Fonctionnement des réseaux VPN

Contenu

Introduction

Ce document couvre les bases des vpn, telles que les composants de VPN, les technologies, le tunneling et la sécurité de base de VPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

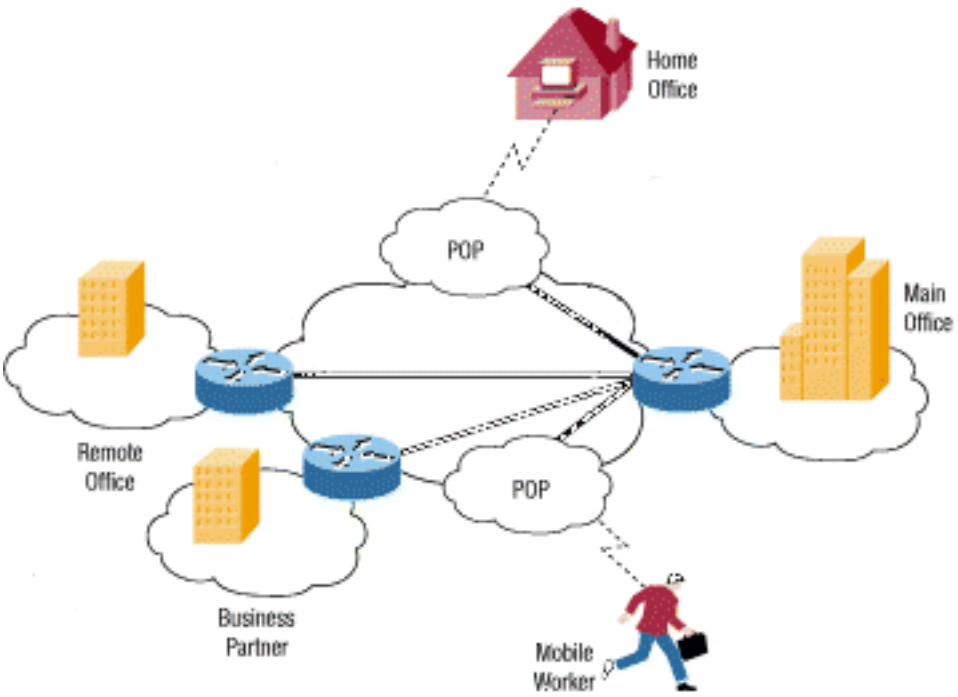
Informations générales

Le monde a beaucoup changé ces dernières décennies. Au lieu de traiter simplement des problématiques locales ou régionales, beaucoup d'entreprises maintenant doivent penser aux marchés globaux avec un système logistique mondial. Beaucoup de sociétés ont déployé leurs lieux d'activités à travers le pays, ou même autour du monde. Mais il y a une chose dont toutes les

sociétés ont besoin : une façon d'assurer la communication rapide, sécurisée et fiable partout où leurs bureaux se trouvent.

Jusqu'à récemment, la communication fiable signifiait l'utilisation des lignes louées pour les réseaux étendus (WAN). Les lignes louées, s'étendant d'Integrated Services Digital Network (le RNIS, qui fonctionne à 144 Kbps) (OC3, qui fonctionne à 155 Mbits/s) à la ligne de fibres optiques Carrier-3, permettent à une société de développer leur réseau privé au-delà de leur zone géographique immédiate. UN WAN a des avantages évidents par rapport à un réseau public, comme Internet quand il s'agit de fiabilité, performances et la sécurité ; mais la mise à jour d'un WAN, en particulier en utilisant des lignes louées, peut devenir tout à fait chère (il y a souvent une augmentations du coût quand la distance entre les bureaux s'accroît). En outre, les lignes louées ne sont pas une solution viable pour des organismes où une partie de la main-d'œuvre est fortement mobile (comme cela est le cas pour le personnel de vente) et devrait fréquemment se reconnecter au réseau de l'entreprise à distance et accéder des données sensibles.

Alors que la popularité d'Internet s'est développée, les entreprises s'en sont servi vers lui afin de développer leurs propres réseaux. D'abord via les intranets, des sites conçus à l'usage par des employés de l'entreprise seulement. Maintenant, beaucoup de sociétés créent leurs propres réseaux virtuels (VPN) pour satisfaire aux besoins des collaborateurs et bureaux distants.



Un VPN typique pourrait avoir un réseau local principal (LAN) au siège social d'une société, d'autres LAN aux bureaux et installations distants et des utilisateurs individuels qui se connectent de l'extérieur.

