ما هو حل الشبكة الخاصة الظاهرية (VPN) المناسب لك؟

المحتويات

المقدمة
قبل البدء
الاصطلاحات
المتطلبات الأساسية
المكونات المستخدمة
nat
اتصال GRE النفقي
تشفير IPSec
PPTP و MPPE
VPDN و L2TP
VPDN
L2TP
PPPoE
MPLS VPN
معلومات ذات صلة

المقدمة

تكتسب الشبكات الخاصة الظاهرية (VPN) رواجا متزايدا كتكلفة أقل وطريقة أكثر مرونة لنشر الشبكة عبر منطقة واسعة. مع التقدم في التقنية تأتي مجموعة متزايدة من الخيارات لتنفيذ حلول الشبكات الخاصة الظاهرية (VPN). تشرح هذه الملاحظة التقنية بعض هذه الخيارات وتصف الأماكن التي يمكن إستخدامها فيها على أفضل وجه.

قبل البدء

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

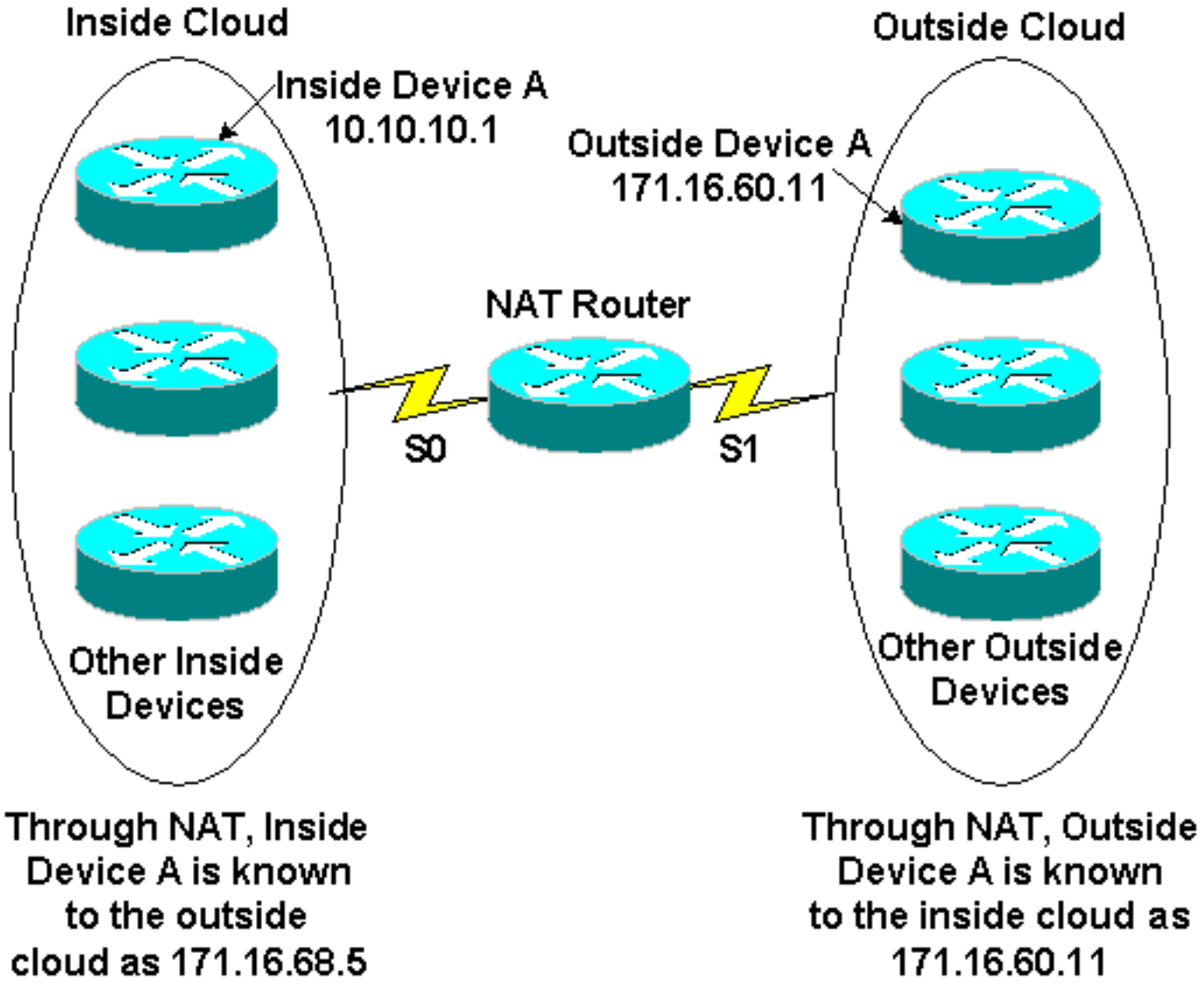
ملاحظة: توفر Cisco أيضا دعم التشفير في الأنظمة الأساسية بخلاف IOS بما في ذلك جدار حماية PIX الآمن من Cisco ومجمع Cisco VPN 3000 ومركز Cisco VPN 5000.

