كيف تعمل الشبكات الخاصة الظاهرية

المحتويات

المقدمة

يغطي هذا المستند أساسيات الشبكات الخاصة الظاهرية (VPN)، مثل المكونات الأساسية للشبكات الخاصة الظاهرية (VPN) والتقنيات والاتصال النفقي وأمان الشبكات الخاصة الظاهرية (VPN).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

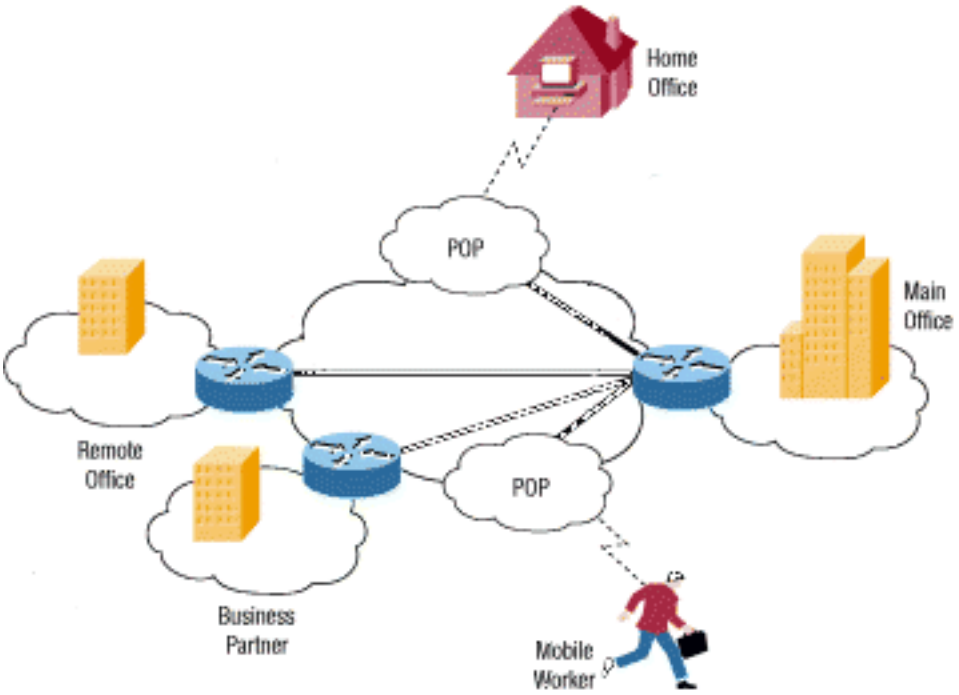
راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

لقد تغير العالم كثيرا في العقود القليلة الماضية. فبدلا من التعامل ببساطة مع المخاوف المحلية أو الإقليمية، بات لزاما على العديد من الشركات الآن أن تفكر في الأسواق العالمية والخدمات اللوجستية. العديد من الشركات لديها مرافق تنتشر في جميع أنحاء البلاد، أو حتى في جميع أنحاء العالم. ولكن هناك أمر واحد تحتاج إليه جميع الشركات: وهو وسيلة للحفاظ على الاتصال السريع والآمن والموثوق أينما كانت مكاتبها.

حتى وقت قريب، كان الاتصال الموثوق يعني إستخدام خطوط مستأجرة للحفاظ على شبكة واسعة (WAN). وتوفر الخطوط المستأجرة، التي تتراوح بين شبكة الخدمات الرقمية المتكاملة (ISDN) التي تعمل بسرعة 144 كيلوبت/ثانية) إلى ألياف الناقل الضوئي-3 (OC3، التي تعمل بسرعة 155 ميجابت/ثانية)، للشركة طريقة لتوسيع شبكتها الخاصة إلى ما وراء منطقتها الجغرافية المباشرة. تتمتع شبكة الاتصال اللاسلكية واسعة النطاق بمزايا واضحة على شبكة عامة مثل الإنترنت عندما يتعلق الأمر بالثقة والأداء والأمان، ولكن الحفاظ على شبكة الاتصال واسعة النطاق (WAN)، وخاصة عند إستخدام خطوط مستأجرة، يمكن أن يصبح مكلفا للغاية (وهو غالبا ما يرتفع في التكلفة مع زيادة المسافة بين المكاتب). وبالإضافة إلى ذلك، فإن الخطوط المستأجرة ليست حلا قابلا للتطبيق بالنسبة للمؤسسات التي يكون فيها جزء من قوة العمل قادرا على التنقل بدرجة عالية (كما هو الحال بالنسبة لموظفي التسويق) وقد يكون من الضروري في كثير من الأحيان الاتصال بشبكة الشركة عن بعد والوصول إلى البيانات الحساسة.