UN VPN est un réseau privé qui fait appel à un réseau public (habituellement l'Internet) pour connecter des sites ou des utilisateurs distants. Au lieu d'utiliser une connexion dédiée et réel, telle que la ligne louée, un VPN utilise les connexions « virtuelles à travers Internet à partir du réseau privé de la société au site distant ou à l'employé.

Que fait un VPN ?

Il y a deux types communs de VPN.

- **Accès à distance** - Egalement appelé un réseau commuté de connexion privée virtuelle (VPDN), ceci est une connexion d'utilisateur-à-LAN utilisée par une société avec des employés qui doivent se connecter au réseau privé de divers sites distants. Typiquement, une société qui souhaite installer un grand VPN d'accès à distance fournit une forme de compte commuté Internet à ses utilisateurs moyennant un fournisseur de services Internet (FOURNISSEUR D'ACCÈS INTERNET). Les télétravailleurs peuvent alors composer un numéro 1-800 pour atteindre Internet et pour employer leur logiciel client VPN pour accéder au réseau de l'entreprise. Un bon exemple d'une société qui a besoin d'un VPN d'accès à distance serait une grande entreprise avec des centaines de vendeurs actifs à l'extérieur. Le VPN d'accès à distance permet des connexions sûres et cryptées entre le réseau privé d'une société et les utilisateurs distants en passant par un fournisseur de services.
- **Site à site** - Par l'intermédiaire du chiffrement dédié de matériel et du cryptage à grande échelle, une société peut relier les sites multiples dans un réseau public tel que l'Internet. Il suffit pour chaque site d'établir d'une connexion locale au même réseau public, ce qui signifie une économie par rapport aux longues lignes privées louées. Les VPN de site à site peuvent être encore classés par catégorie dans des intranets ou des extranets. Un VPN site à site entre les bureaux de la même société est un VPN d'intranet, alors qu'un VPN construit pour relier la société à son partenaire ou client est connu sous le nom d'un VPN d'extranet.

Une société bénéficiera considérablement d'un VPN bien conçu. Par exemple, elle peut :

- Etendre la connectivité géographique
- Réduction des coûts par rapport aux WAN traditionnels
- Réduction du temps de transit et des frais de déplacement pour des utilisateurs distants
- Amélioration de la productivité
- Topologie du réseau simplifiée
- Possibilité de construire un réseau global
- Possibilité de fournir un support de télétravailleur
- Retour sur l'investissement plus rapide que le WAN traditionnel

Quelles fonctionnalités sont nécessaires pour un VPN bien conçu ? Il devrait incorporer les éléments suivants :

- Sécurité
- Fiabilité
- Évolutivité
- Gestion de réseau CSNA
- Gestion des stratégies

Analogie : Chaque LAN est une île

Imaginez que vous viviez sur une île dans un océan énorme. Il y a des milliers d'autres îles tout autour de vous, dont certaines très proches et d'autres plus loin. La façon normale de voyager est de prendre une navette de votre île à une autre île vous souhaitez visiter. Le déplacement sur une navette signifie que vous n'aurez presqu'aucune confidentialité. Tout ce que vous faites peut être vu par quelqu'un d'autre.

Supposez que chaque île représente un local privé et que l'océan est l'Internet. Quand vous voyagez en navette, c'est comme si vous vous connectez à un serveur eb ou à un autre périphérique par Internet. Vous n'avez aucun contrôle des fils et routeurs qui composent l'Internet,

tout comme vous n'avez aucun contrôle en ce qui concerne les autres personnes sur le bateau. Ceci vous laisse vulnérable aux problèmes de sécurité si vous essayez de vous connecter entre deux réseaux privés utilisant une ressource publique.

Votre île décide de construire un pont à une autre île de sorte qu'il y ait un moyen plus facile, plus sécurisé et plus direct pour que les personnes voyagent entre les deux. Il est cher de construire et mettre à jour le pont, même si l'île à laquelle vous vous connectez soit très proche. Mais le besoin d'un chemin fiable et sûr est si grand que vous le faites de toute façon. Votre île voudrait se connecter à une deuxième île, beaucoup plus loin, mais vous décidez que cela est trop cher.

Cette situation ressemble à la solution d'une ligne louée. Les ponts (lignes louées) sont séparés de l'océan (Internet), mais ils peuvent connecter les îles (LAN). Beaucoup de sociétés ont choisi cette route en raison du besoin de fiabilité et de sécurité en connectant leurs bureaux distants. Cependant, si les bureaux sont très éloignés, le coût peut être prohibitif, comme si on construisait un pont qui à une très grande distance.