nat

لقد شهدت شبكة الإنترنت نموا هائلا في وقت قصير، أكثر بكثير مما كان يمكن للمصممين الاصليين توقعه. العدد المحدود للعناوين المتاحة في الإصدار 4.0 من IP هو دليل على هذا النمو، والنتيجة هي أن مساحة العنوان أصبحت أقل توفرا. واحد حل ل هذا مشكلة هو شبكة عنوان ترجمة (nat).

تم تكوين إستخدام NAT Router على الحدود الداخلية/الخارجية مثل أن يرى الخارج (عادة الإنترنت) عنوانا أو بعض العناوين المسجلة بينما قد يحتوي الداخل على أي عدد من البيئات المضيفة باستخدام مخطط عنونة خاص. للحفاظ على سلامة نظام ترجمة العنوان، يجب تكوين NAT على كل موجه حدود بين الشبكة الداخلية (الخاصة) والشبكة الخارجية (العامة). من مزايا NAT من وجهة نظر أمنية أن الأنظمة على الشبكة الخاصة لا يمكنها أن تستلم اتصال IP قادم من الشبكة الخارجية ما لم يتم تكوين بوابة NAT بشكل خاص للسماح بالاتصال. علاوة على ذلك، NAT شفاف تماما إلى المصدر والوجهة. تتضمن العملية الموصى بها من قبل RFC 1918 NAT ، والذي يحدد مخططات عنونة الشبكة الخاصة المناسبة. يتم وصف المعيار ل NAT في RFC1631 .

يوضح الشكل التالي تعريف حد موجه NAT مع تجمع عناوين شبكة الترجمة الداخلية.

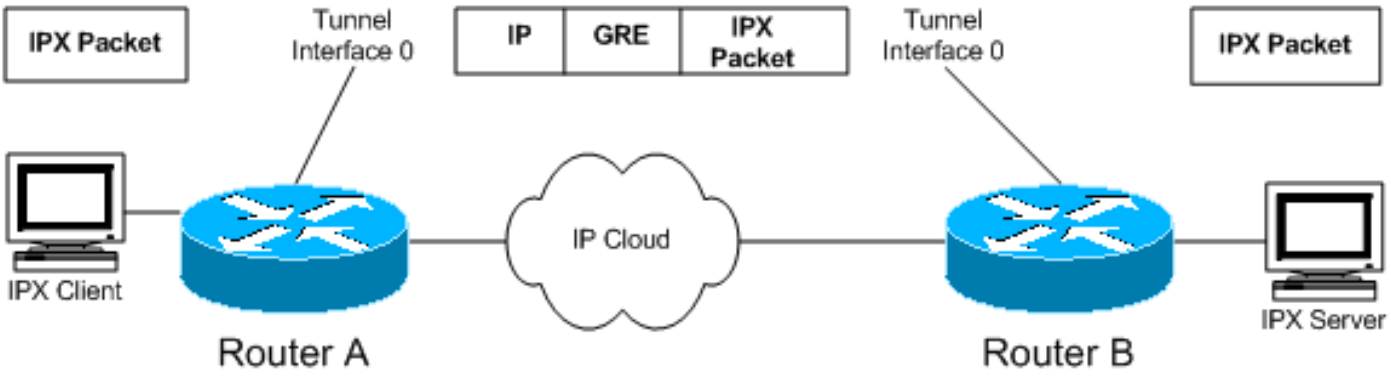


يستخدم NAT بشكل عام لحفظ عناوين IP الموجهة على الإنترنت، والتي تكون مكلفة ومحدودة في العدد. nat أيضا يوفر أمن باخفاء الشبكة داخلي من الإنترنت.

لمعلومات عن عمل NAT، راجع كيف يعمل NAT.