مع أزدياد شعبية الإنترنت، لجأت الشركات اليه كوسيلة لتوسيع شبكاتها الخاصة. في البداية، ظهرت شبكات الإنترنت الداخلية، وهي مواقع مصممة للاستخدام فقط من قبل موظفي الشركة. الآن، تقوم العديد من الشركات بإنشاء شبكاتها الخاصة الافتراضية (VPN) لتلبية إحتياجات الموظفين البعيدين والمكاتب البعيدة.



قد تشتمل الشبكة الخاصة الظاهرية (VPN) النموذجية على شبكة محلية رئيسية (LAN) في المقر الرئيسي للشركة، وشبكات محلية أخرى في المكاتب أو المرافق البعيدة، بالإضافة إلى المستخدمين الأفراد الذين يتواصلون من الميدان.

شبكة VPN هي شبكة خاصة تستخدم شبكة عامة (عادة ما تكون الإنترنت) لتوصيل المواقع البعيدة أو المستخدمين معا. وبدلا من إستخدام اتصال مخصص في العالم الحقيقي، مثل الخط المؤجر، تستخدم الشبكة الخاصة الظاهرية (VPN) الاتصالات "الافتراضية" الموجهة عبر الإنترنت من شبكة الشركة الخاصة إلى الموقع البعيد أو الموظف.

ما الذي يجعل شبكة خاصة ظاهرية (VPN)؟

هناك نوعان شائعان من شبكات VPN.

- **الوصول عن بعد**— يسمى أيضا شبكة الطلب الهاتفي الخاصة الظاهرية (VPDN)، وهذا اتصال من مستخدم إلى شبكة LAN تستخدمه شركة بها موظفون يحتاجون إلى الاتصال بالشبكة الخاصة من مواقع بعيدة مختلفة. في العادة، توفر الشركة التي ترغب في إعداد شبكة خاصة ظاهرية (VPN) كبيرة للوصول عن بعد شكلا ما من حسابات الاتصال الهاتفي عبر الإنترنت لمستخدميها باستخدام مزود خدمة الإنترنت (ISP). ويمكن بعد ذلك للمتفرجين عن بعد طلب رقم 1-800 للوصول إلى الإنترنت واستخدام برنامج عميل VPN الخاص بهم للوصول إلى شبكة الشركة. ومن الأمثلة الجيدة على الشركات التي تحتاج إلى شبكة خاصة ظاهرية (VPN) للوصول عن

بعد أن تكون شركة كبيرة تضم المئات من موظفي المبيعات في هذا المجال. تتيح شبكات VPN للوصول عن بعد إتصالات آمنة ومشفرة بين الشبكة الخاصة لشركة ما والمستخدمين عن بعد من خلال مزود خدمة تابع لجهة خارجية.

- **من موقع إلى موقع** — من خلال إستخدام معدات مخصصة وتشفير على نطاق واسع، يمكن لشركة ما ربط مواقع ثابتة متعددة عبر شبكة عامة مثل الإنترنت. فكل موقع لا يحتاج إلا إلى اتصال محلي بنفس الشبكة العامة، وبالتالي توفير المال على خطوط مستأجرة خاصة طويلة. كما يمكن تصنيف الشبكات الخاصة الظاهرية (VPN) من موقع إلى موقع إلى شبكات داخلية أو شبكات خارجية. يقال إن شبكة خاصة ظاهرية (VPN) من موقع إلى موقع تم إنشاؤها بين مكاتب الشركة نفسها هي شبكة خاصة ظاهرية (VPN) من إنترانت، بينما تتم الإشارة إلى شبكة خاصة ظاهرية (VPN) تم إنشاؤها لتوصيل الشركة بشريكها أو عملائها باسم شبكة خاصة ظاهرية (VPN) من إكسترانت.