Alors comment fonctionne le VPN selon cette analogie ? Nous pourrions donner à chaque habitant de nos îles leur propre petit sous-marin avec ces propriétés.

- Il est rapide.
- Il est facile à prendre avec vous partout où vous allez.
- Il peut vous masquer complètement de tous les autres bateaux ou sous-marins.
- Il est fiable.
- Il coûte peu d'ajouter des sous-marins supplémentaires à votre flotte une fois que le premier est acheté.

Bien qu'ils voyagent dans l'océan en même temps que les autres bateaux, les habitants de nos deux îles peuvent voyager dans les deux sens comme ils veulent en toute sécurité et confidentialité. C'est essentiellement comment un VPN fonctionne. Chaque membre distant de votre réseau peut communiquer d'une manière sécurisée et fiable en utilisant Internet comme support à se connecter au LAN privé. UN VPN peut se développer afin de permettre de relier plus d'utilisateurs et d'endroits différents beaucoup plus facilement qu'un ligne louée. En fait, l'évolutivité est un principal avantage que les VPN ont par rapport aux lignes louées typiques. À la différence entre les lignes louées où le coût augmente proportionnellement aux distances impliquées, les situations géographiques de chaque site ont peu d'importance pour la création d'un VPN.

Technologies VPN

Un VPN bien conçu emploie plusieurs méthodes afin de maintenir votre connexion et données sécurisées.

- **Confidentialité des données** - C'est peut-être le service le plus important fourni par n'importe quelle implémentation de VPN. Puisque vos données privées voyagent dans un réseau public, la confidentialité des données est essentielle et elle peut être garantie en chiffrant les données. Ce processus consiste à prendre toutes les données qu'un ordinateur envoie à l'autre et à les coder les sous une forme que seulement l'autre ordinateur pourra décoder.La plupart des VPN emploient un de ces protocoles pour réaliser le cryptage.**IPsec** - Le protocole d'IPSec (IPsec) offre des fonctionnalités de sécurité étendue telles que des algorithmes de cryptage puissants et une authentification plus complète. IPsec a deux modes de cryptage : tunnel et transport. Le mode tunnel crypte l'en-tête et les données utiles de chaque paquet,

tandis que le mode de transport crypte seulement les données utiles. Seulement les systèmes qui sont IPsec-conformes peuvent tirer profit de ce protocole. En outre, tous les périphériques doivent utiliser une clé ou certificat commun et une configuration très semblable de stratégies de sécurisation.Pour des utilisateurs VPN d'accès à distance, une certaine forme de package de logiciel vendu par un tiers indépendant fournit la connexion et le cryptage sur le PC d'utilisateur. IPsec prend en charge le cryptage 56-bit (DES simple) ou 168-bit (algorithme triple-DES).**PPTP/MPPE** - PPTP a été créé par le forum PPTP, un consortium qui réunit US Robotics, Microsoft, 3COM, Ascend et ECI Telematics. PPTP prend en charge des VPN multiprotocole, avec le cryptage 40-bit et 128-bit utilisant un protocole appelé cryptage point par point de Microsoft (MPPE simultané). Il est important de noter que PPTP par lui-même ne fournit pas le cryptage des données.**L2TP/IPsec** - Généralement appelé L2TP over IPsec, ceci fournit la sécurité du protocole IPsec sur le tunneling du protocole Layer (L2TP). L2TP est le produit d'un partenariat entre les membres du forum PPTP, Cisco et l'Internet Engineering Task Force (IETF). Il est principalement utilisé pour des VPN d'accès à distance avec des systèmes d'exploitation Windows 2000, puisque le Windows 2000 fournit un client indigène d'IPsec et L2TP. Les fournisseurs de services Internet peuvent également fournir des connexions L2TP pour des utilisateurs en accès entrant, puis crypter ce trafic avec IPsec entre leur point d'access et le serveur de réseau de bureau distant.

