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

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Encapsuler la charge utile de Sécurité
Comment le mode transparent NAT fonctionne-t-il ?
Configurez le mode transparent NAT
Configuration de Client VPN Cisco pour utiliser la transparence NAT
Informations connexes

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.

Beaucoup-à-un, la solution NAT le plus généralement mise en application, trace plusieurs adresses privées à une adresse routable simple (de public) ; ceci est également connu comme translation d'adresses d'adresse du port (PAT). L'association est mise en application au niveau de port. La solution de PAT crée un problème pour le trafic d'IPSec qui n'utilise aucun port.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Concentrateur Cisco VPN 3000
- Version 2.1.3 et ultérieures de Cisco VPN 3000 Client

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Encapsuler la charge utile de Sécurité

Protocol 50 (encapsulant charge utile de Sécurité [ESP]) manipule chiffré/paquets encapsulés d'IPSec. La plupart des périphériques de PAT ne fonctionnent pas avec l'ESP puisqu'ils ont été programmés pour fonctionner seulement 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 de PAT ne peuvent pas tracer les plusieurs index de paramètre de Sécurité (SPI). Le mode transparent NAT dans le client VPN 3000 résout ce problème en encapsulant l'ESP dans l'UDP et en l'envoyant à un port négocié. Le nom de l'attribut à lancer sur le concentrateur VPN 3000 est IPSec par NAT.

Un nouveau protocole NAT-T qui est une norme IETF (toujours dans l'étape d'ÉBAUCHE en date de l'écriture cet article) également encapsule des paquets d'IPSec dans l'UDP, mais lui travaille au port 4500. Ce port n'est pas configurable.

Comment le mode transparent NAT fonctionne-t-il ?

Le mode transparent de lancement d'IPSec sur le concentrateur VPN crée des règles de filtrage non-visibles et les applique au filtre public. Le numéro de port configuré est alors passé au client vpn d'une manière transparente quand le client vpn se connecte. Du côté d'arrivée, le trafic d'arrivée d'UDP de ce port passe directement à IPSec pour le traitement. Le trafic est déchiffré et désencapsulé, et puis conduit normalement. Du côté sortant, IPSec chiffre, encapsule et puis applique une en-tête d'UDP (si ainsi configuré). Les règles de filtrage d'exécution sont désactivées et supprimées du filtre approprié dans trois conditions : quand IPSec au-dessus d'UDP est désactivé pour un groupe, quand le groupe est supprimé, ou quand le dernier IPSec actif au-dessus d'UDP SA sur ce port est supprimé. Le Keepalives est envoyé pour empêcher un périphérique NAT de fermer le mappage de ports dû à l'inactivité.