اتصال GRE النفقي

توفر أنفاق تضمين التوجيه العام (GRE) مسارا محددا عبر شبكة WAN المشتركة وتضمين حركة المرور باستخدام رؤوس الحزم الجديدة لضمان التسليم إلى وجهات محددة. الشبكة خاصة لأنه يمكن لحركة المرور إدخال نفق عند نقطة نهاية فقط ويمكنها تركه فقط عند نقطة النهاية الأخرى. لا توفر الأنفاق سرية حقيقية (مثل التشفير) ولكن يمكنها حمل حركة مرور مشفرة. تكون الأنفاق نقاط نهاية منطقية تم تكوينها على الواجهات المادية التي يتم نقل حركة المرور من خلالها.



وكما هو موضح في المخطط، يمكن أيضا إستخدام اتصال GRE النفقي لتضمين حركة المرور غير الخاصة ب IP في IP وإرسالها عبر الإنترنت أو شبكة IP. إن بروتوكولات تبادل حزم الإنترنت (IPX) و AppleTalk هي أمثلة على حركة مرور غير خاصة ب IP. للحصول على معلومات حول تكوين GRE، راجع "تكوين واجهة نفق GRE" في تكوين GRE.

GRE هو حل VPN المناسب لك إذا كانت لديك شبكة متعددة البروتوكولات مثل IPX أو AppleTalk وكان عليك إرسال حركة مرور البيانات عبر الإنترنت أو شبكة IP. كما يتم إستخدام تضمين GRE بشكل عام بالاقتران مع الوسائل الأخرى لتأمين حركة المرور، مثل IPSec.

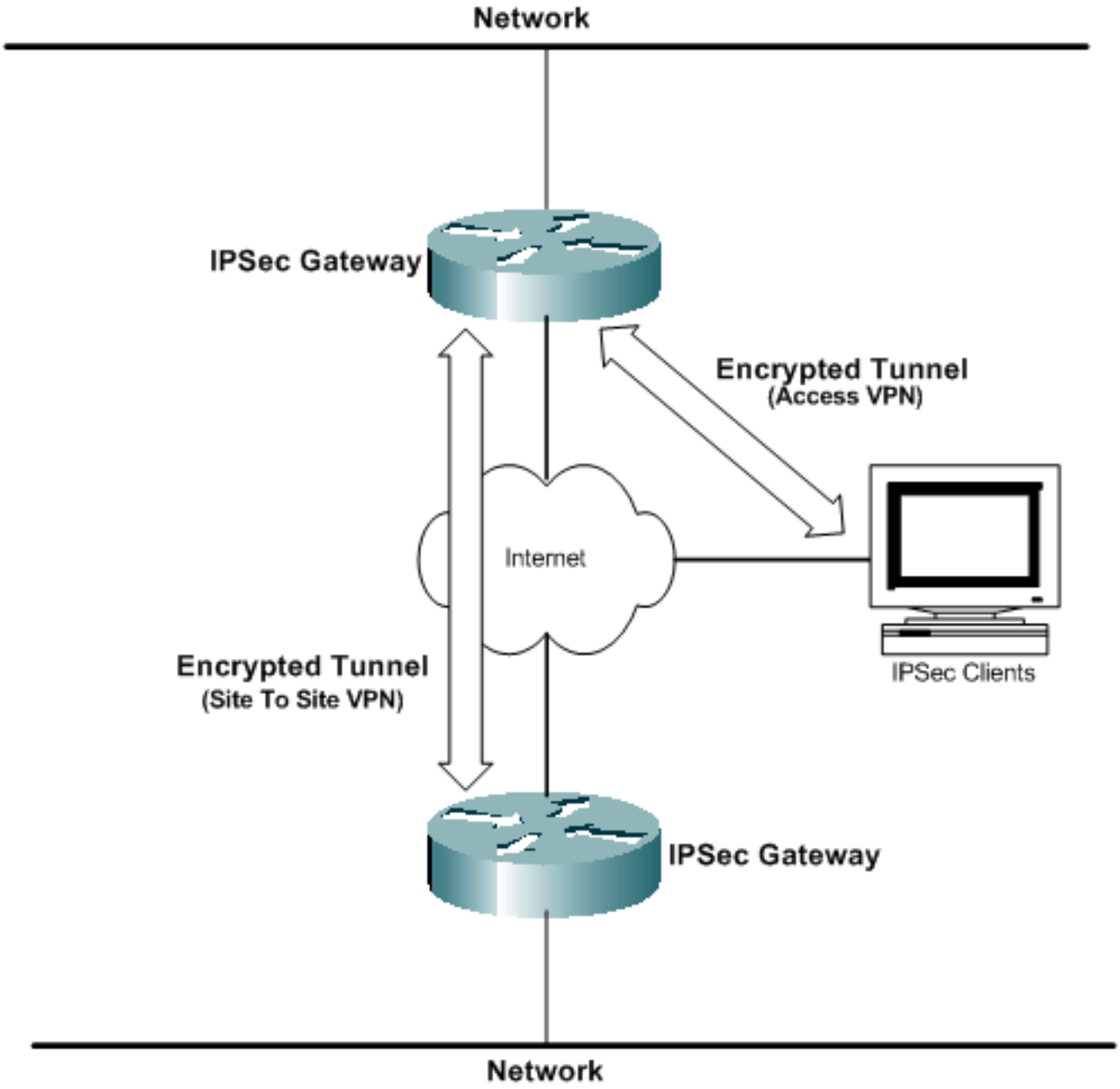
لمزيد من التفاصيل التقنية حول GRE، ارجع إلى RFC 1701 وRFC 2784 .

