NAT transparante modus configureren voor IPSec op de VPN-concentratie 3000

Inhoud

Inleiding

Network Address Translation (NAT) is ontwikkeld om het probleem van Internet Protocol, versie 4 (IPV4), waarvoor de adresruimte niet meer beschikbaar is, aan te pakken. Vandaag de dag gebruiken thuisgebruikers en kleine kantoornetwerken NAT als alternatief voor het kopen van geregistreerde adressen. Bedrijven implementeren NAT alleen of met een firewall om hun interne bronnen te beschermen.

Velen-op-één, de meest geïmplementeerde NAT-oplossing, zet verschillende privé-adressen in één routeerbaar (openbaar) adres in kaart. Dit wordt ook wel PAT (Port Address Translation) genoemd. De vereniging wordt op havenniveau ten uitvoer gelegd. De PAT-oplossing creëert een probleem voor IPSec-verkeer dat geen poorten gebruikt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VPN 3000 Concentrator
- Cisco VPN 3000 clientrelease 2.1.3 en hoger
- Cisco VPN 3000 Client en Concentrator release 3.6.1 en hoger voor NAT-T

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Inkapselende security payload

Protocol 50 (Encrypt Security Payload [ESP]) behandelt de versleutelde/ingekapselde pakketten van IPSec. De meeste PAT-apparaten werken niet met ESP omdat ze zijn geprogrammeerd om alleen te werken met Transmission Control Protocol (TCP), User Datagram Protocol (UDP) en Internet Control Message Protocol (ICMP). Daarnaast zijn PAT-apparaten niet in staat om meerdere security parameter-indexen (SPI's) in kaart te brengen. De transparante NAT-modus in de VPN 3000-client lost dit probleem op door ESP in UDP te integreren en het naar een onderhandeld-poort te sturen. De naam van de eigenschap om op de VPN 3000 Concentrator te activeren is IPSec door NAT.

Een nieuw protocol NAT-T dat een IETF-standaard is (nog steeds in de ontwerpfase vanaf het schrijven van dit artikel) kapselt ook IPSec-pakketten in UDP in, maar het werkt op poort 4500. Die poort is niet aanpasbaar.

Hoe werkt NAT transparante modus?

Wanneer u IPSec transparante modus op de VPN-centrator activeert, creëert u niet-zichtbare filterregels en past u deze toe op het openbare filter. Het geconfigureerde poortnummer wordt vervolgens op transparante wijze aan de VPN-client doorgegeven wanneer de VPN-client is verbonden. Aan de inkomende kant, gaat het inkomende verkeer van UDP van die haven rechtstreeks naar IPSec voor verwerking. Het verkeer wordt gedecrypteerd en gedecapsuleerd, en dan normaal routeerd. Aan de buitenkant, versleutelt IPSec, kapselt het in en past het vervolgens een UDP-header (indien zo geconfigureerd) toe. De run-filterregels worden onder drie omstandigheden gedeactiveerd en uit het filter verwijderd: wanneer IPSec over UDP voor een groep wordt uitgeschakeld, wanneer de groep wordt verwijderd, of wanneer de laatste actieve IPSec over UDP SA op die poort wordt verwijderd. Keepalives worden verstuurd om te voorkomen dat een NAT-apparaat de poortmapping sluit vanwege inactiviteit.

