Configuration du mode transparent NAT pour IPSec sur le concentrateur VPN 3000

Contenu

Introduction

La traduction d'adresses de réseau (NAT) a été créée pour aborder le problème de la quatrième version d'Internet Protocol (IPV4), qui s'exécute hors de l'espace d'adressage. De nos jours, les réseaux domiciliaires privés et ceux des petites entreprises utilisent la NAT au lieu d'acheter des adresses enregistrées. Les plus grandes entreprises mettent en place la NAT seule ou accompagnée d'un pare-feu afin de protéger leurs ressources internes.

Plusieurs à un, la solution NAT la plus couramment implémentée, mappe plusieurs adresses privées à une seule adresse routable (publique) ; c'est également ce que l'on appelle la traduction d'adresses de port (PAT). L'association est mise en oeuvre au niveau des ports. La solution PAT crée un problème pour le trafic IPSec qui n'utilise aucun port.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur Cisco VPN 3000
- Client VPN Cisco 3000 version 2.1.3 et ultérieure

- Client et concentrateur Cisco VPN 3000 version 3.6.1 et ultérieure pour NAT-T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Encapsulation des données utiles de sécurité

Le protocole 50 (Encapsulating Security Payload [ESP]) gère les paquets cryptés/encapsulés d'IPSec. La plupart des périphériques PAT ne fonctionnent pas avec ESP car ils ont été programmés pour fonctionner uniquement avec le protocole TCP (Transmission Control Protocol), le protocole UDP (User Datagram Protocol) et le protocole ICMP (Internet Control Message Protocol). En outre, les périphériques PAT ne peuvent pas mapper plusieurs index de paramètres de sécurité (SPI). Le mode transparent NAT du client VPN 3000 résout ce problème en encapsulant ESP dans UDP et en l'envoyant à un port négocié. Le nom de l'attribut à activer sur le concentrateur VPN 3000 est IPSec via NAT.

Un nouveau protocole NAT-T qui est une norme IETF (toujours à l'étape PROJET au moment de la rédaction de cet article) encapsule également les paquets IPSec dans UDP, mais il fonctionne sur le port 4500. Ce port n'est pas configurable.

Comment fonctionne le mode transparent NAT ?

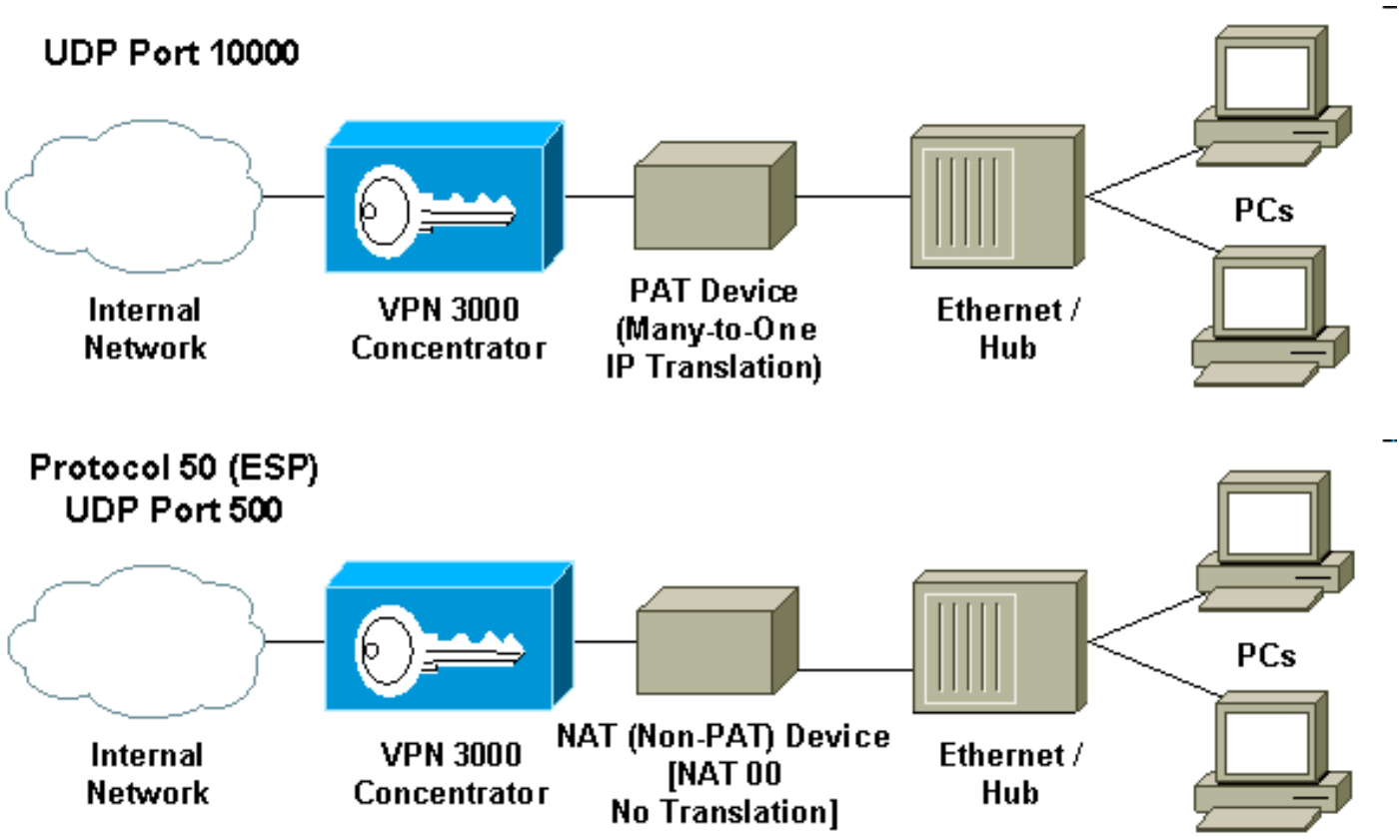
L'activation du mode transparent IPSec sur le concentrateur VPN crée des règles de filtre non visibles et les applique au filtre public. Le numéro de port configuré est ensuite transmis au client VPN de manière transparente lorsque le client VPN se connecte. Du côté entrant, le trafic entrant UDP de ce port passe directement à IPSec pour traitement. Le trafic est déchiffré et décapsulé, puis routé normalement. Sur le côté sortant, IPSec chiffre, encapsule et applique un en-tête UDP (si configuré). Les règles de filtre d'exécution sont désactivées et supprimées du filtre approprié dans trois conditions : quand IPSec sur UDP est désactivé pour un groupe, quand le groupe est supprimé ou quand le dernier IPSec actif sur UDP SA sur ce port est supprimé. Des messages de test d'activité sont envoyés pour empêcher un périphérique NAT de fermer le mappage de port en raison de son inactivité.

Si IPSec sur NAT-T est activé sur le concentrateur VPN, le concentrateur VPN/client VPN utilise le mode NAT-T d'encapsulation UDP. NAT-T fonctionne en détectant automatiquement tout périphérique NAT entre le client VPN et le concentrateur VPN lors de la négociation IKE. Vous devez vous assurer que le port UDP 4500 n'est pas bloqué entre le concentrateur VPN/client VPN pour que NAT-T fonctionne. En outre, si vous utilisez une configuration IPSec/UDP précédente qui utilise déjà ce port, vous devez reconfigurer cette configuration IPSec/UDP précédente pour utiliser un port UDP différent. Puisque NAT-T est un brouillon IETF, il est utile lors de l'utilisation de périphériques multifournisseurs si l'autre fournisseur implémente cette norme.

NAT-T fonctionne à la fois avec les connexions client VPN et les connexions LAN à LAN, contrairement à IPSec sur UDP/TCP. En outre, les routeurs Cisco IOS® et les pare-feu PIX prennent en charge NAT-T.

Il n'est pas nécessaire d'activer IPSec sur UDP pour que NAT-T fonctionne.

Configuration du mode transparent NAT



Suivez la procédure suivante pour configurer le mode transparent NAT sur le concentrateur VPN.

Remarque : IPSec sur UDP est configuré par groupe, tandis qu'IPSec sur TCP/NAT-T est configuré globalement.

1. Configurez IPSec sur UDP :Sur le concentrateur VPN, sélectionnez **Configuration > User Management > Groups**.Pour ajouter un groupe, sélectionnez **Ajouter**. Pour modifier un groupe existant, sélectionnez-le et cliquez sur **Modifier**.Cliquez sur l'onglet IPSec, vérifiez **IPSec via NAT** et configurez l'**IPSec via NAT UDP Port**. Le port par défaut pour IPSec via NAT est 10000 (source et destination), mais ce paramètre peut être modifié.
2. Configurez IPSec sur NAT-T et/ou IPSec sur TCP :Sur le concentrateur VPN, sélectionnez Configuration > **System > Tunneling Protocols > IPSec > NAT Transparency**.Cochez la case **IPSec sur NAT-T et/ou TCP**.

Si tout est activé, utilisez cette priorité :

1. IPSec sur TCP.
2. IPSec sur NAT-T.
3. IPSec sur UDP.

Configuration du client VPN Cisco pour utiliser la transparence NAT

Pour utiliser IPSec sur UDP ou NAT-T, vous devez activer IPSec sur UDP sur Cisco VPN Client 3.6 et versions ultérieures. Le port UDP est attribué par le concentrateur VPN en cas d'IPSec sur

UDP, tandis que pour NAT-T il est fixé au port UDP 4500.

Pour utiliser IPSec sur TCP, vous devez l'activer sur le client VPN et configurer le port qui doit être utilisé manuellement.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support technique - Cisco Systems