تشفير IPSec

يقصد بتشفير البيانات المرسلة عبر شبكة مشتركة تقنية VPN في معظم الأحيان المرتبطة بشبكات VPN. تدعم Cisco طرق تشفير بيانات أمان IP (IPSec). IPSec هو إطار عمل للمعايير المفتوحة يوفر سرية البيانات وسلامة البيانات ومصادقة البيانات بين النظراء المشاركين في طبقة الشبكة.

تشفير IPSec هو معيار صادر عن "فريق عمل هندسة الإنترنت (IETF)" يدعم معيار تشفير البيانات (-56 (DESبت و DES الثلاثي (-168 (3DESبت خوارزميات تشفير المفاتيح المتماثل في برنامج عميل IPSec. تكوين GRE إختياري مع IPSec. كما يدعم IPSec سلطات الشهادات والتفاوض مع مفتاح الإنترنت (IKE). يمكن نشر تشفير IPSec في البيئات المستقلة بين العملاء والموجهات وجدران الحماية، أو إستخدامه بالاقتران مع اتصال L2TP النفقي في شبكات VPN الخاصة بالوصول. يتم دعم IPSec في العديد من منصات أنظمة التشغيل.

يعد تشفير IPSec حل الشبكة الخاصة الظاهرية (VPN) المناسب لك إذا كنت تريد سرية بيانات حقيقية لشبكاتك. كما أن IPSec هو معيار مفتوح، لذلك يسهل تنفيذ إمكانية التشغيل البيني بين الأجهزة المختلفة.



PPTP و MPPE

تم تطوير بروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP) من قبل Microsoft، وهو موضح في RFC2637 . يتم نشر بروتوكول PPTP بشكل واسع في أنظمة التشغيل Windows 9x/ME و Windows NT و Windows 2000 وبرنامج عميل Windows XP لتمكين الشبكات الخاصة الظاهرية (VPN) الطوعية.

(Microsoft Point-to-Point Encryption (MPPE عبارة عن مسودة IETF إعلامية من Microsoft تستخدم تشفير bit-40 أو 128-بت المستند إلى RC4. وتعد MPPE جزءا من حل برامج عميل PPTP من Microsoft وهي مفيدة في بنى شبكات VPN الخاصة بالوصول في الوضع الطوعي. يتم دعم PPTP/MPPE على معظم منصات Cisco.

تمت إضافة دعم PPTP إلى برنامج Cisco IOS الإصدار XE5.12.0.5 على الأنظمة الأساسية Cisco 7100 و 7200. تمت إضافة الدعم لمزيد من الأنظمة الأساسية في Cisco IOS 12.1.5.T. كما يتضمن جدار حماية PIX الآمن من Cisco ومجمع VPN 3000 من Cisco دعم إتصالات عميل PPTP.

ونظرا لأن بروتوكول PPTP يدعم الشبكات غير الخاصة ب IP، فمن المفيد عندما يضطر المستخدمون البعيدين إلى الاتصال بشبكة الشركة للوصول إلى شبكات الشركات غير المتجانسة.

للحصول على معلومات حول تكوين PPTP، راجع تكوين PPTP.