- **Intégrité** - Tandis qu'il est important que vos données soient cryptées dans un réseau public, il est tout aussi important de vérifier qu'elles n'ont pas été modifiées en transit. Par exemple, IPsec a un mécanisme pour garantir que la partie cryptée du paquet, ou l'en-tête et la partie "données" entiers du paquet, n'ont pas été altérés. Si une altération est détectée, le paquet est déposé. L'intégrité peut également impliquer l'authentification de l'homologue distant.
- **Authentification de l'origine des données** - Il est extrêmement important de vérifier l'identité de la source de données qui sont envoyées. C'est nécessaire pour garder contre un certain nombre d'attaques qui dépendent d'usurper l'identité de l'expéditeur.
- **Anti rediffusion** - C'est la capacité de la détecter et rejeter les paquets rejoués et les aides empêchez usurper.
- **Données de tunneling/confidentialité de flux de trafic** - le tunneling est le processus d'encapsuler un paquet entier dans un autre paquet et de l'envoyer sur un réseau. Le tunneling de données est utile dans les cas où il est souhaitable de masquer l'identité du périphérique lançant le trafic. Par exemple, qui utilise un IPsec à un dispositif encapsule le trafic qui appartient à un certain nombre d'hôtes derrière lui et ajoute son propre en-tête sur les paquets existants. En cryptant le paquet original et l'en-tête (et en conduisant le paquet en fonction sur l'en-tête supplémentaire de couche 3 ajouté sur le dessus), le périphérique tunnel masque efficacement la source réelle du paquet. Seulement l'homologue de confiance peut déterminer la véritable source, après qu'il élimine l'en-tête supplémentaire et décrypte l'en-tête original. Comme observé dans RFC 2401 , « … la divulgation des caractéristiques externes de transmission peut également être une préoccupation dans certaines circonstances. La confidentialité de flux de trafic est le service qui aborde cette dernière préoccupation en cachant des adresses d'origine et de destination, la longueur de message, ou la fréquence de transmission. Dans le contexte d'IPsec, utilisant l'ESP dans le tunnel mode, particulièrement à un modem routeur de sécurité, peut fournir un certain niveau de confidentialité de flux de trafic. »Tous les protocoles de chiffrement listés ici utilisent également percer un tunnel en tant que des moyens de transférer les données cryptées à travers le réseau public. Il est important de se rendre compte que le tunneling, par lui-même, ne fournit pas la sécurité des données. Le paquet original est simplement encapsulé à l'intérieur d'un autre protocole et pourrait être toujours visible avec un périphérique de paquet-saisie sinon chiffré. On lui

mentionne ici, cependant, puisque c'est une partie intégrale de la façon dont les VPN fonctionnent.Le Tunneling requiert trois différents protocoles.**Protocole passager** - Les données originales (ROUTAGE IPX, NetBeui, IP) qui sont portées.**Encapsulant le protocole** - Le protocole (GRE, IPsec, L2F, PPTP, L2TP) enroulé autour des données originales.**Protocole d'opérateur** - Le protocole utilisé par le réseau sur lequel les informations voyagent.Le paquet original (protocole passager) est encapsulé dans le protocole encapsulant, qui est alors mis à l'intérieur de l'en-tête d'opérateur (habituellement IP) pour la transmission dans réseau public. Notez que le protocole encapsulant effectue également souvent le cryptage des données. Des protocoles tels que le ROUTAGE IPX et le NetBeui, qui ne seraient pas normalement transférés à travers Internet, peuvent être transmis en toute sécurité.Pour des VPN site à site, le protocole encapsulant est habituellement IPsec ou GRE (GRE). GRE inclut les informations sur le type de paquet encapsulé et les informations sur la connexion entre client et serveur.Pour des VPN d'accès à distance, la transmission tunnel a lieu normalement utilisant le protocole point à point (PPP). Une partie de la pile TCP/IP, PPP est l'opérateur pour d'autres protocoles d'IP pour la communication dans le réseau entre l'ordinateur hôte et un système distant. Le tunneling de PPP utilisera un transfert PPTP, L2TP ou Cisco de couche 2 (L2F).

