ARCHITECTURE DE TÉLÉTRAVAIL CLÉ EN MAIN CISCO

L'architecture Cisco® Business Ready Teleworker est une solution de télétravail robuste, élégante et évolutive qui permet d'optimiser le transport des services données, voix et vidéo de l'entreprise entre le bureau à domicile d'un employé et les ressources de sa société sur les réseaux publics des fournisseurs de services, le tout au sein d'une architecture de réseau entièrement sécurisée et gérée de manière centralisée.

DESCRIPTION GENERALE ET APPLICATIONS DE LA SOLUTION

Sous une forme ou une autre, la plupart des sociétés fournissent des services d'accès à distance pour leurs employés mobiles ou qui travaillent à domicile et que l'on désigne sous l'appellation de télétravailleurs. Par le passé, l'entreprise s'est exclusivement intéressée aux avantages du télétravail en termes de productivité. Les récents progrès ont toutefois permis la transition des activités du siège social vers les bureaux à domicile, améliorant considérablement la capacité des sociétés à continuer de fonctionner malgré différents impondérables comme les intempéries, les problèmes de santé, les grèves ou les embouteillages.

La résilience opérationnelle n'est que l'une des raisons économiques de la généralisation rapide du télétravail. Toutefois, les services traditionnels de télétravail présentent des faiblesses qui augmentent les risques et compliquent leur administration pour l'entreprise. Les télétravailleurs peuvent se connecter à d'autres réseaux comme Internet, partager les ressources réseau avec des utilisateurs n'appartenant pas à l'entreprise, comme leur conjoint ou leurs enfants, attraper un virus ou un ver informatique et le transmettre à leur insu au réseau de l'entreprise lorsqu'ils se connectent. Une organisation peut devoir assurer la gestion et l'assistance technique de milliers de systèmes de télétravail, dont beaucoup risquent d'être installés par les utilisateurs finaux, en fonction de leurs moyens avec des ordinateurs et des appareils qu'ils auront installés ou «bricolés» eux-mêmes.

La solution de télétravail Cisco Business Ready Teleworker fournit aux employés géographiquement dispersés – disposant, par exemple, d'un bureau à domicile – un accès aux applications et aux services équivalent à celui qu'ils auraient au siège social de leur entreprise. Le déploiement d'une telle solution est rapide et économique et offre au télétravailleur un accès de haute qualité et uniforme aux applications du réseau d'entreprise sur une connexion toujours ouverte, sécurisée et gérée de manière centralisée.

La solution Cisco Business Ready Teleworker est particulièrement profitable à l'entreprise : elle crée un plan de secours intégré qui permet de maintenir fonctionnels les processus métiers même dans des circonstances imprévues, stimule la productivité du télétravailleur, accroît la réactivité et donc la satisfaction client, en même temps qu'elle réduit les coûts d'exploitation et d'investissement – sans compromettre ni la sécurité ni la facilité de gestion. Elle établit pour ce faire une connexion de réseau privé virtuel (VPN) à haut débit entre le télétravailleur et le réseau du siège. Cette connexion est assurée par un unique appareil hautement intégré et placé derrière le modem haut-débit (câble ou ADSL) au domicile du télétravailleur.

Dans ce Livre blanc, nous décrivons comment la solution de Cisco Business Ready Teleworker répond à tous les problèmes d'un déploiement à grande échelle avec des services de réseau applicatifs intelligents qui étendent – pour la première fois – au bureau à domicile des services jusqu'à présent réservés au réseau campus d'entreprise.

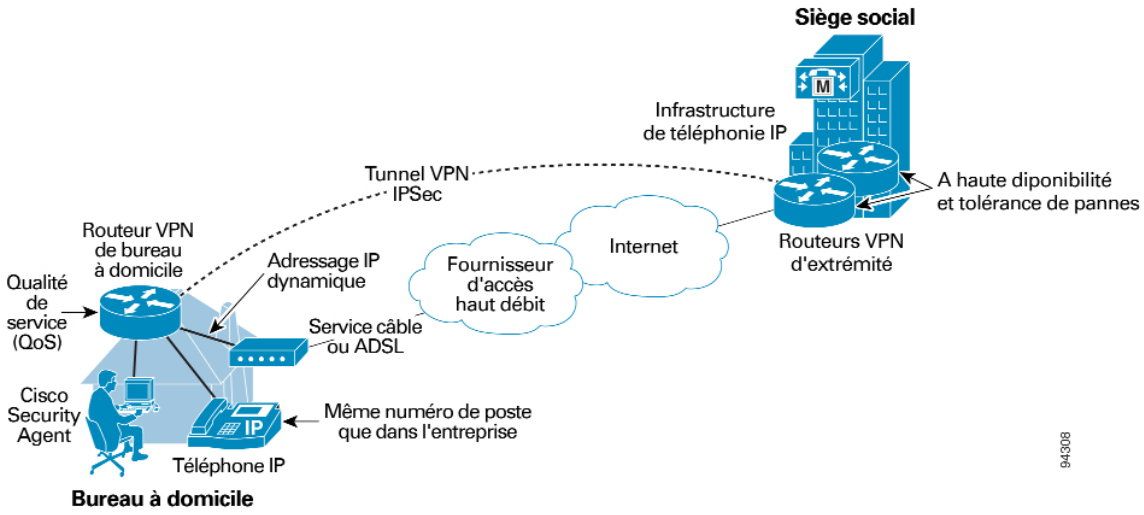
Vous trouverez dans Descriptif de la solution Cisco Business Ready Teleworker un résumé des possibilités de la solution, une description de la manière dont Cisco a mis en place une solution de télétravail clés en mains sur son propre réseau, ainsi qu'une analyse des raisons commerciales qui font de cette solution une composante essentielle de l'environnement de réseau optimisé de l'entreprise.

ARCHITECTURE DE LA SOLUTION CISCO BUSINESS READY TELEWORKER

La solution Cisco Business Ready Teleworker convertit en toute transparence le bureau à domicile du télétravailleur en une extension fonctionnelle de son entreprise. Les télétravailleurs qui accèdent aux services de l'entreprise par le réseau VPN disposent des mêmes fonctions que s'ils étaient au siège social.

La solution repose sur l'architecture technologique V3PN (Systems Voice- and Video-Enabled IPSec VPN) élaborée par Cisco et qui permet d'étendre de manière sécurisée des applications comme la voix et la vidéo entre les environnements de travail à domicile et les sites d'entreprise. Elle réalise un service de réseau privé virtuel (VPN) de bout en bout qui garantit l'acheminement vers les bureaux à domicile des applications de l'entreprise (données, voix et vidéo) de manière rapide, économique, fiable et sécurisée, tout en supportant les exigences de réactivité et de continuité de l'entreprise. La Figure 1 présente l'architecture de la solution Cisco Business Ready Teleworker.

Figure 1 Architecture de la solution Cisco Business Ready Teleworker



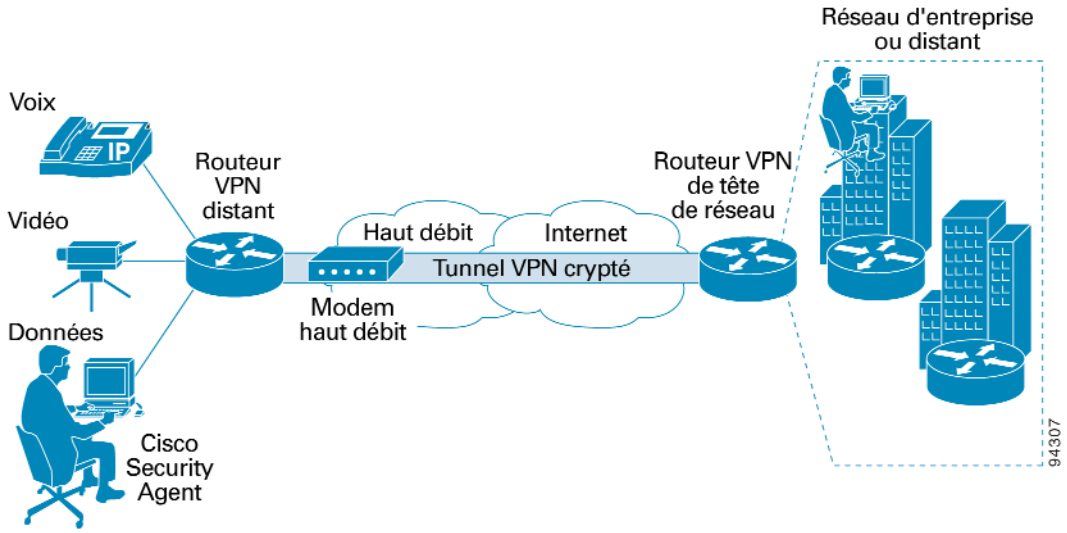
COMPOSANTES DE LA SOLUTION CISCO BUSINESS READY TELEWORKER

Composantes matérielles

La Figure 2 présente les composantes matérielles de l'architecture Cisco Business Ready Teleworker. Ces composantes se subdivisent en :

- composantes pour le bureau à domicile (indispensables)
- infrastructure de Cisco de téléphonie IP (facultative)
- composantes au siège social (indispensables)

Figure 2 Composantes de la solution Cisco Business Ready Teleworker



Composantes pour le bureau à domicile (indispensables)

- un accès câble ou ADSL haut-débit
- un routeur de la gamme Cisco 830 avec qualité de service (QoS)
- un ordinateur portable (ou de bureau)
- un téléphone IP Cisco (facultatif)
- un point d'accès de réseau LAN sans fil (WLAN) Cisco Aironet® (facultatif)

La gamme des routeurs haut-débit sécurisés Cisco 830 se compose du routeur Ethernet haut débit Cisco 831 et du routeur ADSL haut débit Cisco 837. Les routeurs de la gamme Cisco 830 offrent de nombreuses fonctionnalités : qualité de service (QoS) pour la voix, sécurité par VPN, cryptage matériel 3DES (Triple Data Encryption Standard) IPSec hautes performances, tunnellisation partagée, pare-feu, détection des intrusions, authentification évoluée et gestion à distance.

Ils se connectent aux unités d'accès Internet – modems haut-débit – pour réaliser une connectivité à grande vitesse, et aux unités installées dans le bureau à domicile par l'intermédiaire de ports de commutation intégrés Ethernet 10/100. Ils peuvent servir un unique poste de travail ou plusieurs unités de réseau comme des postes de travail, des serveurs et des téléphones IP. En option, des unités de réseau personnelles au domicile peuvent partager la connexion réseau, y compris d'autres PC et des imprimantes.

Les routeurs de la gamme Cisco 830 fournissent des services de base aux unités d'entreprise ou à domicile, notamment la traduction d'adresses NAT (Network Address Translation), le protocole DHCP (Dynamic Host Configuration Protocol) pour l'adressage dynamique de plusieurs unités, et la protection par pare-feu contre les attaques Internet.

La solution Cisco Business Ready Teleworker fournit également au télétravailleur des services et des types d'accès qui ne sont normalement pas disponibles pour les appareils installés à domicile comme l'accès aux données et à la téléphonie d'entreprise. Les appareils utilisés pour le télétravail bénéficient de la qualité de service (QoS) qui différencie le trafic voix et données de l'entreprise du reste du trafic afin de garantir au télétravailleur un niveau de service uniforme et fiable.

Composantes au siège social (indispensables)

Les composantes installées au siège social facilitent l'intégration avec le site central. Ces composantes comprennent :

- une infrastructure de tête de réseau VPN Cisco IOS qui regroupe et termine les tunnels VPN IPSec en provenance des routeurs à domicile – des routeurs Cisco 3700 et 7200, par exemple ;
- la même architecture à tolérance de pannes actuellement utilisée pour l'agrégation des petits bureaux et des agences.

Les routeurs VPN Cisco IOS du siège social regroupent et terminent les tunnels VPN IPSec en provenance des routeurs à domicile.

Infrastructure de Cisco de téléphonie IP (facultative)

La gamme de produits de téléphonie IP Cisco fournit une solution complète de services de bout en bout depuis le siège social jusqu'aux bureaux à domicile des télétravailleurs, réalisant ainsi une solution pleinement convergente et évolutive pour les travailleurs distants. Les produits de la solution de téléphonie IP Cisco comprennent :

- Cisco CallManager – assure le traitement d'appels, la signalisation et le contrôle des unités dans une architecture de groupement hautement évolutive et redondante ;
- le routeur / passerelle voix Cisco IOS – assure le transcodage pour le pontage réseau TDM (time-division multiplexing) et Voix sur IP (VoIP) ;
- un téléphone IP Cisco – fournit des services d'informations de bureau comme les annuaires intégrés et des nouvelles par l'intermédiaire du combiné voix ;
- la messagerie unifiée Cisco Unity™ – assure la consolidation de la messagerie vocale, de la télécopie et du courrier électronique sur le bureau ; simplifie la gestion des messages et augmente la productivité de l'employé grâce aux fonctions Active Assistant ;
- Cisco IP Contact Center – assure le routage intelligent et le traitement des appels, la convergence téléphonie – informatique (CTI) du réseau vers le PC et la distribution automatique des appels (DAA) avec téléphonie IP qui permet de réaliser une infrastructure distribuée de centre de contacts.

Les serveurs Cisco CallManager gèrent le contrôle et le traitement des appels entre le siège social et un téléphone IP installé dans le bureau à domicile du télétravailleur. Sur le combiné du téléphone IP, le raccordement à la ligne s'effectue par le port Ethernet et s'intègre au réseau de données.

Composantes logiques

Les principales composantes logiques de l'architecture Cisco Business Ready Teleworker sont intégrées aux routeurs de la gamme Cisco 830. Ces services comprennent :

- les VPN IPSec
- la sécurité et l'authentification
- la gestion
- la qualité de service (QoS)
- les communications IP

VPN IPSec

La solution Cisco Business Ready Teleworker utilise un VPN de site à site pour connecter les sites distants des télétravailleurs. Un VPN de site à site supporte plusieurs unités à l'aide d'un tunnel VPN entre le bureau à domicile et le siège social. L'environnement de télétravail prend en charge de nombreux équipements comme l'ordinateur portable utilisé en entreprise, les ordinateurs personnels installés à la maison et qui accèdent à Internet et, en option, un téléphone IP.

Cette connexion VPN est toujours ouverte et n'exige pas du télétravailleur qu'il utilise un client VPN logiciel. Transparent pour les applications et l'utilisateur final, le tunnel VPN assure :

- un comportement stable et uniforme des applications sur le réseau WAN, qui protège et élargit les investissements d'infrastructure déjà réalisés ;
- des économies par rapport aux réseaux traditionnels. Les VPN utilisent les connexions haut-débit existantes accessibles à partir du domicile du télétravailleur et réduit les dépenses liées aux équipements, aux lignes d'accès et aux opérateurs téléphoniques en intégrant la voix et les données sur le VPN ;
- la sécurité et le cryptage hautes performances. Les VPN IPSec sont compatibles avec une infrastructure de cryptage à clé publique qui garantit une sécurité de bout en bout. L'authentification mutuelle sécurisée est assurée par le protocole IKE (Internet Key Exchange) de gestion dynamique des clés IPSec ;
- la haute disponibilité à l'aide de la détection DPD (Dead Peer Detection) des protocoles de routage, qui assure la reprise automatique dans le cas d'une interruption du service – aussi bien sur la liaison de communications qu'au niveau de la tête de réseau d'entreprise.

Sécurité et authentification

La sécurité est une composante essentielle de la solution Cisco Business Ready Teleworker. Elle est totalement intégrée à toutes les autres fonctions pour permettre au télétravailleur d'accroître sa productivité en utilisant la technologie de réseau de manière sûre et sécurisée. Cisco est le seul constructeur qui ait adopté une approche intégrée de la sécurité de tous les aspects de votre réseau et de ses points d'extrémité. Cette démarche remplit les trois critères fondamentaux qui garantissent la productivité et la sécurité du télétravailleur :

- la collaboration entre les services de sécurité et les services de réseau – la sécurité est renforcée lorsque les services de réseau comme la qualité de service (QoS) collaborent de manière transparente avec les services IP. La démarche intégrée de Cisco en matière de sécurité permet une collaboration étroite entre les technologies de réseau et les technologies de sécurité ;
- le déploiement souple et personnalisable de la sécurité avec des services intégrés à l'unité de routage installé à domicile – Cisco propose la plus large gamme de technologies de sécurité actuellement disponible auprès d'un constructeur unique. Cette souplesse vous permet de déployer les technologies de sécurité de votre choix ;
- une couverture exhaustive – Cisco vous permet de déployer la sécurité sur la totalité du réseau, depuis les PC et les serveurs jusqu'aux réseaux LAN et WAN, aux succursales d'entreprise et aux bureaux à domicile. Vous bénéficiez ainsi du système de défense homogène indispensable pour mettre l'ensemble des processus vitaux de votre entreprise à l'abri des menaces tant internes qu'externes.

Grâce aux fonctionnalités de haute disponibilité, de sécurité et de qualité de service (QoS) qu'elle intègre aux unités qu'elle gère, la plate-forme logicielle Cisco IOS protège votre réseau contre les pannes, la dégradation des services et les problèmes de sécurité. Ensemble, ces trois critères fondamentaux permettent à votre réseau de réagir aux différents problèmes qu'il peut rencontrer.

Avec les pare-feu Cisco IOS intégrés, les systèmes de détection des intrusions (IDS), les listes de contrôle d'accès (ACL) à horodatage et la fonction de blocage instantané «one-touch lockout», le risque d'un contournement de la sécurité ou d'une mauvaise utilisation du réseau est très fortement réduit. Ces mêmes fonctions de sécurité fournissent également une intelligence adaptative capable de réagir de manière rapide aux menaces émergentes ou imprévues.

Les services d'identification IBNS (Identity-based Networking Services) fournissent un cryptage robuste et une authentification forte des utilisateurs et des unités qui permettent de prévenir les attaques des utilisateurs non autorisés. La norme de contrôle d'accès aux ports 802.1X de l'IEEE permet de faire appliquer les politiques d'entreprise qui supportent les mécanismes d'authentification comme RADIUS (Remote Authentication Dial- In User Service). La norme 802.1X peut également servir à exclure du réseau les unités indésirables ou à assurer le routage intelligent du trafic depuis les unités qui n'appartiennent pas à l'entreprise jusqu'à Internet directement – leur interdisant ainsi l'accès au tunnel VPN et aux ressources de l'entreprise.

Le cryptage matériel – 3DES ou AES (Advanced Encryption Standard) – fournit une puissance de traitement de haut niveau pour la gestion de la sécurité de la couche transport, les clés de cryptage évoluées et le contrôle d'intégrité des messages. Tout le trafic entre le télétravailleur et le réseau d'entreprise est crypté, y compris les données, la voix et la vidéo.

Cisco est le seul constructeur du marché à adopter une démarche convergente de la sécurité sur l'ensemble du réseau jusqu'aux points d'extrémité des télétravailleurs pour vous permettre de protéger et de défendre vos processus métiers contre les attaques internes et externes.

Gestion

La réalisation d'un réseau capable de supporter efficacement le télétravail exige que ses utilisateurs soient en mesure de vérifier, de gérer et d'optimiser leurs connexions vers le réseau d'entreprise. La solution Cisco Business Ready Teleworker permet aux administrateurs IT de réaliser à distance les tâches de surveillance et de gestion quotidiennes sur les unités du bureau à domicile.

La sécurité et la gestion des politiques peuvent être administrées localement, à partir du bureau à domicile, ou de manière centralisée depuis le siège de l'entreprise. Le service informatique du siège social dispose d'une visibilité complète des sites distants. Depuis un unique poste, il peut instantanément mettre à jour la configuration et les politiques de sécurité – y compris les mises à jour des pare-feu et les signatures de détection des intrusions – sur l'ensemble des sites et sans avoir à attendre l'utilisateur. Des outils comme Cisco ISC (IP Solution Center) permettent une gestion détaillée en exécutant des fonctions évolutives de surveillance, d'alerte et de reporting auprès des unités des télétravailleurs.

D'autres outils, comme Cisco SAA (Service Assurance Agent), donnent également aux administrateurs la possibilité de tester périodiquement la connexion du télétravailleur au travers du VPN dans les deux sens afin d'évaluer à tout moment l'incidence des temps de latence, de la gigue et des pertes de paquets. Si un utilisateur final connaît des problèmes de niveau de service, il est possible de surveiller la connexion et de savoir si le problème provient du fournisseur de service ou du service de télétravail lui-même.

Pour les VPN d'entreprise, vous pouvez également confier la gestion des unités VPN à un fournisseur de services.

Qualité de service (QoS)

La qualité de service est une composante critique de la solution de télétravail. La vitesse plus faible des liaisons ascendantes sur la plupart des circuits haut-débit résidentiels peut entraîner un ralentissement du trafic. Ce phénomène peut affecter les performances des applications et des transmissions de données vitales pour l'entreprise qui sont sensibles aux retards, aux variations dans les délais (gigue) ou aux pertes de paquets, notamment les communications IP – la voix, par exemple. Les performances des applications peuvent également subir des perturbations en raison des autres activités du réseau à domicile, comme une sauvegarde ou un téléchargement programmé(e).

La qualité de service (QoS) garantit une qualité uniformément acceptable pour la transmission des données vitales et pour les applications sensibles aux délais. Elle permet également de définir des règles pour le traitement particulier des différents types de trafic. Si, par exemple, le conjoint ou un enfant du télétravailleur partage la connexion avec lui, il est possible d'accorder la priorité au trafic d'entreprise pour garantir des performances constantes et de haute qualité capables de supporter les exigences de productivité.

La QoS intégrée permet l'utilisation optimisée de la bande passante du réseau WAN et l'amélioration des performances des applications vitales de l'entreprise, des services vidéo pour la formation, des communications d'entreprise et des applications avancées comme les communications IP.

Communications IP

Les données, la voix et la vidéo peuvent être transmis de manière convergente sur le réseau, ce qui supprime la nécessité de multiplier les frais d'administration, de formation et de maintenance. La composante logicielle de traitement des appels de la solution de téléphonie IP de Cisco est Cisco CallManager. Entre autres caractéristiques, Cisco CallManager :

- équipe plus de 6500 clients en communications IP dans le monde entier ;
- regroupe le traitement des appels et les applications qui permettent la mobilité des employés et réduisent les coûts administratifs ;
- gère les solutions de communication IP de Cisco en permettant l'interopérabilité avec certains commutateurs privés (PBX) à multiplexage temporel (TDM), suivant les fonctionnalités requises.

Grâce à la téléphonie IP, le télétravailleur n'a plus besoin d'un combiné relié au réseau téléphonique public commuté dans son bureau à domicile. Il peut conserver le même numéro, qu'il soit à son bureau au siège social ou à son domicile : le téléphone sonnera dans les deux pièces mais il n'aura qu'une seule messagerie vocale à consulter. Un client ignorera totalement que la personne qu'il appelle se trouve à son domicile, ce qui accroît encore les économies et les gains de productivité que le télétravail permet de réaliser grâce à la téléphonie IP.

Les solutions comparables exigent des équipements propriétaires et des circuits spécialisés onéreux comme un réseau numérique à intégration de services (RNIS), ce qui les rend prohibitifs. Avec la solution Cisco Business Ready Teleworker, il suffit d'un service haut-débit pour transmettre les données, la voix et la vidéo.

Les services de communication IP innovants réalisent un environnement de télétravail à la fois très efficace et très autonome qui génère des économies, augmente la disponibilité, et autorise une évolution et une croissance souples.

Services Cisco Powered Network

Les partenaires fournisseurs de service Cisco Powered Network offrent des contrats de niveau de service qui garantissent la fiabilité et la disponibilité des connexions de réseau étendu (WAN) – que vous gériez vous-même la connexion où que vous en confiiez la gestion à votre fournisseur de services. A l'avenir, Cisco envisage de créer une appellation Cisco Powered Network pour les fournisseurs de services qui proposent des services gérés destinés aux télétravailleurs en garantissant la sécurité des connexions et des contrats de niveau de service entre le siège social et le bureau à domicile.

AMELIORATIONS DE SECURITE POUR LES RESEAUX DE TELETRAVAIL

La protection du réseau WLAN de télétravail

Si le réseau sans fil est mal configuré, le trafic sans fil provenant du réseau peut être facilement intercepté et analysé à l'extérieur du domicile. Une unité sans fil placée à l'extérieur du bureau du télétravailleur peut aisément utiliser son réseau sans fil lorsque celui est mal sécurisé. Pour protéger l'entreprise, nous recommandons diverses combinaisons de modèles et de méthodes de sécurité, notamment Cisco LEAP et WEP (Wired Equivalent Privacy) qui permettent respectivement l'authentification et le cryptage. Ces méthodes autorisent l'authentification sans utiliser de clés WEP statiques au niveau des points d'accès ou des clients sans fil.

Depuis 2004, les points d'accès sans fil Cisco intégrent l'authentification 802.1X, offrant ainsi un moyen simple, sécurisé, évolutif et normalisé d'authentifier les unités sans fil et leurs utilisateurs. Avec la norme 802.1X, l'authentification utilisateur intervient avant l'attribution d'une adresse IP ce qui garantit que seuls les utilisateurs autorisés peuvent accéder au WLAN. Sans cette norme, toute unité client illégale qui s'associe avec un point d'accès obtient une adresse IP en clair. Un utilisateur non autorisé peut alors s'installer sur le WLAN et lancer des attaques «par l'intermédiaire» ou réduire la bande passante du réseau. La solution Cisco Business Ready Teleworker intégrera l'authentification 802.1X qui protège le WLAN du bureau à domicile et entretient le lien crypté – pour éliminer toute vulnérabilité sur la couche 2.

Partage de la connexion avec le conjoint ou les enfants

Pour permettre au réseau du télétravailleur de servir également un autre utilisateur du domicile, la solution Cisco Business Ready Teleworker offre des options d'authentification et de tunnellisation en fonction de l'utilisateur, ce que l'on appelle également la tunnellisation partagée. Cette méthode permet de diriger vers Internet directement et sans cryptage tout le trafic qui ne fait pas partie des communications de l'entreprise. La tunnellisation partagée ne crypte que le trafic professionnel et évite que les autres utilisateurs des ordinateurs du domicile puissent accéder au réseau d'entreprise.

Les options d'authentification du scénario «conjoint et enfants» comprennent :

- le serveur proxy d'authentification et de pare-feu Cisco IOS – méthode d'authentification HTTP qui fournit, par l'intermédiaire des protocoles TACACS+ et RADIUS, l'authentification individualisée et l'autorisation dynamiques du télétravailleur ;
- l'authentification 802.1X de l'utilisateur – la norme 802.1X permet de gérer les situations où l'unité d'accès au VPN est partagée par le télétravailleur et d'autres utilisateurs du réseau à domicile. Lorsque le télétravailleur connecte un ordinateur portable ou de bureau à un routeur de la gamme Cisco 830, il obtient une adresse IP prise dans un « pool de confiance ». Les unités qui n'appartiennent pas à l'entreprise et qui cherchent à se connecter au réseau obtiennent une adresse provenant d'un «pool non sécurisé» ce qui bloque automatiquement l'accès à la passerelle VPN. Seul un télétravailleur authentifié et ses propres unités professionnelles peuvent accéder au VPN d'entreprise, tandis que les autres utilisateurs du domicile n'obtiennent qu'un accès Internet.

UNE OFFRE A VALEUR AJOUTEE – POURQUOI CISCO ?

La puissance de la solution Cisco Business Ready Teleworker provient de sa capacité à intégrer de multiples solutions et de multiples services sur une plate-forme unique, offrant ainsi d'excellentes capacités de réseau. En association avec Cisco, vous bénéficierez des avantages suivants :

- une solution étroitement intégrée de bout en bout – vous bénéficiez de l'interopérabilité et de la haute disponibilité

des communications convergentes sur IP. L'ensemble du matériel, des services et des logiciels fait partie d'une solution de bout en bout cohérente et fortement intégrée développée autour de normes ouvertes ce qui permet de garantir le plus haut niveau de performances réseau ;

- la possibilité d'activer des fonctions et de les coupler étroitement offre de nouvelles fonctionnalités – ces services de réseau intelligents et applicatifs peuvent être individuellement activés sur la plate-forme logicielle Cisco IOS et étroitement associées à d'autres services et fonctions de réseau pour offrir de nouvelles fonctionnalités reposant sur l'intégration des services de routage, de commutation, de téléphonie, de vidéo, de mobilité et de sécurité ;
- l'interaction entre les fonctions permet de prévoir le comportement du réseau et d'en contrôler les ressources – ces services de réseau sont intelligents ; ils comprennent des protocoles intelligents qui leur permet de savoir ce que chacun fait. Ceci permet d'optimiser le trafic réseau et de personnaliser les services en fonction de vos priorités spécifiques en matière professionnelle, d'application ou d'utilisateur, pour vous donner une meilleure prévisibilité sur l'ensemble du réseau et optimiser l'utilisation de ses ressources ;
- l'expansion permanente des fonctionnalités – la suite de services de réseau applicatifs intelligents développée par Cisco est en constante expansion, de même que ses fonctions de service qui accroissent les fonctionnalités globales du network pour lui permettre de supporter des applications plus évoluées ;
- des schémas directeurs adaptables pour comprendre et réaliser – Cisco propose des schémas directeurs adaptables qui vous permettent de justifier et de réaliser de manière rapide et économique le déploiement de ces services de réseau applicatifs ;
- la simplification des opérations de l'entreprise et du service IT – grâce à la convergence des données, de la voix et de la vidéo sur un unique réseau, que seules une grande disponibilité de réseau et une gestion intégrée et centralisée permettent de fournir, la solution Cisco Business Ready Teleworker vous aide à rationaliser des opérations coûteuses. Cisco vous apporte également une gamme complète de produits, d'aide à la conception de réseau et d'assistance technique ;
- la protection et la pérennisation des investissements d'infrastructure déjà réalisés – la solution Cisco Business Ready Teleworker vous apporte une architecture de réseau particulièrement adaptable qui protège et prolonge vos investissements, vous donnant ainsi les moyens de gérer de manière plus efficace le développement de votre force de télétravail.

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