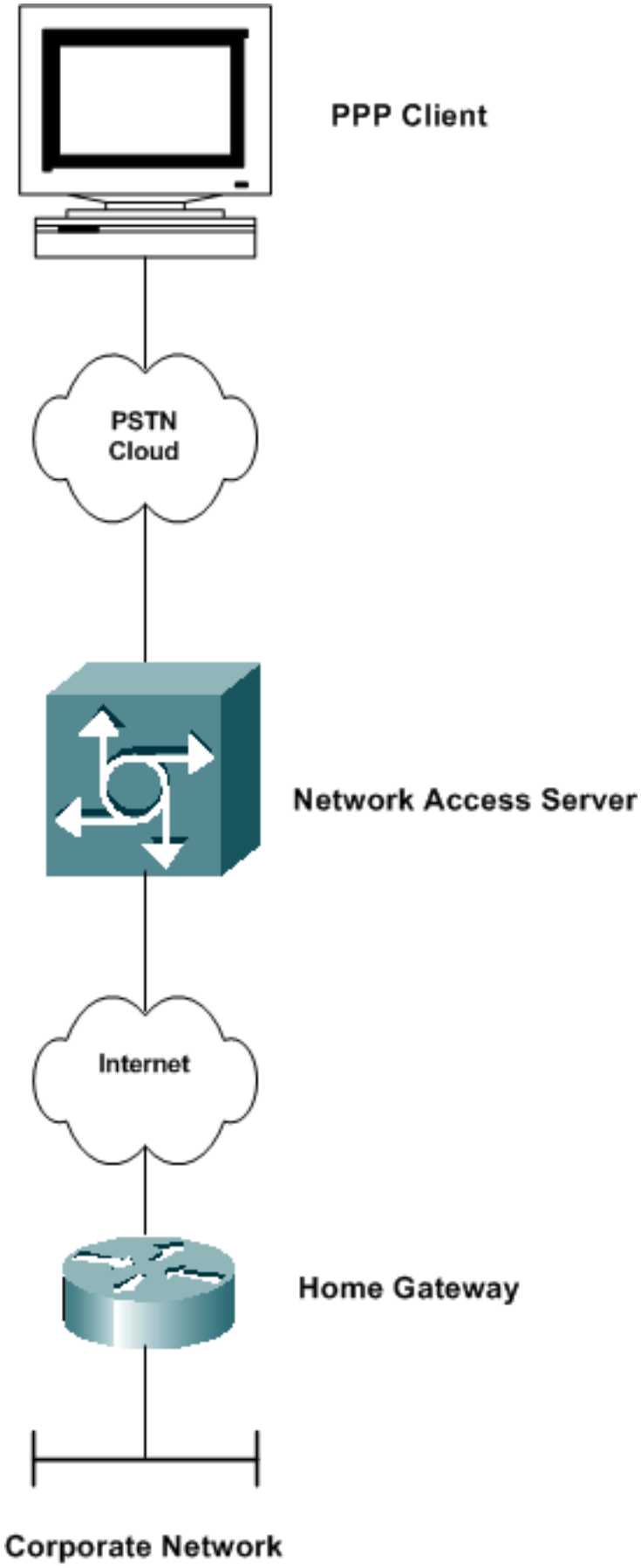
VPDN و L2TP

VPDN

شبكة الاتصال الخاصة الظاهرية (VPDN) هي شبكة قياسية من Cisco تتيح لخدمة طلب اتصال الشبكة الخاصة إمكانية المرور إلى خوادم الوصول عن بعد. في سياق VPDN، يشار عادة إلى خادم الوصول (على سبيل المثال، AS5300) الذي تم الطلب عليه باسم خادم الوصول إلى الشبكة (NAS). تتم الإشارة إلى وجهة مستخدم الطلب الهاتفي باسم البوابة الرئيسية (HGW).

السيناريو الأساسي هو أن يقوم عميل بروتوكول الاتصال من نقطة إلى نقطة (PPP) بالدخول إلى وحدة تخزين متصلة بالشبكة (NAS) محلية. تحدد NAS أنه يجب إعادة توجيه جلسة عمل PPP إلى موجه بوابة رئيسية لذلك العميل. ثم يقوم HGW بمصادقة المستخدم وبدء تفاوض PPP. بعد اكتمال إعداد PPP، يتم إرسال جميع الإطارات عبر وحدات التخزين المتصلة بالشبكة (NAS) إلى العميل والعبارات الرئيسية. تقوم هذه الطريقة بدمج العديد من البروتوكولات والمفاهيم.

للحصول على معلومات حول تكوين شبكة VPDN، راجع *تكوين شبكة طلب هاتفي خاصة افتراضية* في تكوين ميزات الأمان.



