SOLUTION CISCO DE RÉSEAUX PRIVÉS VIRTUELS IPSEC COMPATIBLES VOIX ET VIDÉO

Réaliser des réseaux privés virtuels IPSec multiservices de haute qualité

Les réseaux privés virtuels (VPN) sont une solution économique et particulièrement souple pour remplacer ou élargir les réseaux privés dédiés utilisant des lignes louées, Frame Relay ou le mode de transmission asynchrone (ATM). Les VPN permettent aux entreprises de réaliser des économies considérables sur leurs réseaux de données en passant par des réseaux partagés protégés par des tunnels VPN cryptés. Toutefois, la tendance actuelle est aux réseaux convergents, ce qui impose de nouvelles contraintes sur les VPN. Grâce aux VPN compatibles voix et vidéo (V^3PN : voice and video-enabled VPN) que fournit Cisco, l'entreprise peut ajouter des transmissions voix et vidéo par VPN à son réseau de données sans compromettre ni sa qualité, ni sa fiabilité, et pour un coût très compétitif.

Les solutions V^3PN Cisco intègrent la connectivité économique et sécurisée offerte par les VPN de site à site grâce à l'architecture AVVID qui permet la transmission convergente de la voix, de la vidéo et des données sur les réseaux IP. Les V^3PN assurent une connectivité distante souple et à faible coût tout en fournissant une infrastructure réseau qui supporte les applications de réseau convergent les plus récentes comme la téléphonie IP et la vidéo.

Les solutions V^3PN Cisco offrent des avantages majeurs, et notamment :

- La connectivité économique voix, vidéo et données sur des sites géographiquement dispersés – Nos utilisateurs peuvent exploiter les capacités multiservices des V^3PN pour connecter des environnements de bureaux décentralisés comme des bureaux distants ou à domicile, avec leur propre extension PBX. De plus, le système permet à l'entreprise d'assurer des formations vidéo et de tirer profit sur ces sites des économies offertes par les applications de messagerie unifiée afin de réduire leurs frais d'exploitation.
- L'infrastructure VPN pour les applications modernes – Les V^3PN fournissent une infrastructure VPN capable de transporter le trafic convergent voix, vidéo et données sur un réseau sécurisé IPSec. A la différence de nombreux équipements VPN sur le marché, les plates-formes VPN Cisco s'adaptent aux différentes topologies de réseau et aux types de trafic caractéristiques des VPN IPSec multiservices, et garantissent ainsi que l'infrastructure VPN ne perturbe pas les applications multiservices déployées maintenant ou à l'avenir.
- L'architecture de réseau de bout en bout – Cisco fournit des produits pour tous les éléments des VPN multiservices, depuis les routeurs VPN Cisco exécutant la plate-forme logicielle Cisco IOS® jusqu'à Cisco CallManager et aux téléphones IP. De plus, grâce à l'architecture Cisco AVVID (Architecture for Voice, Video and Integrated Data) pour la création de réseaux convergents et au schéma directeur SAFE de sécurité des réseaux VPN, Cisco propose un modèle global de déploiement de ses produits. Ces modèles de déploiement garantissent une solution de réseau sécurisée, interopérable et fiable avec une prise en charge produit de bout en bout.
- La sécurisation de l'ensemble du réseau multiservice – les solutions de sécurité de réseau Cisco vont bien au-delà du cryptage du trafic multiservice sur le VPN ; elles garantissent également l'interconnexion compatible avec les pare-feu Cisco PIX qui assurent la sécurité périmétrique, et avec le système Cisco IDS de détection des intrusions qui protège le réseau contre les attaques extérieures.

- Nos partenaires fournisseurs de services – Les fournisseurs de services fournissent la bande passante nécessaire aux VPN. Le programme Cisco Powered Network permet aux entreprises de sélectionner les fournisseurs de services capables de fournir le tissu de réseau à faible temps de latence indispensable pour la transmission de la voix et de la vidéo haute qualité sur le VPN, ou encore d'opter pour des services V^{3}PN entièrement gérés.

Les technologies qui sous-tendent le V^{3}PN

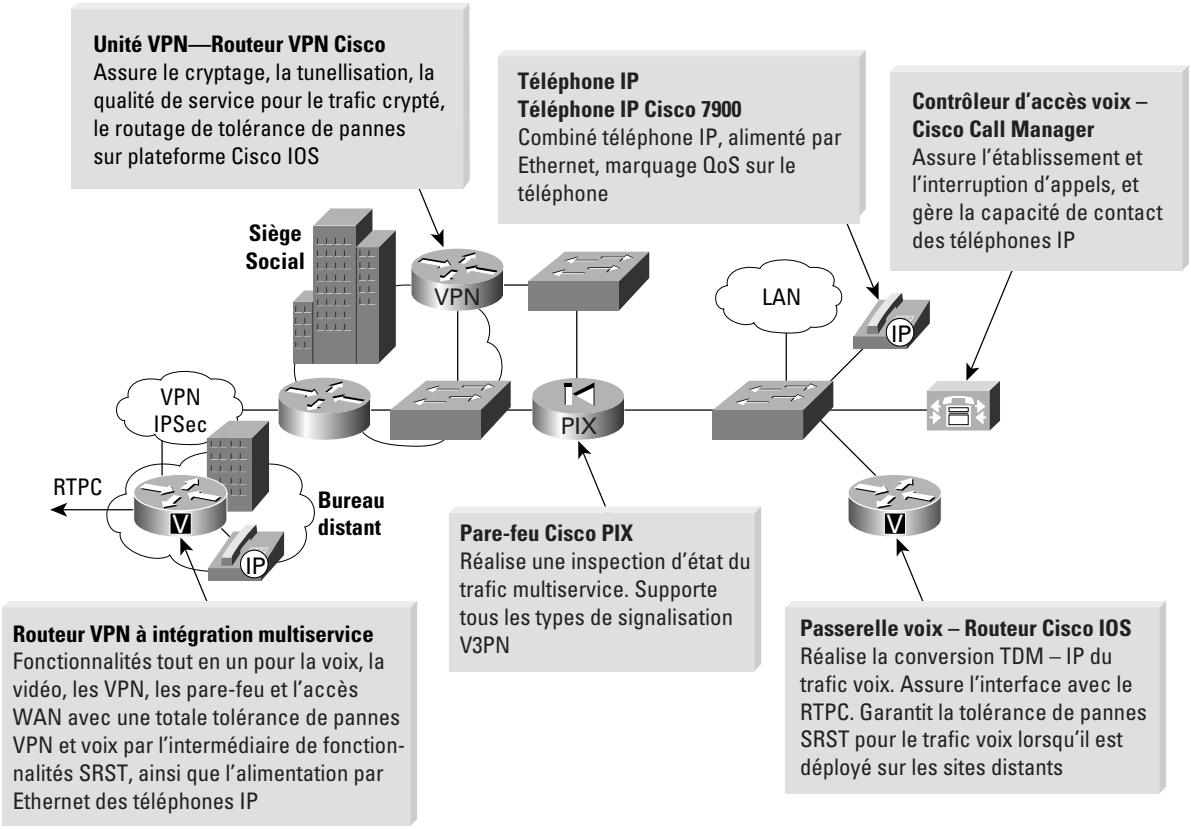
Le cœur d'une solution V^{3}PN Cisco est un routeur VPN Cisco qui exécute la plate-forme logicielle Cisco IOS. L'établissement de VPN IPSec voix et données de haute qualité exige beaucoup plus que la simple capacité à crypter le trafic – il faut pouvoir disposer d'un ensemble harmonisé de technologies multiservices et VPN IPSec évoluées. Les principales technologies de la plate-forme logicielle Cisco IOS qui permettent la mise en œuvre des V^{3}PN Cisco sont les suivantes :

- Qualité de service (QoS) centrée sur le multiservice – Pour fournir des services voix et vidéo de haute qualité, la qualité de service doit pouvoir s'étendre à la qualité du transport de bout en bout. La gestion des files d'attente à faible temps de latence est un facteur essentiel pour attribuer des priorités au trafic multiservice et fournir la bande passante spécifique et les garanties de latence. Cisco offre des fonctionnalités complètes de gestion de files d'attente à faible temps de latence, y compris des fonctions spécifiques de cryptage du trafic voix et vidéo qui traverse le VPN. De plus, les fonctions QoS Cisco – comme le formatage de trafic qui garantit la qualité du débit sur les liaisons asymétriques et la fragmentation et l'entrelacement des liaisons (LFI) qui contrôle la gigue en présence de transmissions de paquets volumineux comme avec FTP – sont des éléments critiques qui garantissent la qualité des transmissions voix et vidéo sur les VPN.
- Prise en charge de divers types de trafic – le trafic voix et vidéo IP, comme les intercoms «Hoot and Holler» ou l'attente musicale, exigent la prise en charge de trafic multicast sur le VPN. Bien que IPSec soit un protocole unicast, les routeurs VPN Cisco qui exécutent la plate-forme logicielle Cisco IOS peuvent gérer le trafic multicast et garantir que l'infrastructure VPN n'altère pas les applications multiservices.
- Prise en charge des topologies de réseau multiservice – Le trafic multiservice est sensible aux délais et les topologies de réseau doivent souvent être adaptées pour réduire les sauts de réseau et minimiser les temps de latence. Les routeurs VPN Cisco définissent la norme en matière de souplesse topologique pour la conception de réseaux en s'adaptant à des topologies qui dépassent le stade élémentaire du réseau en étoile pour prendre en charge des réseaux hiérarchiques entièrement maillés. De plus, les routeurs VPN Cisco disposent de fonctions logicielles intégrées comme les VPN multipoints dynamiques qui réalisent le dimensionnement automatisé dynamique des réseaux maillés pour en faciliter le déploiement.
- Fonctionnalités évoluées de reprise réseau – La solution V^{3}PN Cisco offre une tolérance de pannes complète qui gère aussi bien le transport réseau VPN que le réseau de téléphonie IP. Les fonctionnalités complètes de couche 3 pour le routage et les VPN à inspection d'état des routeurs VPN Cisco offrent une robustesse de réseau qui dépasse celles des unités VPN et s'étend jusqu'à l'hôte réseau, et élimine par conséquent les trous noirs. Les fonctionnalités SRST (Survivable Remote Site Telephony) pour les bureaux distants assurent une tolérance de panne spécifique à la téléphonie pour garantir la continuité du fonctionnement du réseau vocal même en cas de perte de connectivité vers le site du siège social.

Comment réaliser une solution V^{3}PN : les composantes Cisco

Cisco propose un large éventail de produits et d'architectures de déploiement éprouvées pour les réseaux vidéo et téléphonie IP, comme pour les VPN IPSec. Cisco est idéalement positionné sur ce segment de marché pour fournir la solution de réseau convergent qui caractérise les V^{3}PN. Le déploiement des solutions V^{3}PN Cisco garantit l'interopérabilité des applications multiservices sur les VPN IPSec. De plus nous proposons une source unique pour l'aide à la conception de réseaux et l'assistance technique. La Figure 1 présente une solution V^{3}PN Cisco.

Figure 1 La solution VPN IPSec compatible voix et vidéo Cisco



Les produits qui permettent la réalisation d'une infrastructure VPN multiservice de bout en bout comprennent :

- Les routeurs VPN Cisco – Ces routeurs réalisent les fonctions VPN IPSec de base comme le cryptage et la tunnellisation tout en offrant les fonctions indispensables au multiservice comme la qualité de service (QoS) améliorée, le support des VPN multicast et le routage et la reprise à inspection d'état qui garantissent la tolérance de pannes. Pour les sites distants, les routeurs VPN Cisco offrent des fonctionnalités tout en un pour la voix, la vidéo, les VPN, les pare-feu et l'accès WAN avec une totale tolérance de pannes VPN et voix par l'intermédiaire de fonctionnalités SRST, et assurent l'alimentation par Ethernet des téléphones IP Cisco. De nouvelles plates-formes comme les routeurs haut-débit sécurisés de la gamme Cisco 830 et les routeurs VPN de la gamme Cisco 3700, prochainement disponibles, offrent une évolutivité améliorée pour tous les sites réseaux des déploiements V^3PN Cisco.
- Cisco CallManager et passerelles Cisco IOS – Ces unités réalisent l'établissement et l'interruption d'appels ainsi que la conversion TDM – IP du trafic voix et gèrent la capacité de contact des téléphones IP. Les passerelles Cisco IOS fournissent des interfaces vers le réseau téléphonique public commuté (RTPC) ainsi que la tolérance de pannes de type SRST pour le trafic voix lorsqu'ils sont déployés sur les sites distants.
- Téléphones IP Cisco – Ces combinés téléphoniques IP alimentés par Ethernet offrent des fonctionnalités évoluées comme les répertoires internes et les services Web.
- Pare-feu Cisco PIX – Ces unités à inspection d'état surveillent le trafic multiservice et supportent les principaux protocoles de signalisation de la téléphonie IP, notamment les signaux d'appels entre les téléphones IP Cisco et Cisco CallManager.
- Systèmes de détection des intrusions (IDS) Cisco – Les systèmes IDS installés sur l'hôte permettent la détection des intrusions et préviennent les attaques par saturation sur l'infrastructure de téléphonie IP.

Ce que vous y gagnez : la rentabilité opérationnelle

La rentabilité opérationnelle n'a pas la même signification pour les différents intervenants de l'entreprise. Pour l'administrateur réseau, elle se traduit par la facilité de déploiement et de gestion du réseau. Les décideurs de l'entreprise l'envisagent comme la capacité d'utiliser le réseau pour fournir de nouvelles applications qui font la différence avec leurs concurrents et ouvrent de nouveaux marchés. Pour les comptables, il s'agit d'accroître la productivité tout en réduisant les coûts, bref en faire davantage tout en payant moins. Quelle que soit la définition que vous adoptiez, les solutions V^{3}PN Cisco vous apportent la rentabilité opérationnelle en fournissant des communications convergentes de prochaine génération sur la connectivité de réseau la plus économique et la plus souple qui soit – les réseaux privés virtuels.

La suite de solutions VPN multiservice Cisco

La solution V^{3}PN Cisco est un élément de la suite de solutions VPN multiservices proposée par Cisco. Cisco propose également des solutions pour le transport de la voix et de la vidéo sur les réseaux MPLS et les VPN voix gérés à plan de numérotation. Ensemble, ces solutions offrent des capacités inégalées de souplesse de déploiement et de fonctionnalités pour fournir des services de réseau convergent aux réseaux des entreprises et des fournisseurs de services.

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :
www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France • Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas Pérou • Philippines •Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine Russie • Singapour • Slovaquie •Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

RD/LW3799-06/04