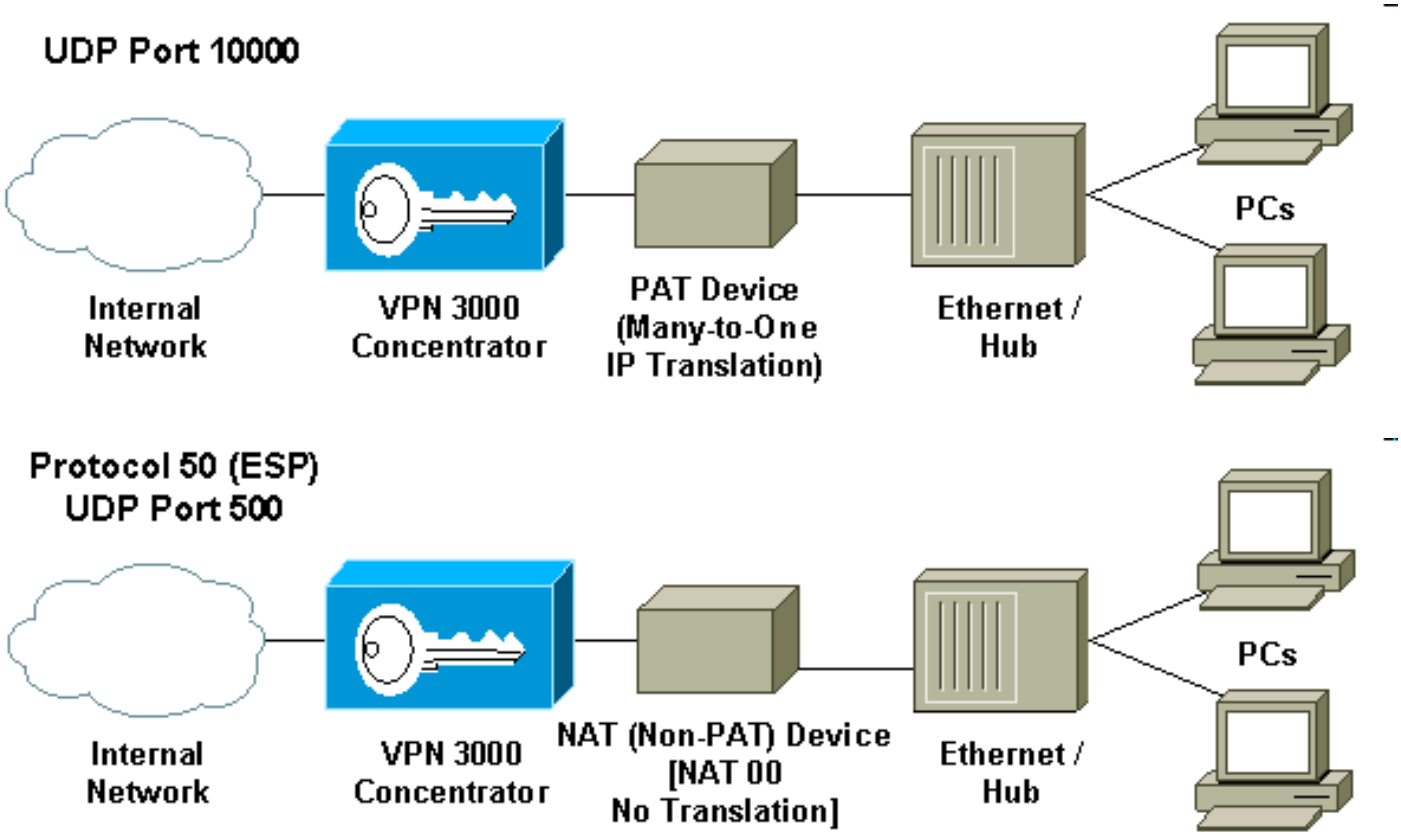
Si IPSec au-dessus de NAT-T est activé sur le concentrateur VPN, alors le client VPN Concentrator/VPN utilise le mode NAT-T de l'encapsulation d'UDP. NAT-T fonctionne à côté de à autodétection n'importe quel périphérique NAT entre le client vpn et le concentrateur VPN pendant la négociation d'IKE. Vous devez s'assurer que le port UDP 4500 n'est pas bloqué entre le client VPN Concentrator/VPN pour que NAT-T fonctionne. En outre, si vous utilisez une configuration précédente IPSec/UDP qui utilise déjà ce port, vous devez modifier cette configuration plus tôt IPSec/UDP pour utiliser un port UDP différent. Puisque NAT-T est un projet soumis à l'IETF, il aide à l'aide des périphériques pluri-constructeurs si l'autre constructeur implémente cette norme.

NAT-T fonctionne avec les connexions client VPN et les connexions entre réseaux locaux IPSec différent au-dessus d'UDP/TCP. En outre, les Routeurs de Cisco IOS® et les périphériques de

Pare-feu PIX prennent en charge NAT-T.

Vous n'avez pas besoin d'IPSec au-dessus d'UDP pour être activé avoir le fonctionnement NAT-T.

Configurez le mode transparent NAT



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

Remarque: IPSec au-dessus d'UDP est configuré sur a par base de groupe, alors qu'IPSec au-dessus de TCP/NAT-T est configuré globalement.

1. Configurez IPSec au-dessus d'UDP :Sur le concentrateur VPN, **Configuration > User Management > Groups** choisi.Pour ajouter un groupe, choisi **ajoutent**. Pour modifier un groupe existant, sélectionner lui et le clic **modifiez**.Cliquez sur l'onglet d'IPSec, vérifiez **IPSec par NAT** et configurez l'**IPSec par le port UDP NAT**. Le port par défaut pour IPSec par NAT est 10000 (source et destination), mais cette configuration peut être changée.
2. Configurez IPSec au-dessus de NAT-T et/ou IPSec au-dessus de TCP :Sur la **configuration de** concentrateur VPN > le **système** > les **protocoles** > l'**IPSec** choisis de **Tunnellisation > transparence NAT**.Cochez l'**IPSec au-dessus de la** case **NAT-T et/ou de TCP**.

Si tout est activé, utilisez cette priorité :

1. IPSec au-dessus de TCP.
2. IPSec au-dessus de NAT-T.
3. IPSec au-dessus d'UDP.

Configuration de Client VPN Cisco pour utiliser la transparence NAT

Pour utiliser IPSec au-dessus d'UDP ou de NAT-T que vous devez activer IPSec au-dessus d'UDP sur le Client VPN Cisco 3.6 et plus tard. Le port UDP est assigné par le concentrateur VPN en cas d'IPSec au-dessus d'UDP, alors que pour NAT-T il est réparé au port UDP 4500.

Pour utiliser IPSec au-dessus de TCP, vous devez l'activer sur le client vpn et configurer le port qui devrait 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