L2TP

بروتوكول الاتصال النفقي للطبقة 2 (L2TP) هو معيار IETF يتضمن أفضل سمات PPTP و L2F. يتم إستخدام أنفاق L2TP بشكل أساسي في الوضع الإلزامي (أي اتصال NAS إلى HGW) للوصول إلى شبكات VPN لكل من حركة مرور IP وغير IP. أضاف Windows 2000 و Windows XP الدعم الأصلي لهذا البروتوكول كوسيلة لاتصال عميل

.VPN

يتم إستخدام L2TP لأنفاق PPP عبر شبكة عامة، مثل الإنترنت، باستخدام IP. بما أن النفق يقع في الطبقة 2، فإن بروتوكولات الطبقة العليا تجهل النفق. وكما هو الحال مع GRE، يمكن أن يقوم L2TP أيضا بتضمين أي بروتوكول من الطبقة 3. يتم إستخدام منفذ UDP 1701 لإرسال حركة مرور L2TP بواسطة بادئ النفق.

ملاحظة: في عام 1996، أنشأت Cisco بروتوكول إعادة توجيه الطبقة 2 (L2F) للسماح بحدوث إتصالات VPDN. لا يزال L2F مدعوما للوظائف الأخرى، ولكن تم إستبداله ب L2TP. كما تم في عام 1996 إنشاء بروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP) وصيغة إنترنت بواسطة IETF. ووفر PPTP وظيفة مماثلة لبروتوكول النفق الشبيه ب GRE لاتصالات PPP.

للحصول على مزيد من المعلومات حول L2TP، راجع بروتوكول نفق الطبقة 2.

PPPoE

PPP عبر الإيثرنت (PPPoE) هو RFC معلوماتي يتم نشره بشكل أساسي في بيئات خط المشترك الرقمي (DSL). يعمل بروتوكول PPPoE على زيادة فعالية البنية الأساسية لشبكة الإيثرنت الحالية للسماح للمستخدمين ببدء جلسات عمل بروتوكول الاتصال من نقطة إلى نقطة (PPP) متعددة داخل شبكة LAN نفسها. وتتيح هذه التقنية إمكانية إختيار الخدمة من المستوى الثالث، وهو تطبيق ناشئ يتيح للمستخدمين إمكانية الاتصال في آن واحد بوجهات متعددة من خلال اتصال واحد للوصول عن بعد. غالبا ما يتم إستخدام PPPoE مع بروتوكول مصادقة كلمة المرور (PAP) أو بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (CHAP) لإعلام الموقع المركزي الذي يتم توصيل الموجهات عن بعد به.

يتم إستخدام PPPoE غالبا في عمليات نشر DSL الخاصة بمزود الخدمة ومخططات الإيثرنت الوسيط.

لمزيد من المعلومات حول تكوين PPPoE، راجع تكوين PPPoE عبر الإيثرنت و IEEE 802.1Q VLAN.

MPLS VPN

تبديل أسماء البروتوكولات المتعددة (MPLS) هو معيار IETF جديد قائم على تحويل علامات Cisco الذي يتيح ميزات الإمداد التلقائي والتشغيل السريع وقابلية التطوير التي يحتاج إليها الموفرون لتوفير خدمات الوصول والإنترانت والإكسترانت VPN بتكلفة منخفضة. تعمل Cisco بشكل وثيق مع موفري الخدمة لضمان الانتقال السلس إلى خدمات VPN التي تم تمكين MPLS بها. يعمل MPLS على نموذج قائم على التسمية، حيث يتم وضع علامات على الحزم أثناء إدخالها إلى شبكة الموفر لتسريع إعادة التوجيه من خلال مركز IP غير متصل. يستخدم MPLS مميزات المسار لتحديد عضوية VPN واحتواء حركة مرور البيانات داخل مجتمع VPN.

كما يضيف MPLS فوائد النهج الموجه نحو الاتصال إلى نموذج توجيه IP، من خلال إنشاء مسارات محولة التسمية، والتي يتم إنشاؤها استنادا إلى معلومات المخطط بدلا من تدفق حركة المرور. يتم نشر شبكة MPLS VPN بشكل واسع في بيئة مزود الخدمة.

رأيت لمعلومة على يشكل MPLS VPN، يشكل MPLS VPN أساسي.

معلومات ذات صلة

- صفحة دعم IPSec
- كيف تعمل الشبكات الخاصة الظاهرية
- صفحة دعم ترجمة عناوين الشبكة (NAT)
- صفحة دعم GRE
- صفحة دعم VPDN

- صفحة دعم PPTP
- صفحة دعم PPPoE
- 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).