- **AAA** — L'authentification, l'autorisation et la comptabilité sont utilisées pour un accès plus sécurisé dans un environnement VPN d'accès à distance. Sans vérification de l'ID de l'utilisateur, n'importe qui s'assied à un laptop/PC avec le logiciel client VPN pré-configuré peut établir une connexion sécurisée dans le réseau distant. Avec la vérification de l'ID de l'utilisateur cependant, un nom d'utilisateur valide et un mot de passe doivent également être entrés avant que la connexion soit complétée. Un nom d'utilisateur et un mot de passe peuvent être enregistrés sur l'équipement de terminaison de VPN lui-même, ou sur un serveur AAA externe, qui peut fournir l'authentification à nombreuses bases de données telles que Windows NT, Novell Routing, LDAP et ainsi de suite.Quand une demande d'établir un tunnel est disponible d'un client RTC, le périphérique VPN invite à saisir un nom d'utilisateur et un mot de passe. Ceci peut alors être authentifié localement ou envoyé au serveur AAA externe, qui vérifie :Qui vous êtes (authentification)Ce que vous êtes permis pour faire (autorisation)Ce que vous faites réellement (gestion des comptes)L'information de comptabilisation est particulièrement utile pour suivre l'utilisation de client pour la sécurité auditant, affichant ou signalant des raisons.
- **Non-répudiation** - Dans certains transferts des données, particulièrement ceux ont associé aux transactions financières, non-répudiation est une fonctionnalité fortement souhaitable. C'est utile pour empêcher des situations où un côté nie ayant participé à une transaction. Tout comme une banque requiert votre signature avant d'honorer votre contrôle, des travaux de non-répudiation en attachant une signature numérique à l'envoyé message, de ce fait excluant la possibilité d'expéditeur refusant la participation à la transaction.

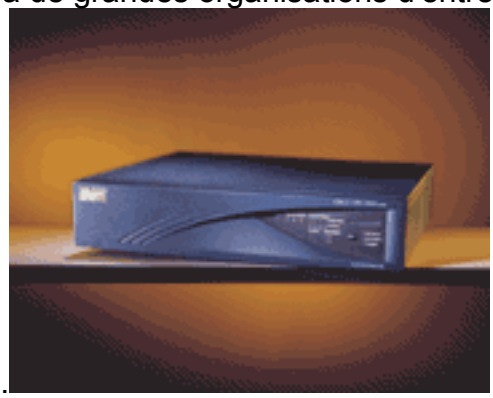
Un certain nombre de protocoles existent qui peuvent être utilisés pour établir des solutions VPN. Tous ces protocoles fournissent un certain sous-ensemble des services listés dans ce document. Le choix d'un protocole dépend de l'ensemble de services désirés. Par exemple, une organisation pourrait être confortable avec les données étant transférées en texte en clair mais très préoccupées au sujet de mettre à jour son intégrité, alors qu'une autre organisation pourrait rechercher la confidentialité des données de mise à jour absolument essentielle. Leur choix des protocoles pourrait être ainsi différent. Pour plus d'informations sur les protocoles disponibles et leurs forces relatives, consultez la section Quelles solutions VPN sont correctes pour vous ?

Produits VPN

Basé sur le type de VPN (accès à distance ou site à site), vous devez mettre certains composants en place pour construire votre VPN. Ceux-ci pourraient inclure :

- Client de logiciel de bureau pour chaque utilisateur distant
- Matériel dédié tel qu'un concentrateur de Cisco VPN ou un Cisco Secure PIX Firewall
- Serveur VPN dédié pour des services RTC
- Serveur d'accès au réseau (NAS) utilisé par le fournisseur de service pour l'accès VPN d'utilisateur distant
- Centre de réseau privé et de gestion des stratégies

Puisqu'il n'y a aucune norme largement acceptée pour mettre en application un VPN, beaucoup de sociétés ont développé les solutions "clés en main" par leurs propres moyens. Par exemple, Cisco offre plusieurs solutions VPN qui incluent :

- Concentrateur VPN - Incorporant la plupart des techniques de cryptage avancé et d'authentification disponibles, des concentrateurs de Cisco VPN sont construits spécifiquement pour créer un accès à distance ou un VPN site à site et sont déployés idéalement là, où la condition requise est qu'un périphérique prenne en charge un très grand nombre de tunnels VPN. Le concentrateur VPN a été spécifiquement développé pour adresser la condition requise pour un VPN d'accès à distance spécifique, périphérique. Les concentrateurs fournissent une haute disponibilité, de hautes performances et l'évolutivité et incluent des composants, appelés modules de cryptage évolutif (SEPT) qui permettent à des utilisateurs d'augmenter facilement la capacité et le débit. Les concentrateurs sont offerts dans les modèles appropriés aux petites entreprises avec 100 ou moins d'utilisateurs d'accès à distance à de grandes organisations d'entreprise avec jusqu'à 10.000 utilisateurs distants simultanés. 
- **Router/VPN-Optimized des Vpn-Activer** - Tous les routeurs Cisco qui exécutent des VPN IPSec de prise en charge du logiciel de Cisco IOS®. La seule condition requise est que le routeur doit exécuter une image Cisco IOS avec le jeu de fonctionnalités approprié. Les solutions VPN de Cisco IOS approuvent pleinement des conditions requises de VPN d'accès à distance, d'intranet et d'extranet. Ceci signifie que les routeurs Cisco peuvent travailler aussi bien une fois connectés à un logiciel client VPN courant d'hôte distant que connectés à un autre périphérique VPN tel qu'un routeur, un pare-feu PIX ou un concentrateur VPN. Les routeurs de VPN sont appropriés pour des VPN avec le cryptage modéré et des conditions requises de transmission tunnel et fournissent des services VPN entièrement par des fonctionnalités logicielles de Cisco IOS. Les exemples des routeurs de VPN incluent les gammes Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 et Cisco 4700.Les routeurs des VPN optimisés Cisco fournissent l'évolutivité, le routage, la sécurité et la qualité de service (QoS). Les routeurs sont basés sur le logiciel Cisco IOS et il y a un périphérique approprié à chaque situation, de l'accès de small-office/accueil-office (SOHO) par l'agrégation de VPN de site central aux besoins d'une grande entreprise. Les routeurs optimisés VPN sont

