Konfigurieren des transparenten NAT-Modus für IPSec auf dem VPN 3000-Konzentrator

Inhalt

Einführung

Network Address Translation (NAT) wurde entwickelt, um dem Problem zu begegnen, dass der Adressbereich von Internet Protocol Version 4 (IPV4) ausgeht. Heute nutzen Heimbenutzer und kleine Büronetzwerke NAT als Alternative zum Kauf registrierter Adressen. Unternehmen implementieren NAT allein oder mit einer Firewall, um ihre internen Ressourcen zu schützen.

Many-to-One, die am häufigsten implementierte NAT-Lösung, ordnet mehrere private Adressen einer einzigen routbaren (öffentlichen) Adresse zu. Dies wird auch als Port Address Translation (PAT) bezeichnet. Die Zuordnung wird auf Port-Ebene implementiert. Die PAT-Lösung schafft ein Problem für IPSec-Datenverkehr, der keine Ports verwendet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN 3000 Concentrator
- Cisco VPN 3000 Client Version 2.1.3 und höher
- Cisco VPN 3000 Client und Concentrator Version 3.6.1 und höher für NAT-T

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Kapselung der Security-Payload

Protokoll 50 (Encapsulating Security Payload [ESP]) behandelt die verschlüsselten/gekapselten Pakete von IPSec. Die meisten PAT-Geräte arbeiten nicht mit ESP, da sie so programmiert sind, dass sie nur mit Transmission Control Protocol (TCP), User Datagram Protocol (UDP) und Internet Control Message Protocol (ICMP) funktionieren. Darüber hinaus können PAT-Geräte nicht mehrere Security Parameter Indixes (SPIs) zuordnen. Der transparente NAT-Modus im VPN 3000-Client löst dieses Problem, indem ESP in UDP gekapselt und an einen ausgehandelten Port gesendet wird. Der Name des Attributs, das im VPN 3000 Concentrator aktiviert werden soll, lautet IPSec through NAT.

Ein neues Protokoll NAT-T, das ein IETF-Standard ist (sich zum Zeitpunkt der Erstellung dieses Artikels noch in der DRAFT-Phase befindet), kapselt auch IPSec-Pakete in UDP, funktioniert aber auf Port 4500. Dieser Port ist nicht konfigurierbar.

Wie funktioniert der transparente NAT-Modus?

Durch Aktivieren des transparenten IPSec-Modus im VPN Concentrator werden nicht sichtbare Filterregeln erstellt und auf den öffentlichen Filter angewendet. Die konfigurierte Portnummer wird dann transparent an den VPN-Client weitergeleitet, wenn der VPN-Client eine Verbindung herstellt. Auf der Eingangsseite wird der von diesem Port eingehende UDP-Datenverkehr zur Verarbeitung direkt an IPSec weitergeleitet. Der Datenverkehr wird entschlüsselt, entkapselt und anschließend normal weitergeleitet. Auf der ausgehenden Seite verschlüsselt IPSec den UDP-Header, kapselt ihn und wendet ihn an (sofern konfiguriert). Die Laufzeitfilterregeln werden unter drei Bedingungen deaktiviert und aus dem entsprechenden Filter gelöscht: wenn IPSec über UDP für eine Gruppe deaktiviert ist, wenn die Gruppe gelöscht wird oder der letzte aktive IPSec über UDP SA an diesem Port gelöscht wird. Keepalives werden gesendet, um zu verhindern, dass ein NAT-Gerät die Port-Zuordnung aufgrund von Inaktivität schließt.

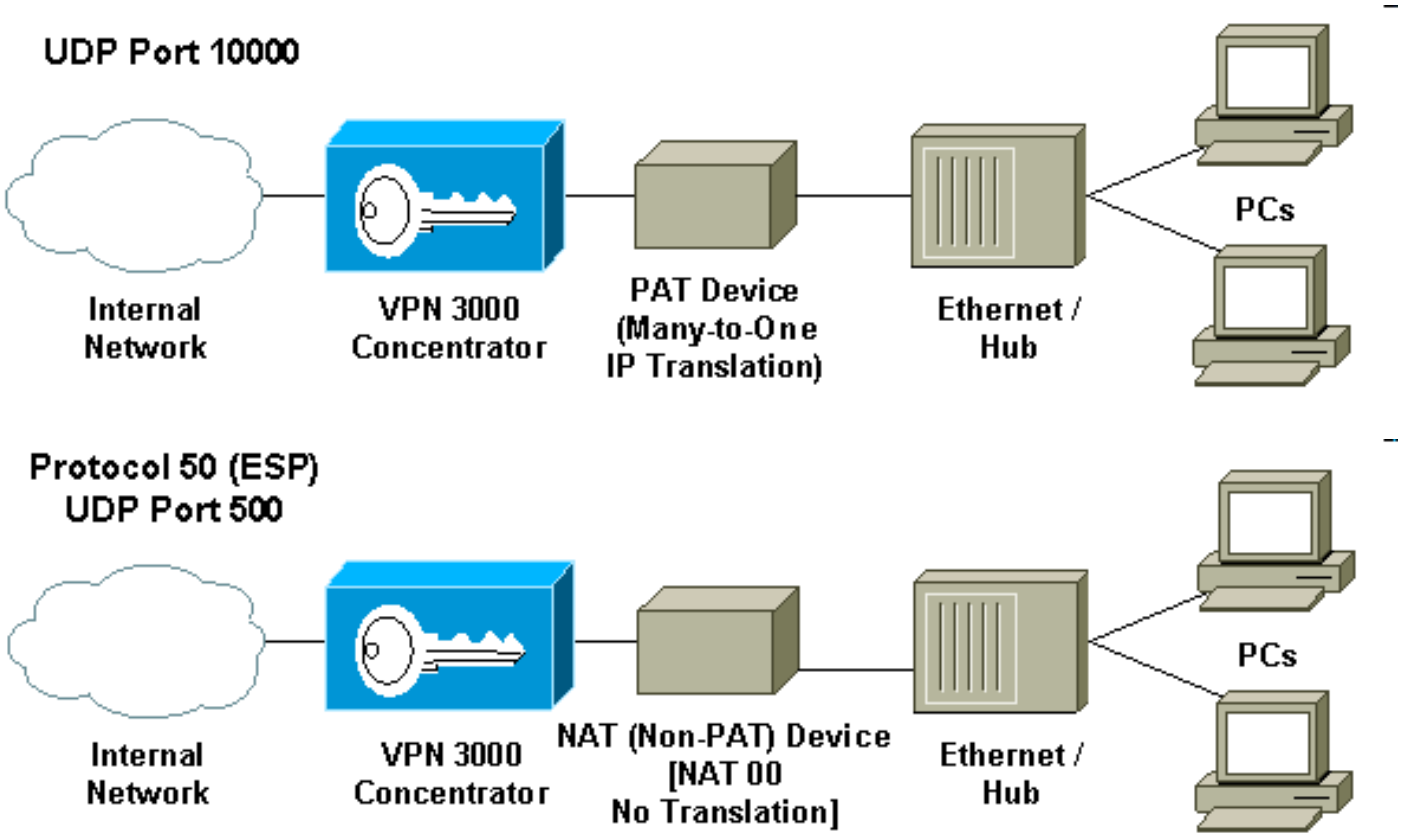
Wenn IPSec over NAT-T auf dem VPN Concentrator aktiviert ist, verwendet der VPN Concentrator/VPN Client den NAT-T-Modus der UDP-Kapselung. NAT-T erkennt während der IKE-Aushandlung automatisch jedes NAT-Gerät zwischen dem VPN-Client und dem VPN-Concentrator. Sie müssen sicherstellen, dass der UDP-Port 4500 nicht zwischen dem VPN-Konzentrator/VPN-Client blockiert wird, damit NAT-T funktioniert. Wenn Sie eine ältere IPSec/UDP-Konfiguration verwenden, die diesen Port bereits verwendet, müssen Sie diese frühere IPSec/UDP-Konfiguration neu konfigurieren, um einen anderen UDP-Port zu verwenden. Da NAT-T ein IETF-Entwurf ist, ist es bei der Verwendung von Geräten verschiedener Hersteller hilfreich, wenn der andere Anbieter diesen Standard implementiert.

NAT-T arbeitet sowohl mit VPN-Client-Verbindungen als auch mit LAN-zu-LAN-Verbindungen

zusammen, im Gegensatz zu IPSec über UDP/TCP. Darüber hinaus unterstützen die Cisco IOS® Router und die PIX-Firewall-Geräte NAT-T.

Damit NAT-T funktioniert, muss IPSec über UDP nicht aktiviert sein.

Konfigurieren des transparenten NAT-Modus



Gehen Sie folgendermaßen vor, um den NAT-transparenten Modus auf dem VPN-Concentrator zu konfigurieren.

Hinweis: IPSec über UDP wird auf Gruppenbasis konfiguriert, während IPSec über TCP/NAT-T global konfiguriert wird.

1. Konfigurieren von IPSec über UDP:Wählen Sie im VPN-Konzentrator **Konfiguration > Benutzerverwaltung > Gruppen aus**.Um eine Gruppe hinzuzufügen, wählen Sie **Hinzufügen aus**. Um eine vorhandene Gruppe zu ändern, wählen Sie sie aus, und klicken Sie auf **Ändern**.Klicken Sie auf die Registerkarte IPSec, aktivieren Sie **IPSec über NAT**, und konfigurieren Sie **IPSec über NAT UDP Port**. Der Standard-Port für IPSec durch NAT ist 10.000 (Quelle und Ziel). Diese Einstellung kann jedoch geändert werden.
2. Konfigurieren Sie IPSec über NAT-T und/oder IPSec über TCP:Wählen Sie im VPN Concentrator die Option **Configuration > System > Tunneling Protocols > IPSec > NAT Transparency aus.**Aktivieren Sie das Kontrollkästchen **IPSec over NAT-T und/oder TCP**.

Wenn alles aktiviert ist, verwenden Sie die folgende Rangfolge:

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

Cisco VPN-Client-Konfiguration für NAT-Transparenz

Um IPSec über UDP oder NAT-T zu verwenden, müssen Sie IPSec über UDP auf Cisco VPN Client 3.6 und höher aktivieren. Der UDP-Port wird im Fall von IPSec über UDP vom VPN Concentrator zugewiesen, während für NAT-T der Port 4500 fest im UDP-Port ist.

Um IPSec über TCP zu verwenden, müssen Sie es auf dem VPN-Client aktivieren und den Port konfigurieren, der manuell verwendet werden soll.

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- Cisco VPN Client Support-Seite der Serie 3000
- IPSec-Support-Seite
- Technischer Support - Cisco Systems