بإمكان الشبكة الخاصة الظاهرية (VPN) المصممة بشكل جيد أن تفيد أي شركة بشكل كبير. على سبيل المثال، يمكنها:

- توسيع نطاق الاتصال الجغرافي
- تقليل تكاليف التشغيل مقابل شبكات WAN التقليدية
- تقليل وقت الانتقال وتكاليف السفر للمستخدمين عن بعد
- تحسين الإنتاجية
- تبسيط مخطط الشبكة
- توفير فرص الاتصال الشبكي العالمي
- توفير الدعم للعاملين عن بعد
- توفير عائد أستثمار (ROI) أسرع من عائد الاستثمار (WAN) التقليدي

ما الميزات المطلوبة في شبكة خاصة ظاهرية (VPN) مصممة بشكل جيد؟ ويجب أن تتضمن هذه البنود:

- الأمان
- موثوقية
- قابلية التطوير
- إدارة الشبكة
- إدارة السياسة

التشبيه: كل شبكة محلية هي شبكة محلية ظاهرية

تخيل أنك تعيش في جزيرة في محيط كبير. هنالك آلاف الجزر الاخرى حولكم، بعضها قريب جدا واخرى بعيدة. الطريقة العادية للسفر هي ان تصطحبوا عبارة من جزيرتكم إلى اية جزيرة ترغبون في زيارتها. السفر على متن عبارة يعني انه ليس لديكم تقريبا اية خصوصية. أي شيء تفعله يمكن أن يراه شخص آخر.

لنفترض أن كل جزيرة تمثل شبكة محلية خاصة وأن المحيط عبارة عن شبكة إنترنت. عندما تسافر بالعبارة، يكون ذلك مماثلا عندما تتصل بخادم ويب أو بجهاز آخر عبر الإنترنت. ليس لديك سيطرة على الأسلاك والموجهات التي تشكل الإنترنت، تماما كما ليس لديك سيطرة على الأشخاص الآخرين على العبارة. وهذا يجعلك عرضة لمشكلات أمان إذا حاولت الاتصال بين شبكتين خاصتين باستخدام مورد عام.

وتقرر جزيرتك بناء جسر إلى جزيرة أخرى بحيث تكون هناك طريقة أسهل وأأمن ومباشرة للناس للتنقل بين الاثنتين. فبناء الجسر وصيانته مكلف جدا، رغم ان الجزيرة التي تصلون بها قريبة جدا. ولكن الحاجة إلى طريق آمن يعتمد عليه كبيرة جدا بحيث تفعلونه على اية حال. ترغب جزيرتك في الاتصال بجزيرة ثانية بعيدة جدا، لكنك تقرر انها غالية جدا.

هذا الوضع يشبه كثيرا إستئجار خط. والجسور (الخطوط المستأجرة) منفصلة عن المحيط (الإنترنت)، ومع ذلك فهي قادرة على الربط بين الجزر (الشبكات المحلية). لقد أختارت العديد من الشركات هذا المسار نظرا للحاجة إلى الأمان والموثوقية في الاتصال بمكاتبها البعيدة. ولكن إذا كانت المكاتب متباعدة جدا، فإن التكلفة قد تكون باهظة للغاية تماما مثل محاولة بناء جسر يمتد لمسافة كبيرة.

إذا كيف تتناسب الشبكة الخاصة الظاهرية (VPN) مع هذا التناظر؟ يمكننا أن نعطي كل ساكن في جزرنا غواصة صغيرة خاصة به مع هذه الخصائص.

- إنه سريع.
- من السهل اصطحابه معك أينما ذهبت.
- وهو قادر على إخفائكم كليا من اية قوارب أو غواصات أخرى.
- يعتمد عليه.
- ولا يكلف الكثير من الغواصات الاضافية التي تضيفها إلى أسطولك ما ان تشترى الاولى.

وعلى الرغم من انهم يسافرون في المحيط مع حركة مرور أخرى، يمكن لسكان جزيرتنا ان يسافروا ذهابا وإيابا كلما أرادوا ذلك بالخصوصية والامن. هذه هي الكيفية التي تعمل بها شبكة خاصة ظاهرية (VPN). يمكن لكل عضو بعيد في شبكتك الاتصال بطريقة آمنة وموثوقة باستخدام الإنترنت كوسيط للاتصال بشبكة LAN الخاصة. يمكن تطوير شبكة خاصة ظاهرية (VPN) لاستيعاب المزيد من المستخدمين والمواقع المختلفة بشكل أسهل بكثير من أي خط مستأجر. وفي الواقع، تعد قابلية التطوير ميزة رئيسية تتمتع بها الشبكات الخاصة الظاهرية (VPN) مقارنة بالخطوط المستأجرة النموذجية. على عكس الخطوط المستأجرة حيث تزيد التكلفة بالتناسب مع المسافات المعنية، فإن المواقع الجغرافية لكل مكتب لا تشكل أهمية كبيرة في إنشاء شبكة خاصة ظاهرية (VPN).

تقنيات VPN

تستخدم الشبكة الخاصة الظاهرية (VPN) المصممة جيدا العديد من الطرق للحفاظ على أمان الاتصال والبيانات.

- **سرية البيانات**—قد تكون هذه هي الخدمة الأكثر أهمية التي يوفرها أي تطبيق للشبكات الخاصة الظاهرية (VPN). بما أن بياناتك الخاصة تنتقل عبر شبكة عامة، فإن سرية البيانات تعد أمرا حيويا ويمكن الحصول عليها من خلال تشفير البيانات. هذه هي عملية أخذ كل البيانات التي يرسلها أحد أجهزة الكمبيوتر إلى جهاز آخر وترميزها إلى نموذج لن يتمكن من فك ترميزه إلا جهاز الكمبيوتر الآخر.تستخدم معظم شبكات VPN أحد هذه البروتوكولات لتوفير التشفير.يوفر بروتوكول أمان بروتوكول الإنترنت **IPsec**—ميزات أمان محسنة مثل خوارزميات تشفير أقوى ومصادقة أكثر شمولا. يحتوي IPsec على وضعي تشفير: النفق والنقل. يقوم وضع النفق بتشفير الرأس والحمولة لكل حزمة بينما يقوم وضع النقل بتشفير الحمولة فقط. يمكن فقط للأنظمة المتوافقة مع IPsec الاستفادة من هذا البروتوكول. أيضا، يجب أن تستخدم جميع الأجهزة مفتاحا أو شهادة مشتركا ويجب أن يكون لها نهج تأمين مشابهة جدا تم إعدادها.بالنسبة لمستخدمي الشبكة الخاصة الظاهرية (VPN) للوصول عن بعد، يوفر شكل من أشكال حزمة البرامج التابعة لجهات خارجية الاتصال والتشفير على كمبيوتر المستخدمين. يدعم IPsec إما تشفير 56 بت (DES أحادي) أو تشفير 168 بت (DES الثلاثي).تم إنشاء **بروتوكول** PPTP—**PPTP/MPPE** من قبل منتدى PPTP، وهو إتحاد يضم شركات روبوتات في الولايات المتحدة، و Microsoft، و 3COM، و Ascend، و ECI Telemtics. يدعم PPTP شبكات VPN متعددة البروتوكولات، مع تشفير 40-بت و 128-بت باستخدام بروتوكول يسمى MPPE) Microsoft Point-to-Point Encryption). ومن المهم ملاحظة أن بروتوكول الاتصال من نقطة إلى نقطة (PPTP) لا يوفر في حد ذاته تشفير البيانات.**L2TP/IPsec** — يسمى L2TP بشكل عام عبر IPsec، يوفر هذا أمان بروتوكول IPsec عبر إنشاء قنوات بروتوكول الاتصال النفقي للطبقة 2 (L2TP). L2TP هو نتاج شراكة بين أعضاء منتدى PPTP، و Cisco، وفرقة عمل هندسة الإنترنت (IETF). يستخدم بشكل أساسي للشبكات الخاصة الظاهرية (VPN) للوصول عن بعد مع أنظمة التشغيل Windows 2000، نظرا لأن Windows 2000 يوفر عميل IPsec و L2TP أصلي. كما يمكن لموفري خدمة الإنترنت توفير إتصالات L2TP لمستخدمي الطلب الهاتفي، ثم تشفير حركة المرور هذه باستخدام IPsec بين نقطة الوصول الخاصة بهم وخادم شبكة المكتب البعيد.
- **تكامل البيانات**—على الرغم من أهمية تشفير بياناتك عبر شبكة عامة، فمن المهم أيضا التحقق من أنها لم تتغير أثناء النقل. على سبيل المثال، يحتوي IPsec على آلية لضمان عدم التلاعب بالجزء المشفر من الحزمة، أو رأس الحزمة بالكامل وجزء البيانات منها. إذا تم اكتشاف التلاعب، يتم إسقاط الحزمة. كما يمكن أن تتضمن سلامة البيانات مصادقة النظير البعيد.
- **مصادقة أصل البيانات**—من المهم للغاية التحقق من هوية مصدر البيانات التي يتم إرسالها. وهذا ضروري للحماية من عدد من الهجمات التي تعتمد على انتحال هوية المرسل.
- **مكافحة إعادة التشغيل**- هذه هي القدرة على اكتشاف الحزم التي تمت إعادة تشغيلها ورفضها والمساعدة على

منع الانتحال.

- **اتصال البيانات النفقي/سرية تدفق حركة مرور البيانات**— هي عملية تضمين حزمة كاملة داخل حزمة أخرى وإرسالها عبر شبكة. يكون اتصال البيانات النفقي مفيدا في الحالات التي يكون من المفضل فيها إخفاء هوية الجهاز الذي يقوم بإنشاء حركة المرور. على سبيل المثال، يقوم جهاز واحد باستخدام IPsec بتضمين حركة مرور البيانات التي تنتمي إلى عدد من البيئات المضيفة خلفه ويضيف رأسه الخاص على الحزم الموجودة. بتشفير الحزمة الأصلية والرأس (وتوجيه الحزمة بناء على رأس الطبقة 3 الإضافي الذي تمت إضافته إلى الأعلى)، يخفي جهاز الاتصال النفقي المصدر الفعلي للحزمة بشكل فعال. يمكن للنظير الموثوق به فقط تحديد المصدر الحقيقي، بعد أن يقوم بشطب الرأس الإضافي وفك تشفير الرأس الأصلي. كما هو مذكور في RFC 2401 ، "...كما أن الإفصاح عن الخصائص الخارجية للاتصالات يمكن أن يشكل مصدر قلق في بعض الظروف. سرية تدفق حركة المرور هي الخدمة التي تعالج هذا القلق الأخير من خلال إخفاء عناوين المصدر والوجهة أو طول الرسالة أو تكرار الاتصال. في سياق IPsec، يمكن أن يوفر إستخدام ESP في وضع النفق، وخاصة في عبارة الأمان، مستوى ما من سرية تدفق حركة المرور.تستخدم جميع بروتوكولات التشفير المدرجة هنا أيضا الاتصال النفقي كوسيلة لنقل البيانات المشفرة عبر الشبكة العامة. من المهم أن ندرك أن إنشاء قنوات الاتصال النفقي لا يوفر بحد ذاته أمانا للبيانات. تقتصر الحزمة الأصلية على التضمين داخل بروتوكول آخر وقد تظل مرئية باستخدام جهاز التقاط الحزم إذا لم يتم تشفيرها. غير أنه مذكور هنا لأنه جزء لا يتجزأ من كيفية عمل الشبكات الخاصة الظاهرية.يتطلب الاتصال النفقي ثلاثة بروتوكولات مختلفة.**بروتوكول الركاب** —البيانات الأصلية (IPX، NetBeui، IP) التي يتم نقلها.**بروتوكول التضمين**—البروتوكول (GRE، IPsec، L2F، PPTP، L2TP) الذي يتم تضمينه حول البيانات الأصلية.**بروتوكول الناقل**- البروتوكول المستخدم من قبل الشبكة التي تتنقل عليها المعلومات.يتم تضمين الحزمة الأصلية (بروتوكول الركاب) داخل بروتوكول التضمين، والذي يتم وضعه بعد ذلك داخل رأس بروتوكول الناقل (عادة IP) للبث عبر الشبكة العامة. لاحظ أن بروتوكول التضمين يقوم أيضا غالبا بتشفير البيانات. ويمكن نقل بروتوكولات مثل IPX و NetBeui، التي لا تنقل عادة عبر الإنترنت، بأمان وأمان.بالنسبة لشبكات VPN من موقع إلى موقع، يكون بروتوكول التضمين عادة IPsec أو تضمين التوجيه العام (GRE). تتضمن GRE معلومات حول نوع الحزمة التي تقوم بتغطيتها ومعلومات حول الاتصال بين العميل والخادم.بالنسبة للشبكات الخاصة الظاهرية (VPN) للوصول عن بعد، يتم إنشاء الاتصال النفقي عادة باستخدام بروتوكول الاتصال من نقطة إلى نقطة (PPP). جزء من مكدس PPP، TCP/IP هو حامل بروتوكولات IP الأخرى عند الاتصال عبر الشبكة بين الكمبيوتر المضيف والنظام البعيد. سيستخدم اتصال PPP النفقي أحد عمليات إعادة توجيه PPTP أو L2TP أو Cisco للطبقة 2 (L2F).
- **AAA**—يتم إستخدام المصادقة والتفويض والمحاسبة للوصول الآمن بشكل أكبر في بيئة شبكة VPN للوصول عن بعد. وبدون مصادقة المستخدم، يمكن لأي شخص يجلس على كمبيوتر محمول/كمبيوتر شخصي مزود ببرنامج عميل شبكة VPN مهيأ مسبقا إنشاء اتصال آمن بالشبكة البعيدة. ومع ذلك، بمصادقة المستخدم، يجب أيضا إدخال اسم مستخدم وكلمة مرور صحيحين قبل اكتمال الاتصال. يمكن تخزين أسماء المستخدمين وكلمات المرور على جهاز إنهاء شبكة VPN نفسه، أو على خادم AAA خارجي، والذي يمكنه توفير المصادقة لقواعد بيانات أخرى عديدة مثل Windows NT و Novell و LDAP وما إلى ذلك.عندما يأتي طلب إنشاء نفق من عميل طلب هاتفي، يطلب جهاز VPN اسم مستخدم وكلمة مرور. ويمكن بعد ذلك مصادقة هذا الإجراء محليا أو إرساله إلى خادم AAA الخارجي، والذي يتحقق من:من أنت (المصادقة)ما هو مسموح لك القيام به (التخويل)ما تقوم به في الواقع (المحاسبة)وتعتبر المعلومات المحاسبية مفيدة بوجه خاص لتعقب إستخدام العملاء لأغراض تدقيق الأمان أو إعداد الفواتير أو إعداد التقارير.
- **عدم التنكر** — في بعض عمليات نقل البيانات، وخصوصا تلك المتعلقة بالمعاملات المالية، يكون عدم التنصل ميزة مرغوب فيها جدا. وهذا مفيد في منع الحالات التي ينفي فيها طرف ما اشتراكه في معاملة ما. وكما يتطلب البنك توقيعك قبل إحترام شيك، فإن عدم التنصل يعمل بإرفاق توقيع رقمي بالرسالة المرسلة، وبالتالي إستبعاد إمكانية رفض المرسل المشاركة في الصفقة.

يوجد عدد من البروتوكولات التي يمكن إستخدامها لإنشاء حل شبكة VPN. توفر جميع هذه البروتوكولات مجموعة فرعية من الخدمات المدرجة في هذا المستند. يعتمد إختيار البروتوكول على مجموعة الخدمات المطلوبة. فعلى سبيل المثال، قد تكون المنظمة مرتاحة للبيانات التي يجري نقلها في نص واضح ولكنها تشعر بقلق بالغ إزاء الحفاظ على سلامتها، بينما قد تجد منظمة أخرى أن الحفاظ على سرية البيانات أمر ضروري للغاية. وبالتالي فإن إختيارها للبروتوكولات قد يكون مختلفا. لمزيد من المعلومات حول البروتوكولات المتاحة ونقاط قوتها النسبية، ارجع إلى أي حل للشبكات الخاصة الظاهرية (VPN) مناسب لك؟

منتجات الشبكات الخاصة الظاهرية (VPN)

استنادا إلى نوع شبكة VPN (الوصول عن بعد أو الوصول من موقع إلى موقع)، يلزمك وضع مكونات معينة لإنشاء شبكة VPN الخاصة بك. وقد تشمل هذه التدابير ما يلي:

- عميل برامج سطح المكتب لكل مستخدم بعيد
- أجهزة مخصصة مثل مركز Cisco VPN أو جدار حماية PIX الآمن من Cisco
- خادم شبكة VPN مخصص لخدمات الطلب الهاتفي
- خادم الوصول إلى الشبكة (NAS) الذي يستخدمه مزود الخدمة للوصول إلى VPN للمستخدم البعيد
- مركز إدارة الشبكات والسياسات الخاصة

نظرا لعدم وجود معيار مقبول على نطاق واسع لتنفيذ شبكة خاصة ظاهرية (VPN)، قامت العديد من الشركات بتطوير حلول حلول سهلة الاستخدام بشكل فردي. على سبيل المثال، توفر Cisco العديد من حلول شبكات VPN التي تتضمن:

- **مركز الشبكة الخاصة الظاهرية (VPN)** - بدمج أكثر تقنيات التشفير والمصادقة المتاحة تقدما، تم تصميم مركزات الشبكات الخاصة الظاهرية (VPN) من Cisco خصيصا لإنشاء شبكة خاصة ظاهرية (VPN) للوصول عن بعد أو من موقع إلى موقع، ويتم نشرها بشكل مثالي حيث يكون الاحتياج لجهاز واحد لمعالجة عدد كبير جدا من أنفاق الشبكات الخاصة الظاهرية (VPN). وقد تم تطوير مركز الشبكة الخاصة الظاهرية (VPN) خصيصا لتلبية متطلبات جهاز الشبكة الخاصة الظاهرية (VPN) مصمم لأغراض معينة ويمكن الوصول إليه عن بعد. وتوفر التركيزات درجة عالية من التوافر والأداء الفائق وقابلية التطوير وتتضمن مكونات تسمى وحدات معالجة التشفير القابل للتطوير (SEP) تمكن المستخدمين من زيادة السعة والإنتاجية بسهولة. يتم توفير أجهزة التجميع في نماذج مناسبة للشركات الصغيرة التي لديها 100 مستخدم للوصول عن بعد أو أقل إلى مؤسسات المؤسسات الكبيرة

التي يتوفر لديها ما يصل إلى 10000 مستخدم عن بعد في آن واحد.
- **الموجه/الموجه** المحسن **VPN الذي تم تمكين VPN به**—جميع موجهات Cisco التي تعمل ببرنامج Cisco IOS® دعم شبكات VPN IPsec. يتمثل المتطلب الوحيد في أنه يجب على الموجه تشغيل صورة برنامج Cisco IOS باستخدام مجموعة الميزات المناسبة. يدعم حل Cisco IOS VPN بالكامل متطلبات الشبكة الخاصة الظاهرية (VPN) الخاصة بالوصول عن بعد والإنترانت والإكسترانت. وهذا يعني أن موجهات Cisco يمكن أن تعمل بشكل متساو عند إتصالها بمضيف بعيد يشغل برنامج عميل VPN أو عند إتصالها بجهاز آخر لشبكة VPN مثل موجه أو جدار حماية PIX أو مركز VPN. تكون الموجهات التي تم تمكين VPN عليها مناسبة للشبكات الخاصة الظاهرية (VPN) التي تتطلب تشفيرا معتدلا ونفقي، وتوفر خدمات VPN بالكامل من خلال ميزات برنامج Cisco IOS. تتضمن أمثلة الموجهات التي تم تمكين VPN عليها السلسلة Cisco 1000 و Cisco 1600 و Cisco 2500 و Cisco 4000 و Cisco 4500 و Cisco 4700.توفر الموجهات المحسنة للشبكات الخاصة الظاهرية (VPN) من Cisco قابلية التطوير والتوجيه والأمان وجودة الخدمة (QoS). تستند الموجهات إلى برنامج Cisco IOS Software، وهناك جهاز مناسب لكل حالة، من الوصول إلى المكتب الصغير/المكتب المنزلي (SOHO) من خلال تجميع الشبكة الخاصة الظاهرية (VPN) للموقع المركزي إلى إحتياجات المؤسسات الكبيرة. تم تصميم الموجهات المحسنة للشبكات الخاصة الظاهرية (VPN) لتلبية متطلبات التشفير العالي والاتصال النفقي، وغالبا ما تستخدم أجهزة إضافية مثل بطاقات التشفير لتحقيق أداء فائق. تتضمن أمثلة الموجهات المحسنة الخاصة بشبكة VPN سلسلة Cisco 800 و Cisco 1700 و Cisco 2600 و Cisco 3600 و Cisco7200 و

Cisco7500.

- **جدار حماية PIX الآمن من Cisco** — يجمع جدار الحماية الخاص بتقنية Internet Xchange (المعروفة بالاختصار PIX) بين ترجمة عنوان الشبكة الديناميكي وخادم الوكيل وترشيح الحزم وجدار الحماية وإمكانات الشبكة الخاصة الظاهرية (VPN) في قطعة واحدة من الجهاز. بدلا من إستخدام برنامج Cisco IOS، يحتوي هذا الجهاز على نظام تشغيل مبسط بدرجة كبيرة يبدل القدرة على معالجة مجموعة متنوعة من البروتوكولات لتوفير القوة الفائقة والأداء الفائق من خلال التركيز على بروتوكول الإنترنت (IP). كما هو الحال مع موجهات Cisco، تدعم جميع طرز جدار حماية PIX شبكة VPN IPsec. كل ما هو مطلوب هو تلبية متطلبات الترخيص لتمكين

ميزة VPN.

- **الوحدات العميلة للشبكات الخاصة الظاهرية (VPN) من Cisco**—توفر Cisco كلا من الأجهزة والبرامج الشبكات الخاصة الظاهرية (VPN). يأتي عميل (البرنامج) شبكة VPN من Cisco مزودا بمركز Cisco VPN 3000 Series Concentrator دون أي تكلفة إضافية. يمكن تثبيت عميل البرنامج هذا على الجهاز المضيف واستخدامه للاتصال بشكل آمن بمركز الموقع المركزي (أو بأي جهاز آخر لشبكة VPN مثل الموجه أو جدار الحماية). ال VPN 3002 جهاز زبون خيار أن ينشر ال VPN زبون برمجية على كل جهاز ويزود VPN توصيل إلى عدة أداة.

إن إختيار الأجهزة التي ستستخدمها لإنشاء حل الشبكة الخاصة الظاهرية (VPN) لديك هو في نهاية المطاف مشكلة في التصميم تعتمد على عدد من العوامل، بما في ذلك الإنتاجية المطلوبة وعدد المستخدمين. على سبيل المثال، في موقع بعيد مزود بعدد قليل من المستخدمين وراء الطراز PIX 501، يمكنك التفكير في تكوين الطراز PIX الحالي كنقطة نهاية للشبكة الخاصة الظاهرية (VPN) لبروتوكول IPsec، شريطة قبول سعة المعالجة ثلاثية الأبعاد الخاصة بالطراز 501 بمعدل نقل بيانات يبلغ 3 ميجابت في الثانية تقريبا والحد الأقصى الذي يبلغ 5 نظراء للشبكة الخاصة الظاهرية (VPN). ومن ناحية أخرى، قد يكون الذهاب إلى موقع مركزي يعمل كنقطة نهاية للشبكة الخاصة الظاهرية (VPN) لعدد كبير من أنفاق الشبكة الخاصة الظاهرية (VPN) للحصول على موجه مثالي للشبكة الخاصة الظاهرية (VPN) أو مركز الشبكة الخاصة الظاهرية (VPN) فكرة جيدة. ويعتمد الاختيار الآن على النوع (شبكة LAN إلى شبكة LAN أو الوصول عن بعد) وعدد أنفاق شبكات VPN التي يتم إعدادها. توفر المجموعة الواسعة من أجهزة Cisco التي تدعم الشبكة الخاصة الظاهرية (VPN) لمصممي الشبكة قدرا كبيرا من المرونة وحلا قويا لتلبية جميع إحتياجات التصميم.

معلومات ذات صلة

- يفهم VPDN
- الشبكات الخاصة الظاهرية (VPN)
- صفحة دعم مركزات Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000
- مفاوضة IPsec/صفحة دعم بروتوكول IKE
- صفحة دعم جدران الحماية من السلسلة PIX 500

- المعيار RFC 1661: بروتوكول الاتصال من نقطة إلى نقطة (PPP)
- المعيار RFC 2661: بروتوكول الاتصال النفقي للطبقة الثانية "L2TP"
- كيف تعمل الأشياء: كيف تعمل الشبكات الافتراضية الخاصة
- نظرة عامة على شبكات VPN
- صفحة الشبكة الخاصة الظاهرية (VPN) الخاصة بتوم دونيغان
- إتحاد الشبكات الخاصة الظاهرية
- طلبات التعليقات (RFCs)
- 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).