seulement EN PARTICULIER avec le cryptage et aucune authentification. En outre, les tunnels entre réseaux locaux d'IKE où le cryptage est spécifié dans le groupe transformé.
- **51 OH (en-tête d'authentification) ?** Tous les clients 3.x excepté le MAC avec l'authentification spécifiée dans le groupe transformé. Tous les clients 2.x excepté le MAC avec l'authentification spécifiée dans le groupe. Tunnels d'ÉTAPE d'entre réseaux locaux avec l'authentification. En outre, les tunnels entre réseaux locaux d'IKE où l'authentification est spécifiée dans le groupe transformé.

Ports UDP/TCP nécessaires pour expédier par un Pare-feu

Les ports UDP/TCP nécessaires pour expédier par un Pare-feu sont :

- **ISAKMP de l'UDP 500 (protocole de gestion de clés d'association de sécurité internet) ?** Les tunnels de tout le d'IKE IKE de clients et d'entre réseaux locaux exigent du port UDP 500 et de leur protocole respectif d'établir un tunnel. Les protocoles IP répertoriés dans ce document doivent également être considérés. Si le trafic d'IntraPort traverse un Pare-feu, alors il doit permettre les mêmes ports pour les types de clients qui tentent de se connecter à lui.
- **TCP 80 (HTTP) ?** Le port TCP 80 est exigé pour initier la transmission entre le client d'IntraPort et le serveur d'IntraPort si NAT (traduction d'adresses réseau) est utilisé n'importe où le long du chemin entre les deux.**Remarque:** C'est approprié seulement pour la version 5.1 ou ultérieures de logiciel de serveur d'IntraPort, et la version du client 3.3.0 d'IntraPort ou plus tard.

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)