conçus pour répondre au cryptage élevé et aux conditions requises de tunneling et se servent souvent du matériel supplémentaire tel que des cartes de cryptage pour réaliser des hautes performances. Les exemples des routeurs optimisés VPN incluent Cisco 800, Cisco 1700, Cisco 2600, Cisco 3600, Cisco7200, la série

Cisco7500.

- Cisco Secure PIX Firewall - Le pare-feu privé Internet eXchange (PIX) combine la traduction d'adresses de réseau dynamique, le serveur proxy, la filtration de paquet, le pare-feu et les fonctionnalités VPN dans un seul paquet. Au lieu d'utiliser le logiciel Cisco IOS, ce périphérique a un système d'exploitation fortement profilé échangeant la capacité de prendre en charge un grand choix de protocoles pour la robustesse et les performances extrêmes en se concentrant sur l'IP. Comme avec des routeurs Cisco, tous les modèles de pare-feu PIX prennent en charge le VPN IPSec. Tout ce qui est requis est que les exigences d'accorder une licence d'activer la fonction VPN doivent être

réalisées.

- **Clients VPN Cisco** - Cisco offre clients VPN matériels et logiciels. Le Client VPN Cisco (logiciel) est livré groupé avec le concentrateur de la série Cisco VPN 3000 à aucun coût supplémentaire. Ce client logiciel peut être installé sur l'ordinateur hôte et être utilisé pour se connecter sécurisé au concentrateur de site central (ou à tout autre périphérique VPN un tel routeur ou pare-feu). Le client matériel du VPN 3002 est une alternative au déploiement du logiciel client VPN sur chaque machine et fournit la connectivité VPN à un certain nombre de périphériques.

Le choix des périphériques que vous aviez l'habitude d'utiliser pour établir vos solutions VPN est finalement un problème de conception qui dépend d'un certain nombre de facteurs, y compris le débit désiré et le nombre d'utilisateurs. Par exemple, sur un site distant avec quelques utilisateurs derrière un PIX 501, vous pourriez envisager de configurer le PIX existant comme point final de VPN IPSec, à condition que vous acceptiez le débit 3DES de 501 d'approximativement 3 Mbits/s et la limite d'un maximum de 5 homologues VPN. D'autre part, sur un site central agir en tant que point terminal VPN pour un grand nombre de tunnels VPN, allant vers un routeur optimisé VPN ou un concentrateur optimisé VPN serait probablement une bonne idée. Le choix dépendrait maintenant du type (LAN à LAN ou accès à distance) et du nombre de tunnels VPN étant installés. Le large éventail de périphériques Cisco qui prennent en charge le VPN offre aux concepteurs du réseau beaucoup de souplesse et une solution robuste correspondant à chaque besoin de conception.

Informations connexes

- Présentation de VPDN
- Réseau privé virtuel (VPNs)
- Page de support pour Concentrateurs VPN Cisco 3000
- Page de support pour le Client Cisco VPN 3000
- Page de support pour Protocole IKE/Négociation IPsec
- Page d'assistance de pare-feu PIX 500 Series
- RFC 1661 : Le Protocole point à point (PPP)
- RFC 2661 : Protocole de canalisation en tunnel "L2TP" de la couche deux
- Comment la substance fonctionne : Fonctionnement des réseaux VPN
- Présentation des VPN
- Page de VPN de Tom Dunigan
- Consortium de réseau virtuel (VPN)
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems