تكوين الوضع الشفاف ل NAT ل IPSec على مركز VPN 3000

المحتويات

المقدمة

تم تطوير ترجمة عنوان الشبكة (NAT) لمعالجة مشكلة نفاد مساحة العنوان الخاصة ببروتوكول الإنترنت الإصدار 4 (IPv4). اليوم، يستخدم مستخدمو المنازل وشبكات المكاتب الصغيرة NAT كبديل لشراء العناوين المسجلة. تطبق الشركات NAT بمفردها أو باستخدام جدار حماية لحماية مواردها الداخلية.

multi-to-one، الأكثر تطبيقا nat حل، يخطط عدة عنوان خاص إلى واحد مسحاج تخديد (عام) عنوان، هذا يعرف أيضا ب ترجمة عنوان أيسر (ضرب). يتم تنفيذ الاقتران على مستوى المنفذ. ال ضرب يخلق حل مشكلة ل IPSec حركة مرور أن لا يستعمل أي ميناء.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مركز Cisco VPN 3000
- Cisco VPN 3000 Client الإصدار 2.1.3 والإصدارات الأحدث
- الإصدار 3.6.1 من Cisco VPN 3000 Client and Concentrator والإصدارات الأحدث ل NAT-T

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

حمولة أمان التضمين

يعالج البروتوكول 50 (تضمين حمولة الأمان [ESP]) الحزم المشفرة/المغلفة من IPSec. لا تعمل معظم أجهزة PAT مع ESP لأنه قد تم برمجتها للعمل فقط مع بروتوكول التحكم في الإرسال (TCP)، وبروتوكول مخطط بيانات المستخدم (UDP)، وبروتوكول رسائل التحكم في الإنترنت (ICMP). بالإضافة إلى ذلك، يتعذر على أجهزة PAT تعيين فهارس معلمات أمان متعددة (SPIs). يحل وضع NAT الشفاف في عميل VPN 3000 هذه المشكلة عن طريق تضمين ESP داخل UDP وإرساله إلى منفذ تم التفاوض عليه. اسم السمة التي سيتم تنشيطها على مركز VPN 3000 هو IPSec من خلال NAT.

كذلك، فإن بروتوكول NAT-T جديد هو معيار IETF (لا يزال في مرحلة المسودة منذ كتابة هذه المقالة) يغلف حزم IPSec في UDP، ولكنه يعمل على المنفذ 4500. هذا المنفذ غير قابل للتكوين.

كيف يعمل وضع NAT الشفاف؟

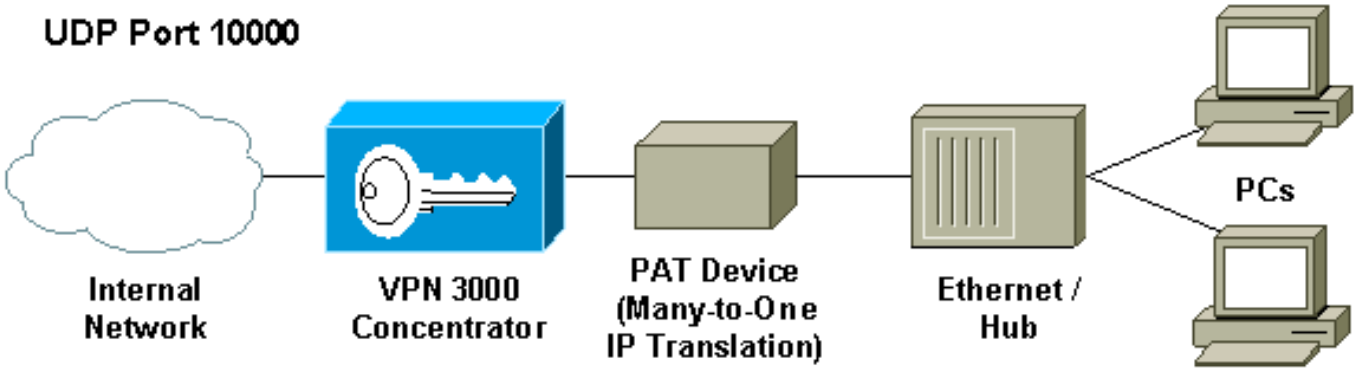
يؤدي تنشيط وضع IPSec الشفاف على مركز VPN إلى إنشاء قواعد تصفية غير مرئية وتطبيقها على عامل التصفية العام. ثم يتم تمرير رقم المنفذ الذي تم تكوينه إلى عميل VPN بشكل شفاف عند اتصال عميل VPN. على الجانب الوارد، تمر حركة مرور UDP الواردة من ذلك المنفذ مباشرة إلى IPSec للمعالجة. يتم فك تشفير حركة المرور وفك كبسلها، ثم توجيهها بشكل طبيعي. على الجانب الصادر، يقوم IPSec بتشفير رأس UDP وتغليفه ثم تطبيقه (إذا تم تكوينه). يتم إلغاء تنشيط قواعد عامل تصفية وقت التشغيل وحذفها من عامل التصفية المناسب بموجب ثلاثة شروط: عند تعطيل IPSec عبر UDP لمجموعة ما، أو عند حذف المجموعة، أو عند حذف آخر IPSec نشط عبر UDP SA على ذلك المنفذ. يتم إرسال رسائل Keepalives لمنع جهاز NAT من إغلاق تعيين المنفذ بسبب عدم النشاط.

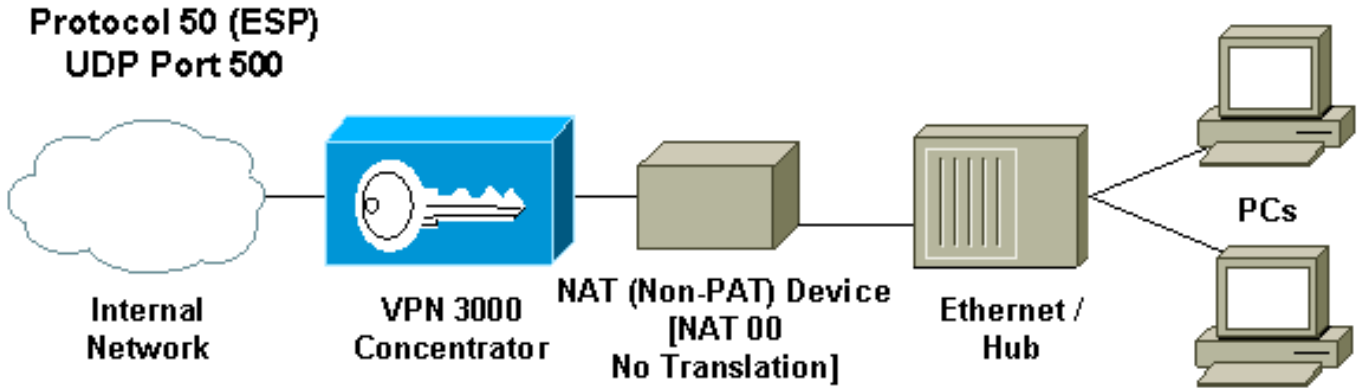
إذا تم تمكين IPSec عبر NAT-T على مركز الشبكة الخاصة الظاهرية (VPN)، فعندئذ يستخدم عميل مركز/شبكة VPN وضع NAT-T من تضمين UDP. يعمل NAT-T عن طريق الكشف التلقائي لأي جهاز NAT بين عميل VPN ومجمع VPN أثناء تفاوض IKE. أنت ينبغي ضمنت أن لا يمنع UDP ميناء 4500 بين ال VPN مركز/VPN زبون ل NAT-T أن يعمل. أيضا، إذا كنت تستخدم تكوين IPSec/UDP سابق يستخدم هذا المنفذ بالفعل، فيجب عليك إعادة تكوين IPSec/UDP السابق لاستخدام منفذ UDP مختلف. بما أن NAT-T عبارة عن مسودة IETF، فإنها تساعد عند إستخدام أجهزة متعددة الموردين إذا كان المورد الآخر يطبق هذا المعيار.

يعمل NAT-T مع كل من إتصالات عميل VPN وإتصالات شبكة LAN إلى شبكة LAN بخلاف IPSec عبر UDP/TCP. كما تدعم موجهات Cisco IOS® وأجهزة جدار حماية PIX تقنية NAT-T.

أنت لا تحتاج IPSec عبر UDP أن يكون مكنت أن يعمل NAT-T.

تشكيل nat أسلوب شفاف





أستخدم الإجراء التالي لتكوين الوضع الشفاف NAT على مركز VPN.

ملاحظة: يتم تكوين IPSec عبر UDP على أساس كل مجموعة، بينما يتم تكوين IPSec عبر TCP/NAT-T بشكل عام.

1. تكوين IPSec عبر UDP:على مركز الشبكة الخاصة الظاهرية (VPN)، حدد **التكوين > إدارة المستخدم > المجموعات**.لإضافة مجموعة، حدد **إضافة**. لتعديل مجموعة موجودة، قم بتحديدها وانقر فوق **تعديل**.طقطقت ال IPSec علامة تبويب، فحصت **IPSec من خلال NAT** وشكلت **ال IPSec من خلال UDP NAT ميناء**. يكون المنفذ الافتراضي ل IPSec من خلال NAT هو 10000 (المصدر والوجهة)، ولكن قد يتم تغيير هذا الإعداد.
2. تكوين IPSec عبر NAT-T و/أو IPSec عبر TCP:على مركز VPN، حدد تكوين > **نظام > بروتوكولات الاتصال النفقي > IPSec > شفافية NAT**.حدد خانة الاختيار **IPSec عبر NAT-T و/أو TCP**.

إذا كان كل شيء متاحا، أستخدم هذه السابقة:

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

تكوين عميل Cisco VPN لاستخدام شفافية NAT

لاستخدام IPSec عبر UDP أو NAT-T، يلزمك تمكين IPSec عبر UDP على Cisco VPN Client 3.6 والإصدارات الأحدث. يعين ال UDP ميناء ب ال VPN مركز في حالة IPSec على UDP، بينما ل NAT-T هو ثابت إلى UDP ميناء 4500.

لاستخدام IPSec عبر TCP، يلزمك تمكينه على عميل VPN وتكوين المنفذ الذي يجب إستخدامه يدويا.

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة دعم IPSec
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).