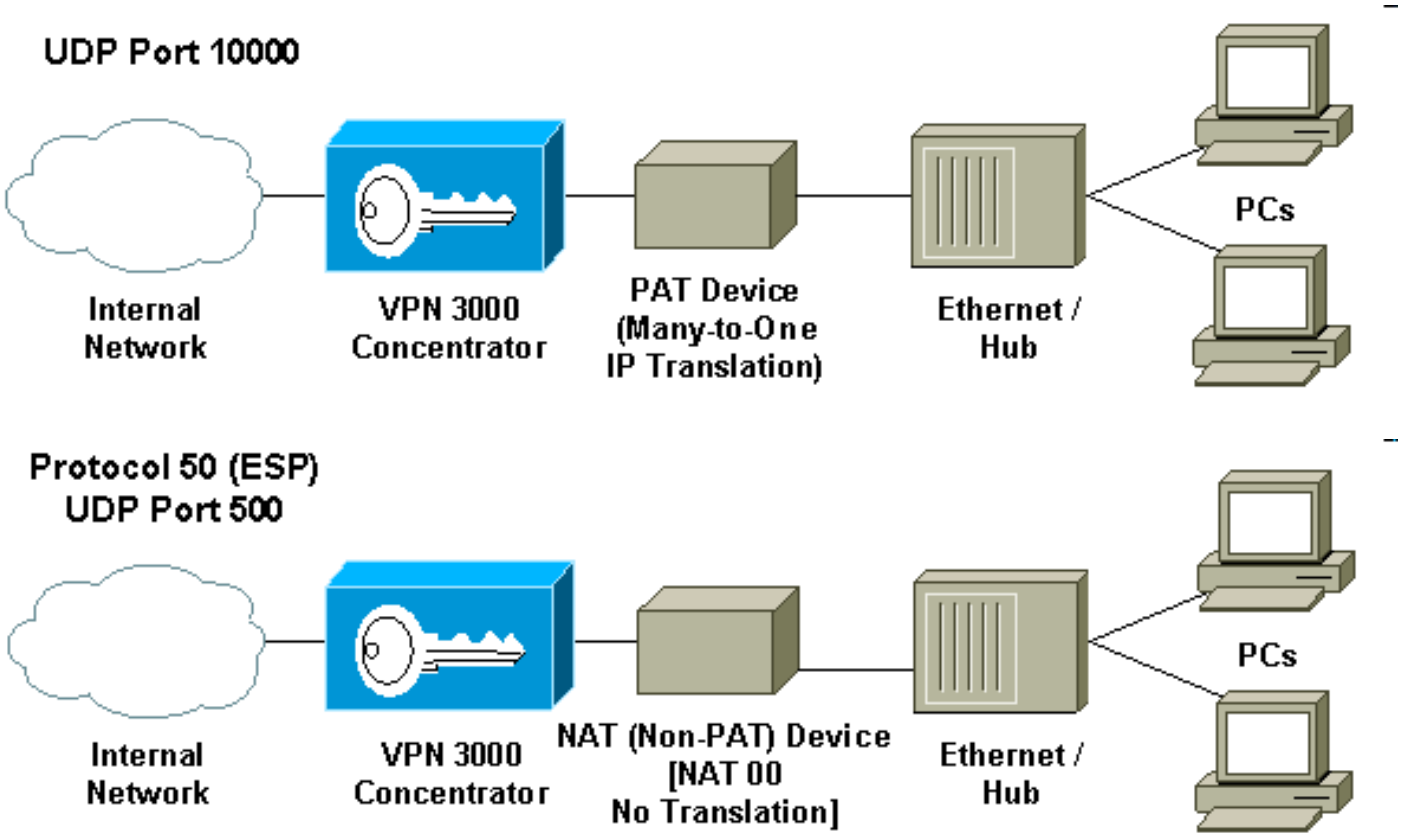
Als IPSec over NAT-T op de VPN-Concentrator is ingeschakeld, gebruikt de VPN-Concentrator/VPN-client NAT-T-modus van UDP-insluiting. NAT-T werkt door tijdens IKE-onderhandeling automatisch een NAT-apparaat te detecteren tussen de VPN-client en VPN-Concentrator. U moet ervoor zorgen dat UDP-poort 4500 niet geblokkeerd is tussen de VPN-centrator/VPN-client voor NAT-T om te kunnen werken. Als u een vorige IPSec/UDP-configuratie gebruikt die al die poort gebruikt, moet u die eerdere IPSec/UDP-configuratie opnieuw configureren om een andere UDP-poort te gebruiken. Aangezien NAT-T een IETF-concept is, helpt het bij het gebruik van multi-mode-apparaten als de andere verkoper deze standaard toepast.

NAT-T werkt met zowel VPN-clientverbindingen als LAN-to-LAN verbindingen in tegenstelling tot

IPSec over UDP/TCP. Tevens ondersteunen Cisco IOS® routers en de PIX-firewallapparaten NAT-T.

U hoeft IPSec niet over UDP niet in te schakelen om NAT-T te laten werken.

NAT transparante modus configureren



Gebruik de volgende procedure om NAT transparante modus op de VPN-centrator te configureren.

Opmerking: IPSec over UDP wordt geconfigureerd op groepsbasis, terwijl IPSec over TCP/NAT-T mondiaal wordt geconfigureerd.

1. Configuratie IPSec via UDP:Selecteer in VPN Concentrator de optie **Configuratie > Gebruikersbeheer > Groepen**.Als u een groep wilt toevoegen, selecteert u **Toevoegen**. Als u een bestaande groep wilt wijzigen, selecteert u deze en klikt u op **Wijzigen**.Klik op het tabblad IPSec, controleer **IPSec via NAT** en stel de **IPSec** vast **via NAT UDP-poort**. De standaardpoort voor IPSec door NAT is 10000 (bron en bestemming), maar deze instelling kan worden gewijzigd.
2. Configuratie IPSec over NAT-T en/of IPSec over TCP:Selecteer in VPN Concentrator **Configuration > System > Tunneling-protocollen > IPSec > NAT Transparency.**Controleer **IPSec over NAT-T en/of TCP-**selectieteken.

Als alles is geactiveerd, gebruik dan deze prioriteit:

1. IPsec over TCP.
2. IPsec over NAT-T.
3. IPsec over UDP.

Cisco VPN-clientconfiguratie voor gebruik van NAT-transparantie

Om IPSec over UDP of NAT-T te gebruiken moet u IPSec over UDP op Cisco VPN-client 3.6 en hoger inschakelen. De UDP-poort wordt toegewezen door de VPN-Concentrator in het geval van IPSec over UDP, terwijl het voor NAT-T is gekoppeld aan UDP-poort 4500.

Om IPSec over TCP te gebruiken, moet u het op de client van VPN inschakelen en de poort configureren die handmatig moet worden gebruikt.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- Cisco VPN 3000 Series clientondersteuningspagina
- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen