UNIVERSITÉ PARIS-EST Marne-la-Vallée

IFIAG

SSL VPN

Project technique

BENCHCHAOUI OMAR ADIL

Contents

I. Résumé:

La mondialisation, l'utilisation accrue d'Internet, et le coût exorbitant des lignes spécialisés, a obligé les fournisseurs d'informatique à proposer des solutions pour gérer, contrôler et permettre l'accès distance.

La technologie appelé **Virtual Private Network ;** en plus bref **VPN** ; a donné la possibilité au entreprise de connecter leurs sites éparpillés dans le monde, ou à permettre a leur employés distant d'avoir accès aux ressources internes de l'entreprise.

Dans ce rapport, je vais parler brièvement de la solution VPN, des différentes technologies qui règnent sur le marché, dans la partie pratique, j'ai simulé un accès a distance au routeur configuré avec la technologie SSLVPN.

Partie Théoriques :

II. Introduction au VPN:

Un VPN (**Virtual Private Network**) est une connexion réseau privée sécurisée construite au sommet d'infrastructures accessibles au public. Il offre une alternative à l'utilisation du serveur proxy pour accéder à distance aux ressources ainsi qu'une méthode sécurisée pour vous authentifier sur un réseau.

III. Problématiques:

La croissance rapide de l'Internet et le déploiement généralisé des réseaux créent une demande pour de nouvelles capacités dans les réseaux IP. Certaines entreprises ont mis en place leur propre réseau WAN (Wide Area Network) en utilisant une ligne spéciale. Mais ces réseaux sont coûteux, et il n'est pas possible dans un tel système de partager la bande passante entre plusieurs clients.

IV. La solution:

1) Réseaux privée VPN :

VPN est l'atout le plus populaire dans les solutions d'accès à distance. Il fournit une méthode sécurisée de transfère de données critiques. Les fournisseurs comme Cisco Systems améliorent continuellement leurs produits pour fournir des fonctionnalités qui tirent parti des progrès réalisés dans les normes et les protocoles comme IPSec et L2TP (Layer 2 Tunneling Protocol).

La solution VPN doit pouvoir contenir toute sorte de fonctions :

Protection des données en utilisant les technologies de cryptage, tels que RC-4, DES, 3DES et AES.
Protection contre la falsification de paquets à l'aide des fonctions de hachage comme MD5 et SHA.
Protection contre les attaques « man-in-the-middle » en utilisant des mécanismes d'authentification, tels que les clés pré-partagées ou les certificats numériques.
Protection contre les attaques par « rejet » (*replay attack*) en utilisant des numéros de séquence lors de la transmission des données protégées.

Définir des mécanismes sur façon dont les données sont encapsulées et protégées, et comment protéger le trafic lors de la transmission entre les différents dispositifs.

2) Type :

VPN prend en charge au moins trois différents types d'utilisation:

Les connexions d'accès à distance au client.
L'interconnexion entre deux réseaux LAN.
L'accès contrôlé au sein d'un intranet.

3) Principe de fonctionnement :

Le VPN a attiré l'attention de nombreux organismes qui cherchent à la fois, à développer leurs capacités réseaux et à réduire leurs coûts.
Le VPN peut être trouvé dans sur les lieux de travail chez les professionnels ainsi que chez les particuliers, où il permet aux employés de se connecter en toute sécurité aux réseaux d'entreprise. Les télétravailleurs et ceux qui voyagent souvent trouvent dans le VPN la solution la plus commode pour rester connecté à l'intranet de l'entreprise.

a. Les avantages :

La réduction des coûts par rapport à un WAN traditionnel.
Etendre la connectivité géographique.
Améliorer la sécurité.
Réduire les coûts et le temps de transit et des transport pour les utilisateurs à distance.
Offre la possibilité d'un réseau mondial.

b. Les inconvénients :

Le VPN nécessite une compréhension détaillée des questions de sécurité réseau et une installation et une configuration soignée pour assurer une protection suffisante sur un réseau public comme Internet.
La fiabilité et la performance d'un VPN sur Internet n'est pas sous le contrôle direct d'une organisation. Au lieu de cela, la solution repose sur un FAI et leur qualité de service.
Les technologies VPN de différents fournisseurs peuvent ne pas bien fonctionner ensemble en raison de normes encore immatures.
Le VPN doit tenir compte des autres protocoles de réseaux internes afin de ne pas créer des incompatibilités.

4) Type d'utilisation du VPN :

Les trois grands cas d'utilisation de VPN sont les suivants:

- Raccordement des télétravailleurs ou travailleurs mobiles. Ceux-ci se raccordent aux ressources de l'entreprise via un modem, RNIS ou xDSL.

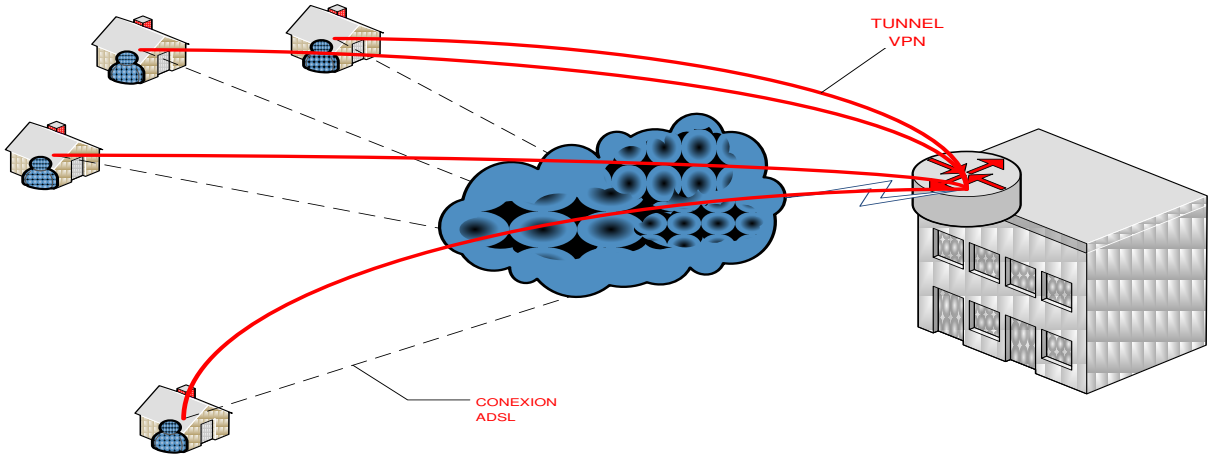


Figure 1 : Raccordement de télétravailleurs ou travailleurs mobiles

- Interconnexion des sites distants d'une même entreprise qui partagent les mêmes ressources sans pour autant avoir recours à des lignes spécialisées (LS).

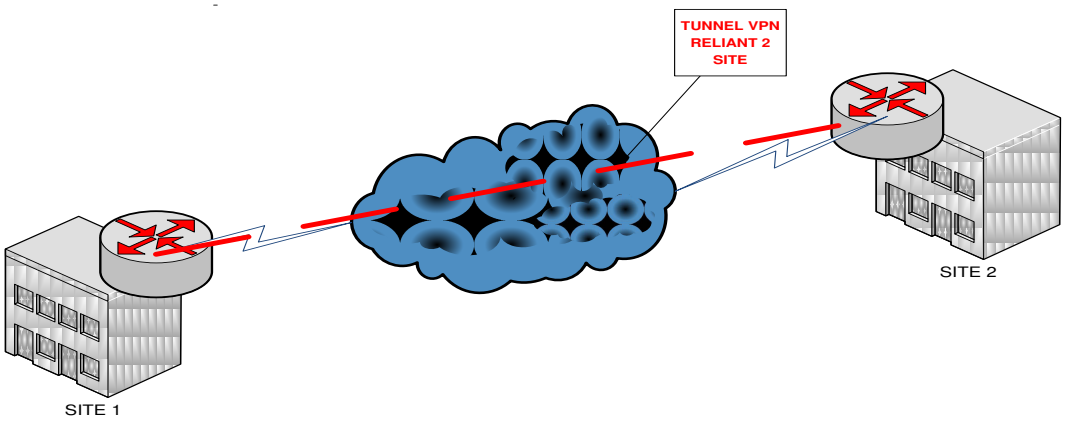


Figure 2 : interconnexion de sites

- Exploitation de réseaux extranets.

V. Protocoles du VPN :

Plusieurs protocoles réseau d'authentification et de chiffrement sont devenus populaires en raison de l'évolution du VPN:

1. **PPTP.**
2. **L2TP.**
3. **IPsec.**
4. **SSL VPN.**

L'authentification permet aux clients VPN et les serveurs d'établir correctement l'identité des personnes sur le réseau. Le cryptage des données potentiellement sensibles permet d'être caché aux yeux du grand public.

1) Types de tunnels VPN

Plusieurs protocoles de réseau informatique ont été mis en place spécifiquement pour une utilisation avec des tunnels VPN. Les protocoles les plus populaires de tunneling VPN énumérés ci-dessous continuent de se concurrencer les uns avec les autres pour leur acceptation dans l'industrie. Malheureusement ces protocoles sont généralement incompatibles les uns avec les autres.

a. Point-to-Point Tunneling Protocol (PPTP)

Plusieurs sociétés ont travaillé ensemble pour créer la spécification PPTP. Les gens associent généralement PPTP avec Microsoft, car presque tous les produits Windows incluent une prise en charge des clients pour ce protocole. Les premières versions de PPTP pour Windows présentaient des caractéristiques de sécurité que certains experts estimaient trop faibles pour un usage professionnel.

PPTP - Point-to-Point Tunneling Protocol - étend le protocole point à point (PPP) pour les accès réseau à distance traditionnels. PPTP est le mieux adapté pour les applications d'accès distance VPN.

PPTP fonctionne au niveau de la couche 2 du modèle OSI.

b. Fonctionnement du PPTP :

PPTP encapsule les données dans des paquets PPP, ensuite ces derniers sont eux aussi encapsulés dans des paquets IP (datagrammes) pour leur transmission à travers un tunnel VPN basé sur Internet. PPTP supporte donc le cryptage des données et la compression des

paquets. Le PPTP utilise aussi une forme de **General Routing Encapsulation (GRE)** pour obtenir des données de et vers sa destination finale.

Les tunnels VPN sont créés en deux étapes:

1. Le client PPTP se connecte à votre FAI en utilisant PPP Dial-Up Networking (modem classique ou ISDN).

2. Via un dispositif de courtier, PPTP crée une connexion de contrôle TCP entre le client VPN et le serveur VPN afin établir un tunnel. Le PPTP utilise le port TCP 1723 pour ses connexions.

Le PPTP prend également en charge la connectivité VPN via un réseau local.

Le PPTP supporte l'authentification, le cryptage et le filtrage des paquets. Il utilise des protocoles d'authentification basés sur PPP comme EAP, CHAP et PAP. Il supporte aussi le filtrage de paquets sur les serveurs VPN. Les routeurs intermédiaires et autres pare-feu peuvent également être configurés pour router le trafic PPTP.

c. Layer Two Tunneling Protocol (L2TP)

Le concurrent direct au PPTP est le L2F, un protocole mis œuvre principalement dans les produits Cisco. Dans une tentative pour améliorer le L2F, les meilleures caractéristiques de celui-ci et PPTP ont été combinées dans le but de créer un nouveau standard appelé le L2TP. Comme le PPTP, le L2TP existe au niveau de la couche liaison de données dans le modèle OSI.

Tout comme le PPTP, le L2TP encapsule les données dans des trames PPP et les transmet à travers un backbone IP. Contrairement au PPTP, le L2TP utilise le UDP comme méthode d'encapsulation des données. Considérant que le PPTP utilise pour le chiffrement MPPE (qui est négocié via PPP), le L2TP s'appuie sur une solution plus sécurisée: les paquets L2TP sont protégés par IPSec ESP en utilisant le mode transport.

On peut aussi utiliser le L2TP sans IPSec, mais le principal problème de cette approche est que le protocole L2TP lui-même n'est pas un protocole de chiffrage et doit donc s'appuyer sur autre protocole. Par conséquent, la mise en œuvre du L2TP nécessite l'utilisation d'IPsec.

d. Internet Protocol Security (IPsec) :

L'IP sécurité, ou IPsec, est en fait un ensemble de protocoles qui fournissent des fonctionnalités uniques de sécurisation de la couche réseau entre deux équipements qui permettent :

- La confidentialité des données.
- L'intégrité des données.
- L'authentification des données.
- La détection d'anti-replay.

- L'Authentification entre les différents équipements.

Il peut être utilisé comme une solution de protocole VPN complet ou tout simplement comme un schéma de cryptage au sein du L2TP ou PPTP. IPsec existe au niveau de la couche réseau du modèle OSI.

Les services d'IPsec:

La confidentialité des données : Se fait par chiffrement pour protéger les données contre les tentatives d'écoute; Les algorithmes de chiffrement supportés sont le DES, le 3DES et l'AES.

L'intégrité des données et l'authentification : Se fait grâce la fonction HMAC (Hash-based Message Authentication Code) qui vérifie que les paquets n'ont pas été altérés et sont en cours de réception par un équipement autorisé ; en d'autres termes, empêcher une attaque par détournement man-in-the-middle ou le vol de session. Les fonctions HMAC supporté par l'IPsec sont le MD5 et le SHA-1.

La détection d'anti-replay : se fait en incluant les numéros de séquence des paquets cryptées pour s'assurer à ce qu'un replay attaque ne se produise pas par un dispositif man-in-the-middle.

L'authentification entre les équipements : veille qu'avant que les données soient transmises entre les équipements, qu'ils soient identifiés et validés ; Le dispositif d'authentification prend en charge les clés pré-partagées symétriques et asymétriques, ainsi que les certificats numériques. Les connexions d'accès à distance prennent en charge l'authentification des utilisateurs en utilisant le XAUTH court pour l'authentification étendue.

VI. SSL (Secure Socket Layer) VPN :

Dans les chapitres précédents, on as vu trois types de VPN (IPSec, L2TP, et PPTP). Tous les trois offrent une protection de la couche réseau. Cependant, l'inconvénient est qu'ils nécessitent qu'un logiciel spécial soit installé sur la machine cliente, et la formation des utilisateurs sur la façon d'utiliser le logiciel.

Certaines entreprises veulent une solution qui soit plus simple à utiliser et plus facile à entretenir que les trois qu'on vient de mentionner. Le Secure Socket Layer (SSL) a commencé comme un protocole de protection du trafic Web (HTTP) entre les dispositifs clients et les serveurs web. Normalement, il est utilisé pour fournir une protection pour les achats en ligne et des informations d'identité confidentielle sur les sites de E-commerce. Toutefois, de nombreux fournisseurs de réseau ont optimisé les capacités et l'utilisation du SSL pour mettre en œuvre des solutions VPN. Un des principaux avantage est que le SSL VPN ne requière aucun logiciel VPN installé sur le poste de l'utilisateur ; le SSL VPN utilise un navigateur web pour connecter le client avec le serveur VPN. L'Utilisation d'un navigateur web permet à un utilisateur d'accéder à un site intranet en toute sécurité depuis les équipements internes et externes.

Le reste de ce chapitre mettra l'accent sur l'utilisation du SSL pour les implémentations VPN.

1) Qu'est-ce qu'un SSL VPN?

SSL VPN est une des implémentations émergentes sur le marché. Il a été conçu pour les solutions d'accès à distance et ne fournissent pas de connexions de site à site. Le VPN SSL offre un accès sécurisé aux applications principalement basé sur le Web. Etant donné que le SSL utilise un navigateur Web, les utilisateurs n'ont généralement pas à utiliser de logiciel client spécifique sur leurs ordinateurs.

VPN SSL fonctionne au niveau de la couche session du modèle OSI. Et du fait que le client est un navigateur web, seules les applications qui prennent en charge un navigateur web peuvent utiliser cette solution VPN. Par conséquent, des applications telles que Telnet, FTP, SMTP, POP3, téléphonie IP, le contrôle de bureau à distance, et d'autres ne peuvent fonctionner avec les SSL VPNs. Bien sûr, beaucoup de vendeurs utilisent Java ou ActiveX pour améliorer les VPN SSL dans l'optique de prendre en charge les applications non-HTTP, le POP3 et SMTP, et partage de fichiers et d'impression Microsoft Windows. Par exemple, le Cisco SSL VPN prend en charge les applications non-Web, tels que Citrix, Windows Terminal Services, et bien d'autres.

Le Cisco VPN SSL est communément appelé « **WebVPN** ».

2) Les Avantages du VPN SSL :

Les solutions VPN SSL sont idéales pour les clients qui utilisent des navigateurs web pour interagir avec les applications d'une entreprise. Voici une brève liste des avantages du VPN SSL:

- Aucun logiciel supplémentaire ne doit être installé sur les postes des utilisateurs.
- On peut accéder à des applications en toute sécurité depuis n'importe quel endroit, on n'a besoin que d'une machine munie un navigateur web.
- Une très grande variété de navigateurs Web est prise en charge.
- Peu de formations sont nécessaires pour les utilisateurs (user friendly).
- Les utilisateurs peuvent généralement être authentifiés grâce à plusieurs méthodes, y compris les mots de passe statiques, les certificats, ou les services d'annuaire. Avec les services d'annuaire, un unique processus de connexion est utilisé pour l'authentification de l'utilisateur auprès de passerelle SSL, en plus de l'authentification auprès du service d'annuaire.

3) Inconvénients du SSL VPN :

Compte tenu de leurs avantages, les SSL VPN ont leurs limites et leurs inconvénients. Ce chapitre étudie quelques-uns d'entre eux. Les applications Web utilisent le port TCP : 80 pour

leurs connexions. Les connexions Web crypté SSL utilisent également le protocole TCP, mais sur un port différent : le 443. En utilisant le protocole TCP, SSL a ces deux avantages:

-Il peut détecter les attaques par les messages par rejeu.
-il protège les données utiles de la trame TCP, et donc le trafic engendré par une connexion SSL VPN peut traverser un dispositif NAT ou PAT.

SSL utilise les numéros de séquence TCP pour détecter et rejeter les messages d'attaques par rejeu. Même si elle peut remplir cette fonction, les VPN de la couche 3, comme IPsec, peuvent effectivement faire mieux. IPsec effectue ce processus au niveau de la couche réseaux, cependant le SSL les détecte au niveau de la couche supérieure (la couche transport). Par conséquent, l'IPsec est plus efficace.

TCP a un autre facteur limitatif: il est plus sensible aux attaques de déni de service (DoS). Par exemple, avec une connexion IPsec, qui utilise le protocole UDP, il est assez facile de se prémunir de ces attaques en examinant la signature numérique dans le paquet UDP. Cependant, avec le SSL et le TCP, c'est pire, car une attaque TCP SYN flood remplirait la table de session TCP sur l'appareil, ce qui peut engendrer une défaillance du périphérique.

4) Les technologies du SSL VPN :

Comme la technologie SSL VPN est devenue plus avancé et a rapidement été déployée ces dernières années, elle a attiré l'attention des administrateurs réseau qui sont à la recherche d'une solution VPN d'accès distant qui fournit un accès universel, avec un déploiement et une gestion à faible coût. À l'heure actuelle, aucune norme officielle n'existe pour les technologies de VPN SSL, divers fournisseurs utilisent leurs propres implémentations.

Les VPN transportent le trafic privé sur des réseaux publics. Un VPN sécurisé doit donc satisfaire les exigences de base suivantes:

- **L'Authentification** garantit que l'entité VPN communique avec l'équipement destinée. elle peut s'appliquer soit à un dispositif VPN ou un utilisateur VPN. Par exemple, dans un VPN d'accès distant, le périphérique VPN peut authentifier le PC de l'utilisateur afin de s'assurer que c'est bien le PC qui possède l'adresse IP qui est utilisé pour se connecter au concentrateur. Le concentrateur peut également authentifier l'utilisateur final qui utilise le PC pour bien attribuer des privilèges sur la base d'informations de l'utilisateur.
- **La confidentialité** garantit la confidentialité des données par le cryptage ces dernières.
- **L'intégrité du message** garantit que le contenu des données n'a pas été altéré pendant la transmission.

a. Le hachage

Le hachage joue un rôle important dans un système de sécurité en assurant l'intégrité du message transmis. Un algorithme de hachage transforme un champ de texte de longueur variable dans une chaîne de taille fixe. Les algorithmes de hachage utilisés dans un système de sécurité ont les deux propriétés suivantes:

- Un mécanisme de hachage à sens unique: Cela signifie que, compte tenu de la sortie de hachage, il est par conséquent difficile d'inverser la fonction de hachage pour obtenir le message original.
- Sortie sans collision: Cela signifie que pour un algorithme de hachage, ce calcul est impossible de trouver deux données qui ont le même hachage de sortie.

Jusqu'à présent, les algorithmes les plus couramment utilisés pour le hachage cryptographique ont été le Message Digest Algorithm 5 (MD5) et le Secure Hash Algorithm 1 (SHA-1). Ces deux éléments ont été conçus pour un travail à sens unique et sans collision d'algorithmes de hachage. MD5 permet un encodage 128-bit, et SHA-1 à 160-bit. En raison de sa grande taille, SHA-1 est normalement considéré comme plus sûr, mais son calcul est plus couteux, que le MD5. Avec le matériel et la mise en œuvre des logiciels des réseaux d'aujourd'hui, la différence de performance n'est généralement pas une réelle préoccupation. Par conséquent, SHA-1 est l'algorithme de hachage préféré pour une utilisation dans un déploiement SSL VPN.

b. Le cryptage :

Les algorithmes de cryptage transforment un texte clair en texte chiffré illisible. Différent du hachage, les algorithmes de chiffrement nécessitent des clés pour le chiffrement et le déchiffrement. Deux principaux types d'algorithmes de chiffrement existent :

Le cryptage symétrique : utilise la même clé pour le chiffrement et le déchiffrement. Il est également appelé cryptage à clé secrète. Les algorithmes symétriques sont normalement utilisés pour crypter le contenu d'un message. Deux principaux types d'algorithmes de chiffrement symétrique existent :

- Le cryptage de « Stream » (en continu), comme le RC4.
- Le cryptage par blocs, tels que : DES, Triple DES (3DES) et Advanced Encryption Standard (AES).

Le cryptage asymétrique: est l'utilisation des différentes clés pour le chiffrement et le déchiffrement. Le chiffrement asymétrique est aussi appelée cryptage à clé publique. Un système de chiffrement asymétrique est composé de deux clé de calculs associés. Une, connue dans le domaine public, est appelée la clé publique, l'autre n'est connue que par le propriétaire de la paire des clés. Selon l'utilisation des paires de clés publiques et privées, les algorithmes asymétriques peut être utilisée à des fins de chiffrement ou d'authentification.

Parce que les algorithmes symétriques sont beaucoup plus rapides que les algorithmes asymétriques, la certification numérique ou de gestion des clés est plus couramment utilisée pour le chiffrement des données que les algorithmes asymétriques. Les exemples populaires des algorithmes asymétriques sont Diffie-Hellman (DH) algorithmes et Rivest, Shamir et Adelman (RSA).

c. Signatures numériques et certification numérique :

L'authentification et l'intégrité sont des propriétés importantes pour les VPN sécurisés. Il s'agit notamment de l'authentification de l'entité, de l'origine des données, de l'intégrité et la non-répudiation. Les signatures numériques et les certificats fournissent un système de confiance évolutif.

La signature numérique se réfère à l'action du chiffrage du hachage des données à l'aide des clés privées de l'expéditeur. Le résultat est appelée une signature numérique. La signature peut être facilement vérifiée a l'aide de la clé publique correspondante qui est disponible dans le domaine public.

Un certificat numérique est essentiellement une liaison entre l'identité d'un utilisateur et sa clé publique. Les certificats numériques sont émis par une entité étrangère appelée autorité de certification (CA), qui permet d'assurer la confiance et l'authenticité du certificat.

5) Les étapes principales d'une connexion SSL :

Cette section porte sur les messages et les opérations nécessaires pour établir une connexion SSL. On décrira comment les différents éléments évoqués jusqu'ici (algorithmes cryptographiques et les protocoles SSL) travaillent ensemble pour établir une connexion SSL.

Les protocoles Handshake SSL sont utilisés pour que le client et le serveur SSL établissent la connexion. Les principales étapes de ce processus sont les suivantes:

- **Des fonctions de sécurité Négociante :** Cette version gère les protocoles et les suites de chiffrement.
- **L'authentification :** Le client authentifie le serveur. facultativement, le serveur peut également authentifier les clients.
- **L'échange de clés :** les deux parties échangent des clés ou des informations qui sont nécessaires pour générer les clés principales.
- **Le détournement de Clés :** Les deux parties détournent la clé principale qui est ensuite utilisé pour générer des clés utilisées pour le chiffrement des données.

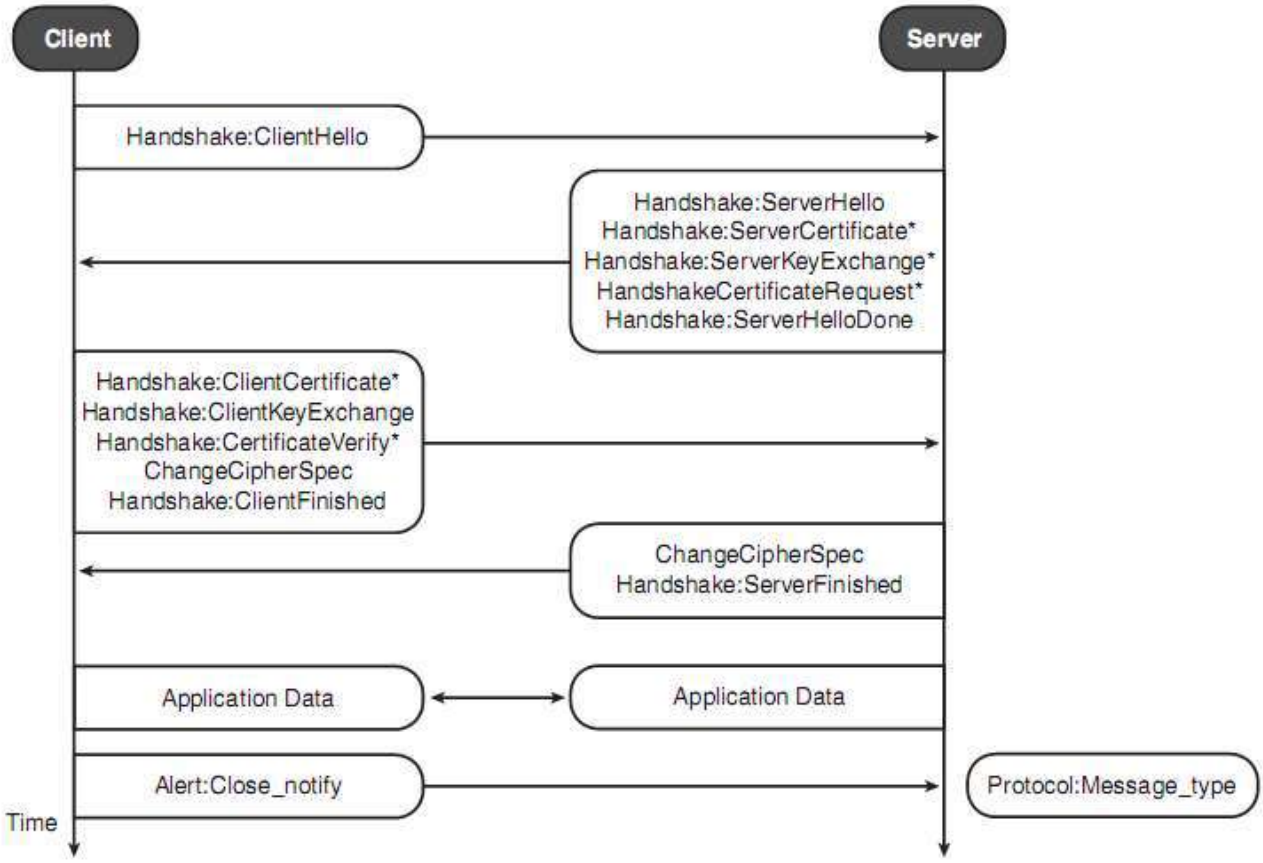


Figure 3 : Handshake SSL

6) Les méthodes d'accès utilisé par SSL VPN:

- **Reverse-proxy :** Le reverse-proxy est basée sur la méthode d'accès est la plus courante pour les utilisateurs. Seul un nombre limité d'applications qui peuvent être utilisés par le Web sont pris en charge. Il s'agit normalement d'applications WEB e-mail comme par exemple le Microsoft OWA (Outlook Web Access). Jusqu'à ces dernières années, ce fut la cause principale pour l'utilisation de SSL VPN.
- **Redirection de port :** cette méthode peut être utilisée pour donner un accès aux partenaires d'affaires ou entrepreneurs qui ont besoin d'accéder à un nombre très limité d'applications client/serveur qui ne sont pas adapté au web. Cependant, la plupart de ces solutions ne prennent pas en charge les données TCP et ne peuvent supporter les applications qui utilisent des types de protocoles tels que l'UDP ou l'ICMP. En outre, la plupart d'entre elles ne peuvent supporter les applications réseau qui utilisent les plages d'adresses dynamiques des ports TCP, telles que la VoIP, la messagerie instantanée et le NetMeeting.
- **Tunnel client** : également connu sous le nom d'un client VPN SSL complet. Il est similaire à un client VPN IPSec standard, mais toutes les données sont envoyées via le protocole SSL. établir une connexion se fait donc sans la nécessité de déployer une

application client ou un agent sur l'ordinateur distant. Les tunnels peuvent être utilisés pour aider les utilisateurs qui ont besoin de pouvoir accéder à des ressources intégrales. En raison des exigences de privilèges d'utilisateur et la nature de l'accès au réseau complet, les clients du tunnel ne devraient être déployés sur les systèmes des utilisateurs corporatifs, tels que les ordinateurs portables de travail.

7) Les produits Cisco VPN SSL :

Cisco Systems a introduit la notion SSL VPN dans sa ligne de produits concentrateur VPN 3000.

En mi 2005, Cisco a présenté la série 5500 Adaptive Security Appliance (ASA) pour fournir une solution de sécurité complète pour les entreprises, qu'il s'agisse d'un pare-feu, VPN, système de prévention d'intrusion (IPS), système de détection d'intrusion (IDS), ou même de filtrage du contenu. Pour apporter une solution VPN complète, Cisco a implanté toutes les fonctionnalités spécifiques du VPN de la ligne des produits VPN 3000 dans ses produits ASA. En outre, un nombre significatif de IPsec et SSL VPN caractéristiques ont également été introduits dans la gamme de produits ASA.

Cisco offre actuellement la fonctionnalité SSL VPN (**WEBVPN**) dans un certain nombre de ses produits :

- Concentrateur Cisco VPN 3000 séries
- Cisco ASA 5500 séries
- Cisco VPN routeurs

Et pour fournir une solution VPN SSL complète pour les entreprises, Cisco propose également un certain nombre d'applications et produits :

- Cisco AnyConnect VPN client
- Cisco Security Device Manager (SDM)
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco Security Manager (CSM)

En outre, Cisco a introduit la fonctionnalité SSL VPN dans la quasi-totalité de ses IOS ligne de produits routeurs. Sept routeurs Cisco IOS supportent le **WEBVPN** :

- Cisco 870 séries
- Cisco 1800 séries
- Cisco 2800 séries
- Cisco 3700 séries
- Cisco 3800 séries
- Cisco 7200 séries (IOS utilisé dans la mise en œuvre technique)
- Cisco 7300 séries

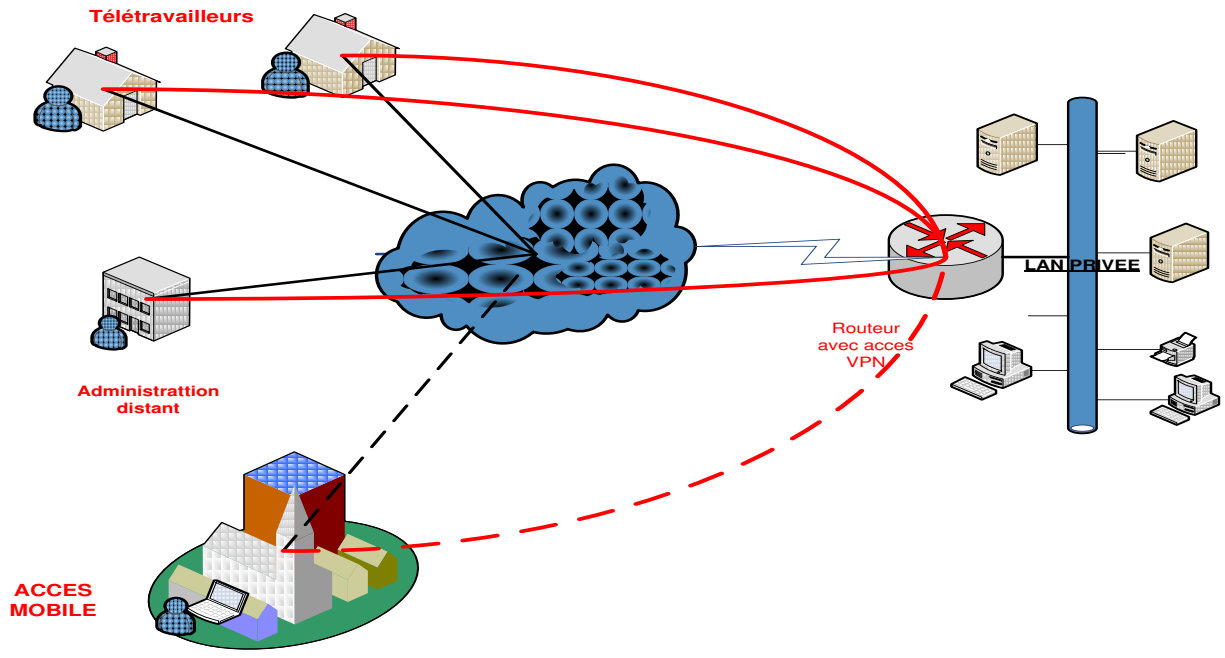
Le support de SSL VPN dans la large gamme de produits IOS peut permettre à toute entreprise, qu'il s'agisse de petites ou moyennes, de fournir un accès VPN distance peu onéreux et robuste dans son infrastructure réseaux.

Partie Pratique :

Une connexion VPN étend la limite physique des réseaux. Les ordinateurs qui ont accès à un VPN peuvent potentiellement accéder à toutes les ressources du réseau privé, comme s'ils étaient physiquement connectés. Cela permet à des travailleurs, des consultants, des fournisseurs externes de se connecter au réseau de l'entreprise à partir de n'importe quel endroit sur la terre, et d'effectuer leur travaux à distance. Le nombre de connexions VPN simultanées n'est limité que par la bande passante du réseau public et les performances du serveur/appareil VPN.

Le VPN fournit le cryptage des données et des mesures de sécurité supplémentaires pour s'assurer que seuls les utilisateurs autorisés ont accès au réseau et ses données. Le trafic est crypté dans les deux sens pendant qu'il parcourt le réseau public.

VPN est une méthode sécurisée qui permet un accès distant aux utilisateurs d'un réseau privé (et dans la plupart des cas - moins cher et plus rapide que les anciennes connexions dial-up), les VPN sont généralement utilisés dans les cas où les utilisateurs doivent avoir un accès distance sécurisé aux ressources réseau qui n'a pas pu être consulté par tout autre moyen. Par exemple, les VPN permettent à distant aux administrateurs de diagnostiquer et de résoudre les problèmes et effectuer des tâches de gestion du réseau privée.



VII. Mise en œuvre technique :

Dans l'IOS ver. 12.3 (14) T Cisco introduit la fonctionnalité Cisco VPN SSL, baptisée **WebVPN**. Cette fonctionnalité permet de configurer un routeur pour mettre en fonction « user-based » VPN SSL. En d'autres termes, un routeur avec WebVPN configuré, est en gros un proxy web sécurisé.

Les exigences bureau de l'utilisateur sont essentiellement :

- La prise en charge du SSL navigateur: Internet Explorer, Netscape, Mozilla, ou FireFox.
- Sun Microsystems Java Runtime (pour la redirection de port, ou Client léger).
- En outre, il support les services client e-mail: Microsoft Outlook, Netscape Mail, ou Eudora.

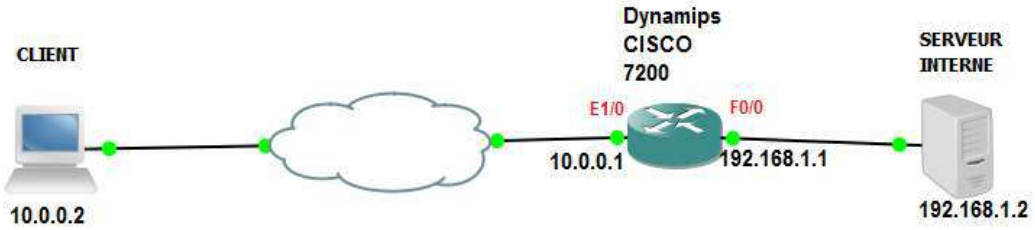
Le VPN SSL utilisent une formule pour le transport des données privées à travers le réseau Internet public. Au lieu de s'en remettre à l'utilisateur final d'avoir un logiciel configurée et sécurisée sur son ordinateur, SSL VPN utilise SSL/HTTPS qui est un mécanisme de transport sécurisé intégré à tous les navigateurs Web standard. Avec le VPN SSL, la connexion entre l'utilisateur et la ressource interne se produit via une connexion HTTPS au niveau de la couche application.

1) Configuration requis :

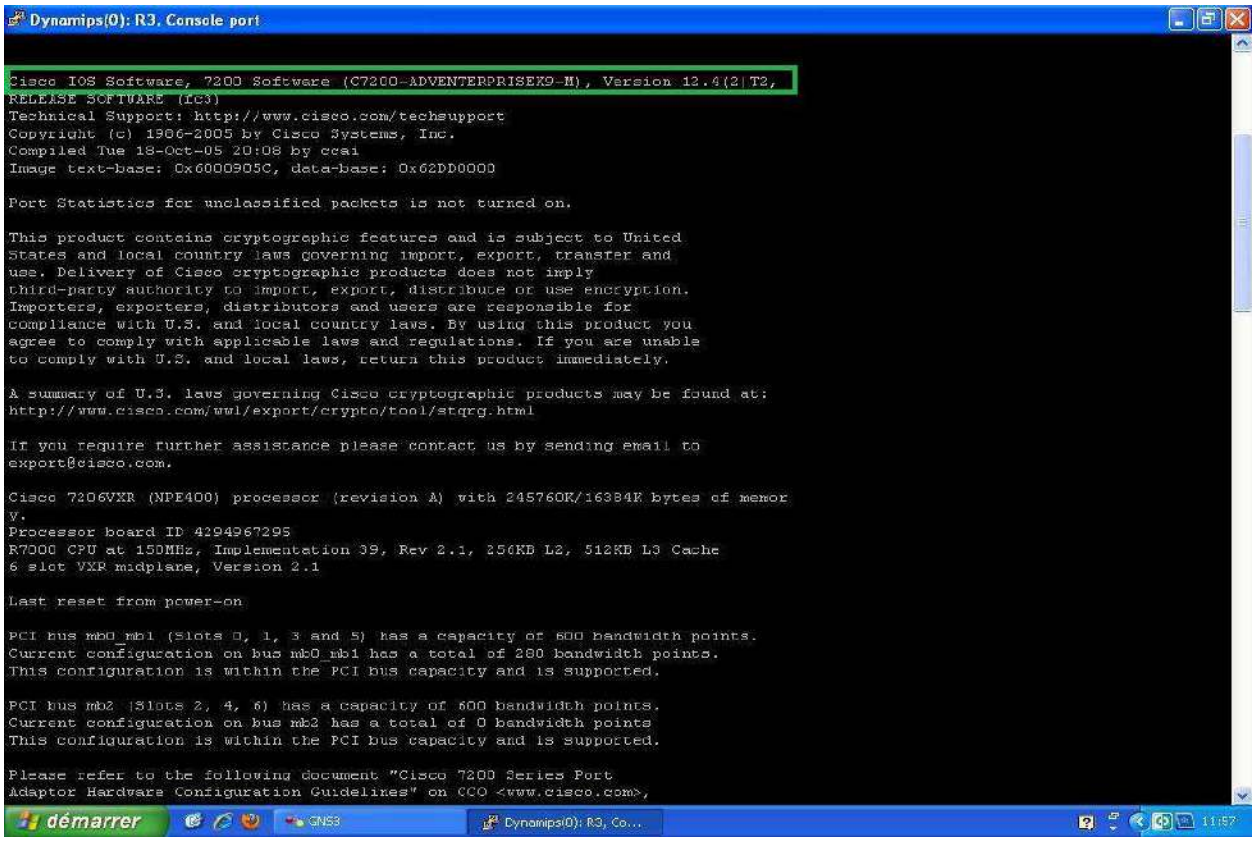
Cette mise en œuvre technique décrit comment configurer Cisco SSL VPN sur les routeurs Cisco IOS ver. 12.4(2) T2.

Le laboratoire est construit sur Dynamips 7200 simulateur dans GNS3 **(voire annexe page 38).**

La topologie utilisée est la suivante :



Le démarrage de Dynamips 7200 simulateur :



La configuration des interfaces et du TELNET :

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#enable secret 1234
Router(config)#line vty 0 4
Router(config-line)#password 1234
Router(config-line)#login
Router(config-line)#exi
Router(config)#int e1/0
Router(config-if)#i add 10.0.0.1 255.255.255.252
% Ambiguous command:  "i add 10.0.0.1 255.255.255.252"
Router(config-if)#ip add 10.0.0.1 255.255.255.252
Router(config-if)#no sh
Router(config-if)#ex
Router(config)#in
*Jul  8 11:50:21.407: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Jul  8 11:50:22.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to upt f0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#
*Jul  8 11:50:47.159: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o down
*Jul  8 11:50:47.159: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Admin
istrative State Down
*Jul  8 11:50:47.159: %ENTITY_ALARM-6-INFO: ASSERT CRITICAL Fa0/0 Physical Port
Link Down
Router(config-if)#ex
```

2) WebVPN installation :

L'installation et la maintenance/suivi des connexions sur les routeurs IOS WebVPN n'est pas difficile. Les étapes suivantes résument ce processus:

Étape 1 : Configuration Préalables: AAA, DNS, et les certificats.
Étape 2 : Configuration du WebVPN.
Étape 3 : Création d'URL et redirections des Ports Entrées pour la page d'accueil (en option, mais recommandé).
Étape 4 : Le maintien, la surveillance et le dépannage des connexions WebVPN.

Dans les sections suivantes, je vais discuter les commandes nécessaires pour effectuer les étapes ci-dessus.

a. La configuration Préalables :

Avant de commencer la configuration WebVPN sur votre routeur, vous aurez besoin pour effectuer certaines tâches préalables qui sont nécessaires pour le WebVPN. Il s'agit notamment de:

Mise en place d'AAA pour authentifier les utilisateurs WebVPN.
Mise en place DNS pour résoudre les informations de nom d'URL.
Obtention d'un certificat SSL pour le routeur.

Les paragraphes qui suivent expliquent ces tâches de manière plus approfondie.

b. AAA Configuration :

Lorsque les utilisateurs veuillent accéder au routeur WebVPN, ils doivent s'authentifier pour que le VPN SSL soit établie. Le nom d'utilisateur et le mot de passe peut être situé localement sur le routeur ou définis sur un serveur AAA en utilisant soit le **TACACS** + ou **RADIUS** protocoles de sécurité. Voici un aperçu des commandes:

Si vous spécifiez « **local** » comme méthode d'authentification pour la connexion de commande **aaa authentification**, le routeur va chercher les noms d'utilisateur défini par la commande **username** sur le routeur. Si vous spécifiez **group TACACS +** ou **group RADIUS**, vous aurez besoin de configurer un serveur AAA (le TACACS-serveur et serveur radius-commandes, respectivement).

c. Configuration DNS

Le DNS est nécessaire pour le WebVPN :

- Pour générer une paire de clés RSA pour protéger les connexions SSL.
- Pour résoudre les noms dans les URL (rappelez-vous que le routeur agit comme un proxy web).

La configuration du DNS :

```
Router(config)#ip domain-name IFIAG.com
Router(config)#ip name-server 10.0.0.1
```

La commande **ip domain-name** est nécessaire pour générer des clés RSA sur le routeur qui sera utilisé pour le certificat SSL. La commande **ip name-server** vous permet de spécifier jusqu'à six serveurs DNS que le routeur peut utiliser pour résoudre les noms de domaine complets.

d. Configuration certificat SSL

Pour utiliser SSL, le routeur WebVPN a besoin d'un **certificat**: les clés sur le certificat sont utilisées pour protéger les données entre le bureau de l'utilisateur et le routeur. Il ya deux façons pour obtenir un certificat du routeur:

- Obtenir un certificat d'un CA
- Créer un certificat auto-signé

Dans cette section, j'ai configuré un certificat auto-signé, ce qui implique les commandes suivantes:

```
Router(config)#crypto ca trustpoint SSLVPN
Router(ca-trustpoint)#enrollment selfsigned
Router(ca-trustpoint)#subject-name CN=SSLVPN OU=cisco O=cisco
Router(ca-trustpoint)#rsakeypair SSLVPN 512
Router(ca-trustpoint)#exi
```

Comme vous pouvez le voir sur les commandes ci-dessus, cette procédure est identique à l'obtention d'un certificat d'un CA. La commande **crypto ca trustpoint** spécifie un point de confiance ; pour un certificat auto-signé, le routeur lui-même est un **trustpoint**: donc, le nom donné n'a pas d'importance. Cependant, Cisco recommande généralement l'utilisation de "SSLVPN," parce que c'est le **trustpoint** par défaut qui utilise WebVPN.

La commande **enrollment selfsigned** précise que le routeur obtient un certificat d'lui-même. La commande **subject-name** spécifie les éléments à être mis sur le certificat. La commande **rsakeypair** spécifie une étiquette de clé à utiliser pour les clés RSA et le module à utiliser lors de la création de la signature et les clés de chiffrement.

Lorsque vous générez votre certificat auto-signé avec la commande **crypto pki enroll**, le routeur génère la paire de clés RSA et le certificat auto-signé.

```
Router(config)#crypto pki enroll SSLVPN
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Generate Self Signed Router Certificate? [yes/no]: y

Router Self Signed Certificate successfully created
```

Une fois cela fait, vous pouvez utiliser les commandes d'affichage **show crypto key mypubkey rsa** pour afficher les deux paires de clés créé ; et **show crypto ca certificates** pour afficher le certificat auto-signé qui a été généré.

```
Router(config)#do sh crypto ca certificates
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    hostname=Router.IFIAG.com
    cn=SSLVPN OU\=cisco O\=cisco
  Subject:
    Name: Router.IFIAG.com
    hostname=Router.IFIAG.com
    cn=SSLVPN OU\=cisco O\=cisco
  Validity Date:
    start date: 11:52:55 UTC Jul 8 2010
    end   date: 00:00:00 UTC Jan 1 2020
  Associated Trustpoints: SSLVPN

Router(config)#do sh crypto key mypubkey rsa
% Key pair was generated at: 11:52:46 UTC Jul 8 2010
Key name: SSLVPN
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D98F67 DC030074
  3D807019 86BC60B9 23D13681 49B2EAA5 93988496 84347E34 CD592EFE 5F774245
  8C93B831 5C0BDC60 67BF8FD1 63E861B4 4BAC0D29 EAF7F106 CF020301 0001
% Key pair was generated at: 11:52:47 UTC Jul 8 2010
Key name: SSLVPN.server
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DD3682 DD01A3ED
  5E9356B3 5C882F24 7E641C45 B99C573F 6DFEEF87 547CB4B8 01976AA7 FCB5E4C4
  FC0178FF 19E487C5 9A0061E1 13EEFE4E 9E11F26F 01A2AF02 0994CEBE E4AABDD1
  A9502940 CBCA93A0 944078D2 A5722DC1 90D9C993 01E9EAE0 CF020301 0001
```

3) Commandes IOS pour activer la fonctionnalité WEBVPN

Une fois votre certificat importé, nous allons pouvoir configurer la fonctionnalité WebVPN proprement parlé.

```
Router(config)#webvpn enable gateway-addr 10.0.0.1
Router(config)#webvpn
Router(config-webvpn)#ssl trustpoint SSLVPN
Router(config-webvpn)#title "CISCO Portable Page"
Router(config-webvpn)#text-color black
Router(config-webvpn)#secondary-text-color black
Router(config-webvpn)#$votre LOGIN et MOTSDEPASS avant de continuer"
Router(config-webvpn)#ssl encryption rc4-md5
Router(config-webvpn)#idle-timeout 300
Router(config-webvpn)#url-list SSLVPNaccess
Router(config-webvpn-url)#heading "VPN IFIAG URLs"
Router(config-webvpn-url)#$IAG url-value http://www.SSlVPN.ifiag.com
URL entry with text "IFIAG" exists
Router(config-webvpn-url)#$port 7200 remote-server 192.168.1.2 remote-port 23
Router(config-webvpn)#exi
Router(config)#_
```

La commande **WebVPN enable** permet d'activer les services WebVPN sur le routeur. En option, vous pouvez spécifier une adresse IP sur le routeur qui terminera la connexion

WebVPN, sinon, le routeur acceptera les sessions WebVPN sur l'une de ses adresses IP configurées

La commande **WebVPN** passe en mode de sous-commande WebVPN on peut configurer les paramètres d'interaction avec le client et la page d'accueil WebVPN. La commande **ssl trustpoint** spécifie le « trustpoint » qui a le certificat du routeur WebVPN utilisable. Pour les certificats auto-signés, si on avait spécifié le nom trustpoint comme **SSLVPN**, il n'est pas nécessaire de préciser les trustpoint en mode sous-commande. La commande de cryptage SSL spécifie le chiffrement des paquets et l'algorithme d'authentification à utiliser. Par défaut, les algorithmes spécifiés dans la commande ci-dessus sont activés dans l'ordre indiqué. Avec la commande de cryptage SSL, vous pouvez modifier l'ordre des algorithmes ou les algorithmes à utiliser.

La commande **title** permet de créer un titre pour la page d'accueil qui apparaît une fois un utilisateur s'authentifie. Le titre peut contenir jusqu'à 255 caractères; si le titre n'est pas définie, il est par défaut "**WebVPN service**". **title-color** spécifie la couleur de la barre de titre doit être, par défaut, il est violet. La valeur est limitée à 32 caractères. La commande **text-color** indique la couleur du texte dans la barre de titre doit être mis sur la page d'accueil WebVPN. Cela peut être noir ou blanc.

La commande **secondary-color** Spécifie la couleur que les barres de titre secondaire devraient être sur la page d'accueil WebVPN. La commande **secondary-text-color** spécifie la couleur du texte dans les barres de titre secondaire; si vous omettez cette commande, la valeur par défaut est la couleur au noir.
La commande **login-message** spécifie une position qui apparaît au-dessus du nom d'utilisateur et du mot de passe. Le message de connexion peuvent être jusqu'à 255 caractères, il est par défaut "Please enter your username and password."

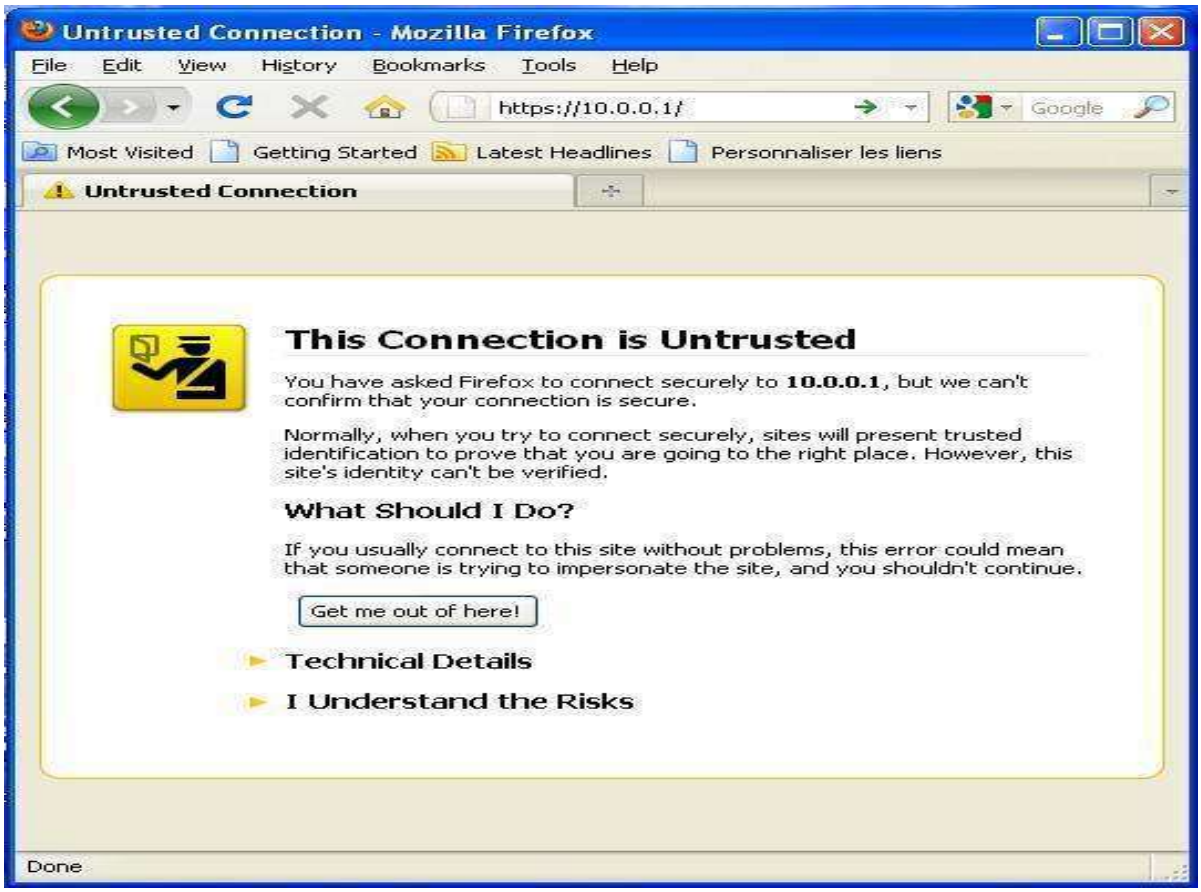
La commande idle-timeout spécifie le nombre de secondes pour maintenir la session WebVPN ouvert.

P.S : Les commandes **WebVPN enable** et **WebVPN** sont les deux seuls nécessaires pour permettre WebVPN sur votre routeur, en supposant que le trustpoint est appelé "SSLVPN."

Enfin, la commande **port-forward list telnet local-port 60001 remote-server 192.168.1.3 remote-port 23** est configuré pour le Telnet. Dans ce cas, lorsqu'un utilisateur clique sur le bouton «Démarrer Application Access" lien hypertexte, la fenêtre de transfert de port s'ouvre. Il indique l'adresse IP réelle et le numéro de port, l'utilisateur doit telnet, d'accéder à Telnet sur le serveur distant. Dans cet exemple, si l'utilisateur telnets à 127.0.0.1 sur le port 60001, le code JavaScript WebVPN JavaScript redirects renvoi la requête vers le serveur réelle (192.168.1.3) sur le port 23.

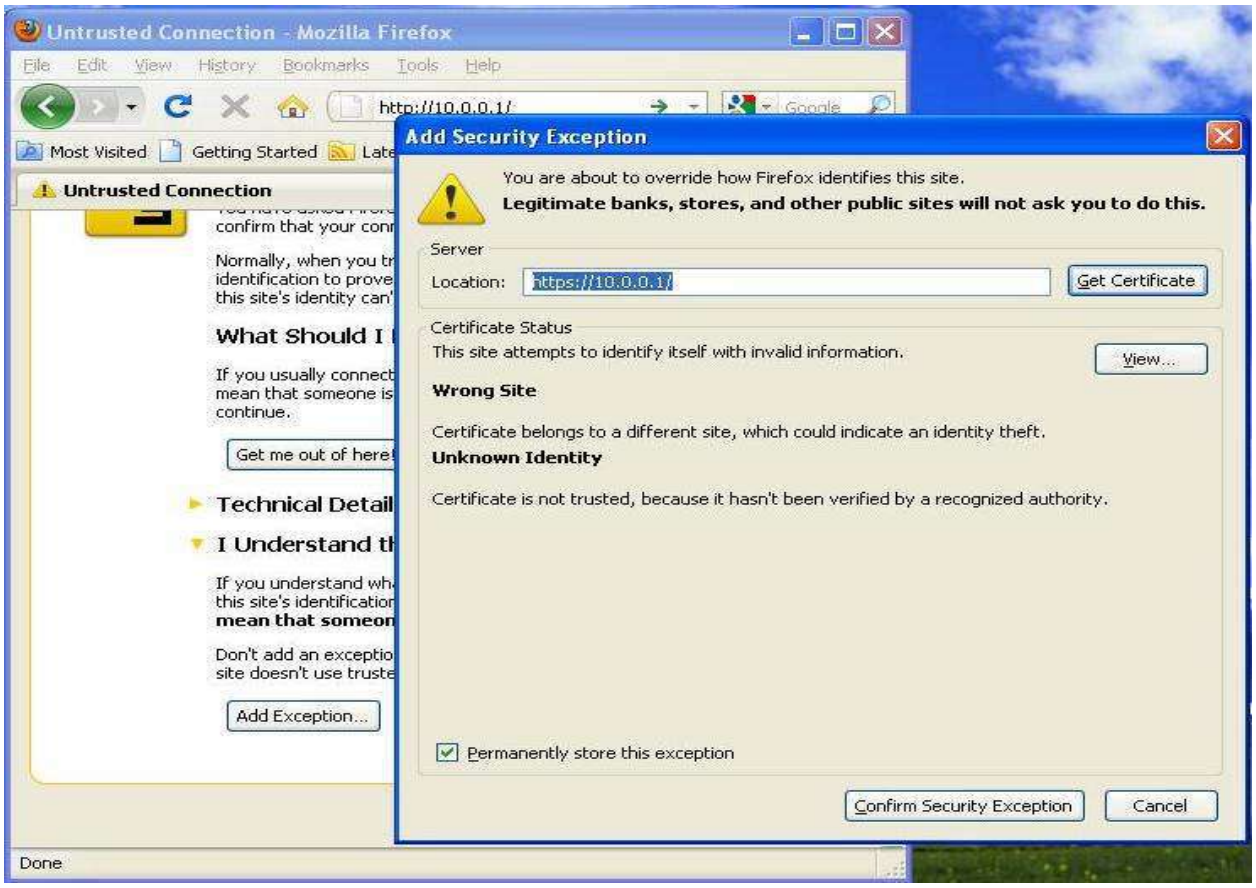
4) Test de fonctionnalité (navigation Web) :

J'ai utilisé Firefox pour tester la fonctionnalité WebVPN. J'ai entré **"http://10.0.0.1/"** dans la barre d'adresse.



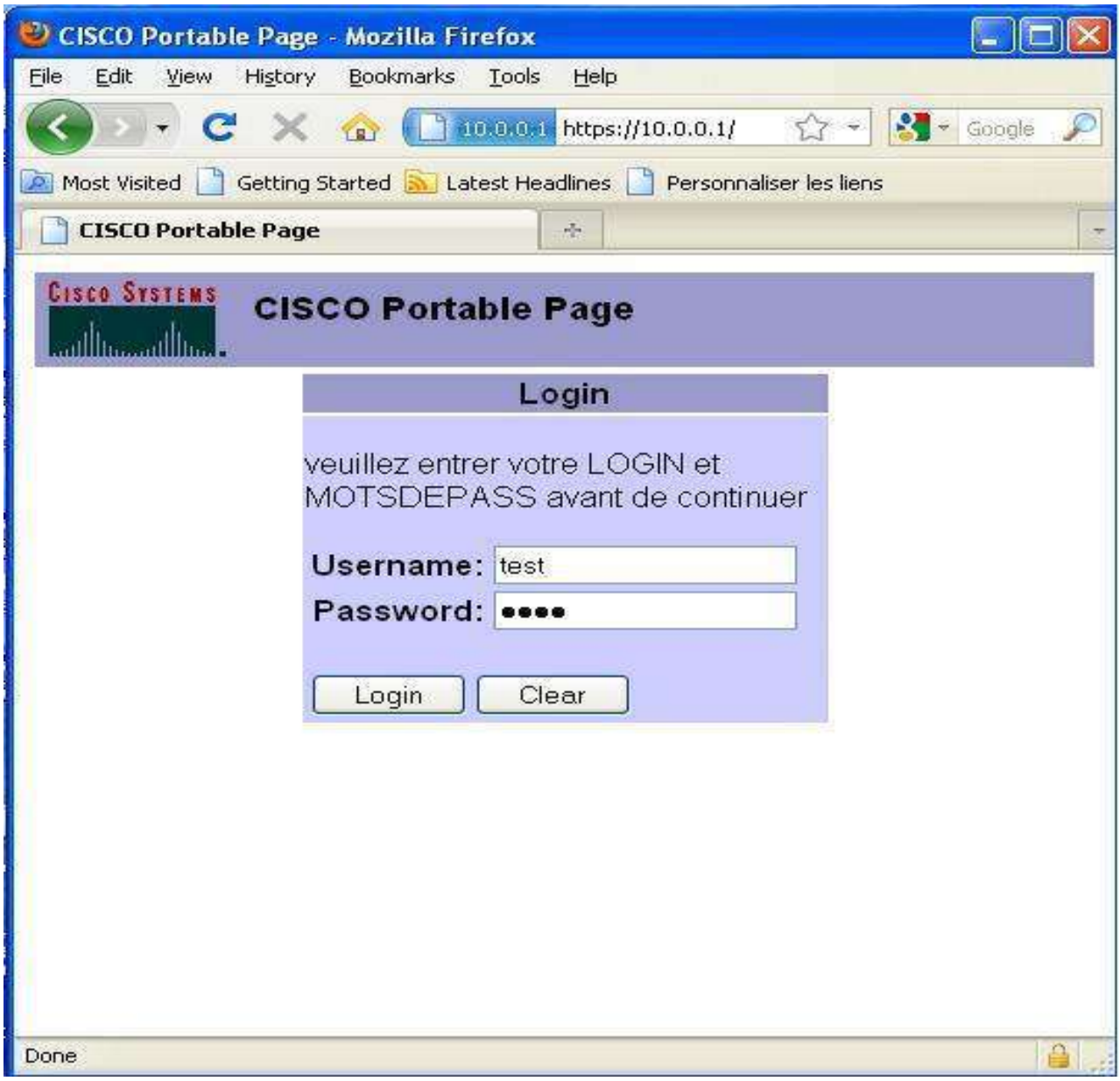
Le navigateur WEB indique que le site est non fiable.

J'oblige le navigateur à accéder au site.

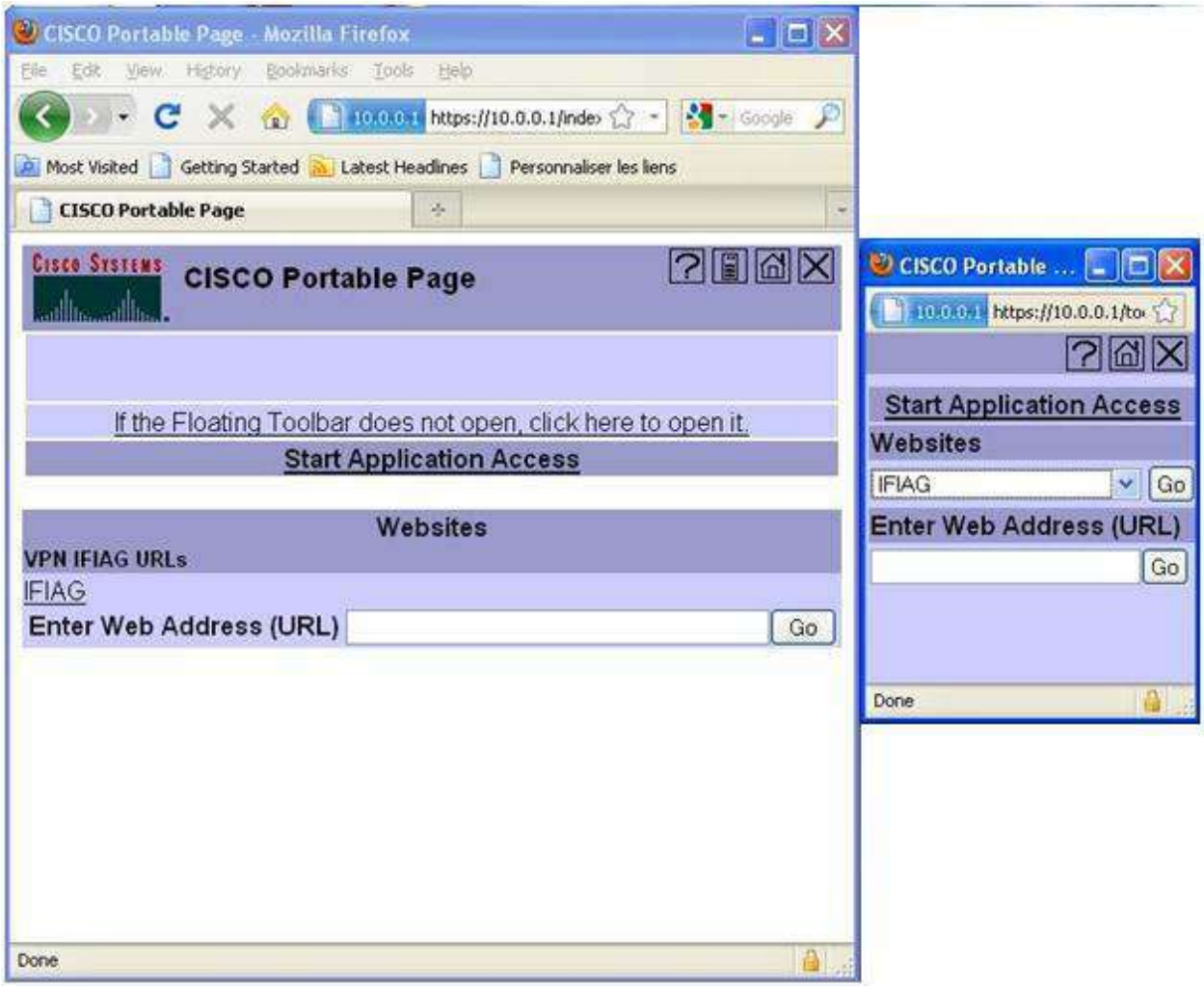


Le navigateur me donne la possibilité de télécharger le certificat préconfiguré dans le routeur WEBVPN.

Après l'authentification du certificat, la page d'accueil WebVPN s'affiche



J'entre mon login et mots de passe configurer dans le serveur AAA (dans notre cas le routeur lui-même) « TEST ; 1234 »



.

Maintenant, j'ai succéder à l'accès au WEBVPN.

5) Vérification de fonctionnalité (WIRESHARK) :

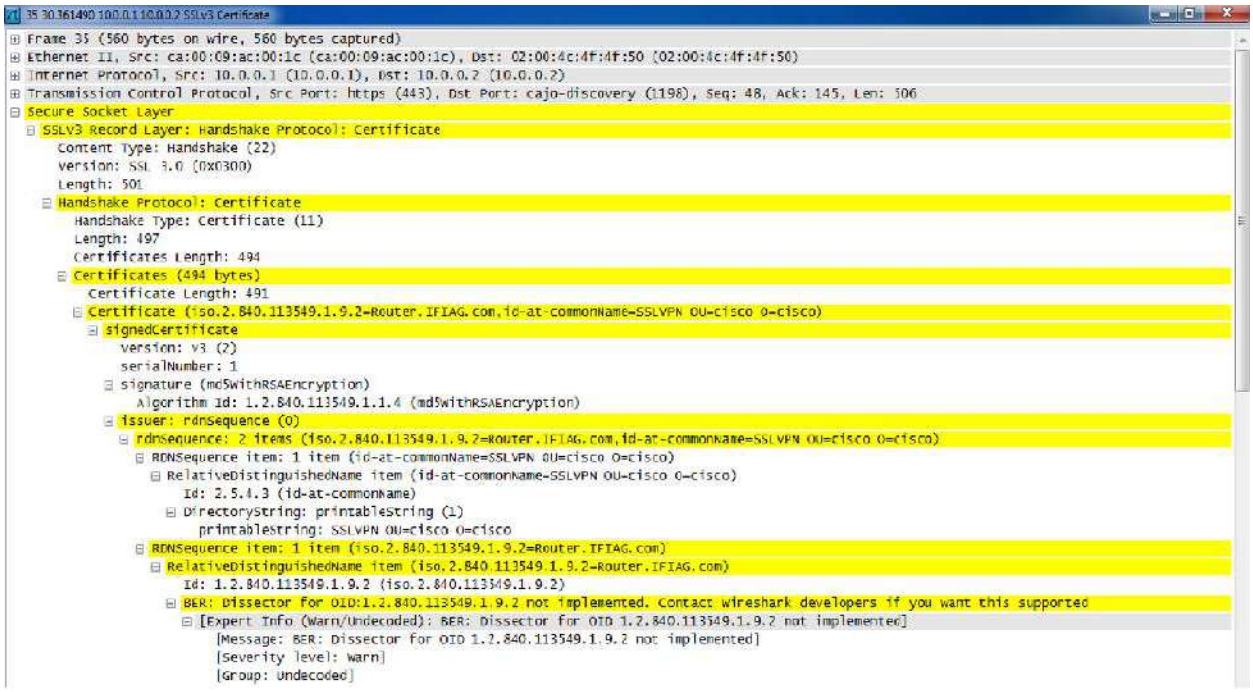
J'ai utilisé WIRESHARK pour la capture du trafic entre l'ordinateur distant et le routeur

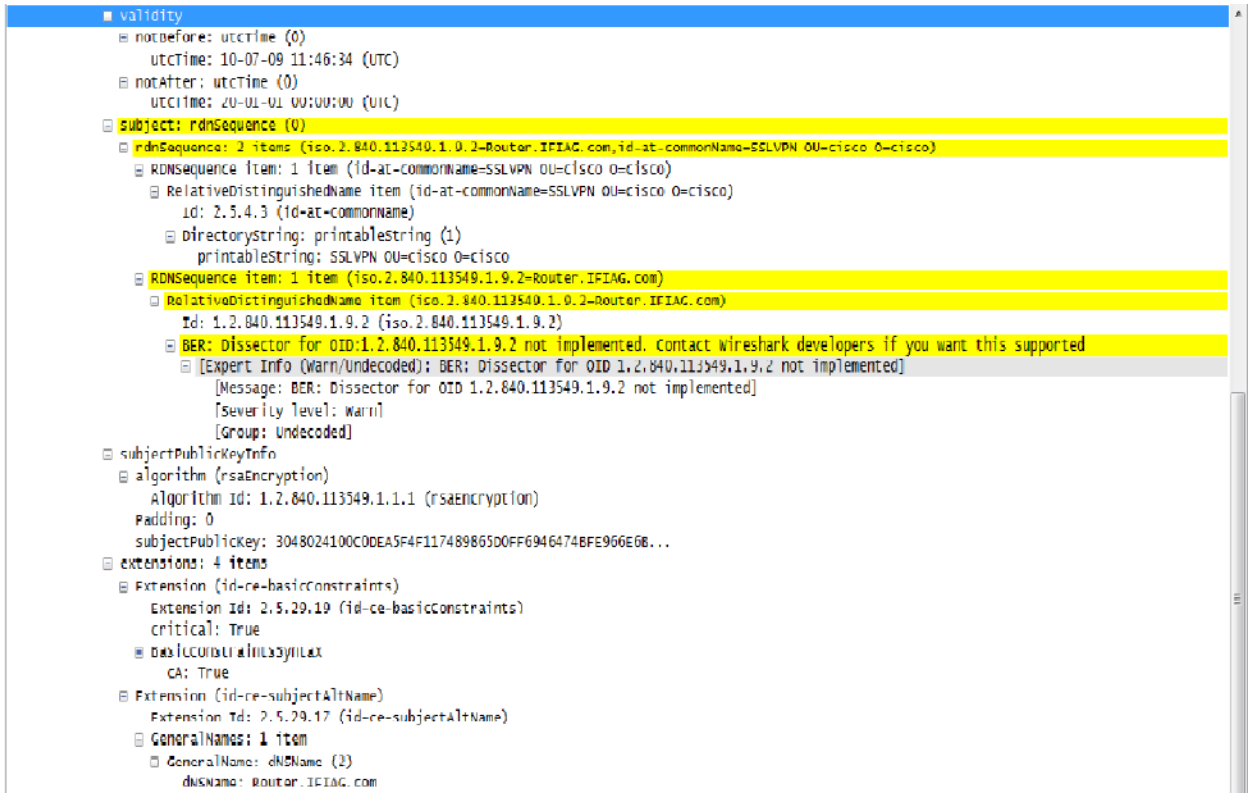
No.	Time	Source	Destination	Protocol	Info
40	30.410401	10.0.0.2	10.0.0.1	TCP	cajo-discovery > https [RST, ACK] Seq=153 Ack=563 Win=0 Len=0
41	30.530452	10.0.0.2	10.0.0.1	TCP	dmidi > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
42	30.561198	10.0.0.1	10.0.0.2	TCP	https > cajo-discovery [FIN, PSH, ACK] Seq=563 Ack=152 Win=3977 Len=0
43	30.561237	10.0.0.2	10.0.0.1	TCP	cajo-discovery > https [RST] Seq=152 Win=0 Len=0
44	30.561617	10.0.0.1	10.0.0.2	TCP	https > cajo-discovery [ACK] Seq=564 Ack=153 Win=3977 Len=0
45	30.561647	10.0.0.2	10.0.0.1	TCP	cajo-discovery > https [RST] Seq=153 Win=0 Len=0
46	30.637660	10.0.0.1	10.0.0.2	TCP	https > dmidi [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
47	30.637711	10.0.0.2	10.0.0.1	TCP	dmidi > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
48	30.696297	10.0.0.2	10.0.0.1	SSL	Client Hello
49	30.873419	10.0.0.1	10.0.0.2	SSLv3	Server Hello
50	30.876917	10.0.0.1	10.0.0.2	SSLv3	Certificate
51	30.876971	10.0.0.2	10.0.0.1	TCP	dmidi > https [ACK] Seq=145 Ack=554 Win=16967 Len=0
52	30.878527	10.0.0.2	10.0.0.1	SSLv3	Alert (Level: Fatal, Description: Certificate Unknown)
53	30.878774	10.0.0.2	10.0.0.1	TCP	dmidi > https [FIN, ACK] Seq=152 Ack=554 Win=16967 Len=0
54	30.889807	10.0.0.1	10.0.0.2	SSLv3	Server Hello Done
55	30.889876	10.0.0.2	10.0.0.1	TCP	dmidi > https [RST, ACK] Seq=153 Ack=563 Win=0 Len=0
56	31.016419	10.0.0.1	10.0.0.2	TCP	https > dmidi [FIN, PSH, ACK] Seq=563 Ack=152 Win=3977 Len=0
57	31.016458	10.0.0.2	10.0.0.1	TCP	dmidi > https [RST] Seq=152 Win=0 Len=0
58	31.017142	10.0.0.1	10.0.0.2	TCP	https > dmidi [ACK] Seq=564 Ack=153 Win=3977 Len=0
59	31.017174	10.0.0.2	10.0.0.1	TCP	dmidi > https [RST] Seq=153 Win=0 Len=0
60	33.829142	10.0.0.2	10.0.0.1	TCP	scol > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
61	33.954016	10.0.0.1	10.0.0.2	TCP	https > scol [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
62	33.954067	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
63	34.019909	10.0.0.2	10.0.0.1	SSL	Client Hello

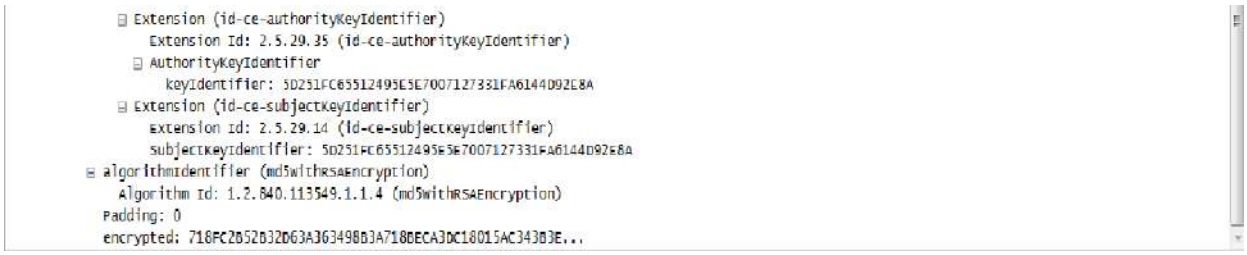
N° 63 : le début de l'envoi des packet SSL.

62	33.954067	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
63	34.019909	10.0.0.2	10.0.0.1	SSL	Client Hello
64	34.157016	10.0.0.1	10.0.0.2	SSLv3	Server Hello
65	34.160739	10.0.0.1	10.0.0.2	SSLv3	Certificate
66	34.160792	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=145 Ack=554 Win=16967 Len=0
67	34.177186	10.0.0.1	10.0.0.2	SSLv3	Server Hello Done
68	34.177838	10.0.0.2	10.0.0.1	SSLv3	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
69	34.390710	10.0.0.1	10.0.0.2	SSLv3	Change Cipher Spec
70	34.392986	10.0.0.1	10.0.0.2	SSLv3	Encrypted Handshake Message
71	34.393040	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=285 Ack=630 Win=16891 Len=0
72	34.393874	10.0.0.2	10.0.0.1	SSLv3	Application Data
73	34.592300	10.0.0.1	10.0.0.2	SSLv3	Application Data
74	34.595804	10.0.0.1	10.0.0.2	TCP	[TCP segment of a reassembled PDU]
75	34.595857	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=668 Ack=2271 Win=17520 Len=0
76	34.732490	10.0.0.1	10.0.0.2	TCP	[TCP segment of a reassembled PDU]
77	34.733202	10.0.0.1	10.0.0.2	SSLv3	Application Data
78	34.733250	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=668 Ack=3753 Win=17520 Len=0
79	34.749991	10.0.0.2	10.0.0.1	SSLv3	Application Data
80	34.857841	10.0.0.2	10.0.0.1	TCP	nucleus-sand > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
81	34.891307	10.0.0.1	10.0.0.2	SSLv3	Application Data
82	34.893520	10.0.0.1	10.0.0.2	SSLv3	Application Data
83	34.893573	10.0.0.2	10.0.0.1	TCP	scol > https [ACK] Seq=1062 Ack=4360 Win=16913 Len=0

Voila on détaille la certificat comme il est définie par WIRESHARK (N°65) :


35 30.361490 100.0.1 10.0.0.2 SSLv3 Certificate
Frame 35 (560 bytes on wire, 560 bytes captured)
Ethernet II, Src: ca:00:09:ac:00:1c (ca:00:09:ac:00:1c), Dst: 02:00:4c:4f:4f:50 (02:00:4c:4f:4f:50)
Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
Transmission Control Protocol, Src Port: https (443), Dst Port: cajo-discovery (1198), Seq: 48, Ack: 145, Len: 506
Secure Socket Layer
SSLv3 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 501
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 497
Certificates Length: 494
Certificates (494 bytes)
Certificate Length: 491
Certificate (iso.2.840.113549.1.9.2=Router.IFIAG.com,id-at-commonName=SSLVPN OU=cisco O=cisco)
signedCertificate
version: v3 (2)
serialNumber: 1
signature (md5WithRSAEncryption)
Algorithm Id: 1.2.840.113549.1.1.4 (md5WithRSAEncryption)
issuer: rdnSequence (0)
rdnSequence: 2 items (iso.2.840.113549.1.9.2=Router.IFIAG.com,id-at-commonName=SSLVPN OU=cisco O=cisco)
RDNSequence item: 1 item (id-at-commonName=SSLVPN OU=cisco O=cisco)
RelativeDistinguishedName item (id-at-commonName=SSLVPN OU=cisco O=cisco)
Id: 2.5.4.3 (id-at-commonName)
DirectoryString: printableString (1)
printableString: SSLVPN OU=cisco O=cisco
RDNSequence item: 1 item (iso.2.840.113549.1.9.2=Router.IFIAG.com)
RelativeDistinguishedName item (iso.2.840.113549.1.9.2=Router.IFIAG.com)
Id: 1.2.840.113549.1.9.2 (iso.2.840.113549.1.9.2)
BER: Dissector for OID:1.2.840.113549.1.9.2 not implemented. Contact Wireshark developers if you want this supported
[Expert Info (Warn/Undecoded): BER: Dissector for OID 1.2.840.113549.1.9.2 not implemented]
[Message: BER: Dissector for OID 1.2.840.113549.1.9.2 not implemented]
[Severity level: Warn]
[Group: Undecoded]

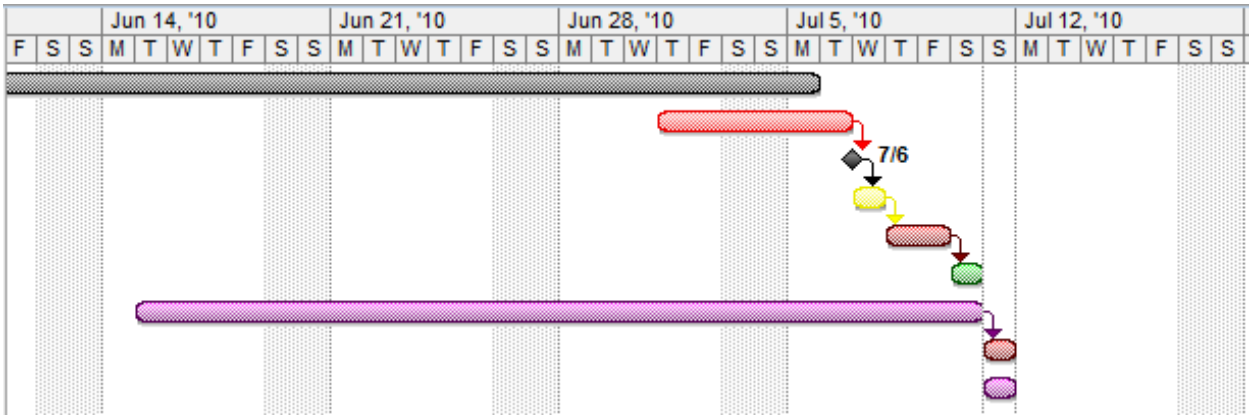

validity
notBefore: utcTime (0)
utcTime: 10-07-09 11:46:34 (UTC)
notAfter: utcTime (0)
utcTime: 20-01-01 00:00:00 (UTC)
subject: rdnSequence (0)
rdnSequence: 2 items (iso.2.840.113549.1.9.2=Router.IFIAG.com,id-at-commonName=SSLVPN OU=cisco O=cisco)
RDNSequence item: 1 item (id-at-commonName=SSLVPN OU=cisco O=cisco)
RelativeDistinguishedName item (id-at-commonName=SSLVPN OU=cisco O=cisco)
Id: 2.5.4.3 (id-at-commonName)
DirectoryString: printableString (1)
printableString: SSLVPN OU=cisco O=cisco
RDNSequence item: 1 item (iso.2.840.113549.1.9.2=Router.IFIAG.com)
RelativeDistinguishedName item (iso.2.840.113549.1.9.2=Router.IFIAG.com)
Id: 1.2.840.113549.1.9.2 (iso.2.840.113549.1.9.2)
BER: Dissector for OID:1.2.840.113549.1.9.2 not implemented. Contact Wireshark developers if you want this supported
[Expert Info (Warn/Undecoded): BER: Dissector for OID 1.2.840.113549.1.9.2 not implemented]
[Message: BER: Dissector for OID 1.2.840.113549.1.9.2 not implemented]
[Severity level: Warn]
[Group: Undecoded]
subjectPublicKeyInfo
algorithm (rsaEncryption)
Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
Padding: 0
subjectPublicKey: 3048024100C0DEA5F4F117489865D0FF6946474BFE966E68...
extensions: 4 items
Extension (id-ce-basicConstraints)
Extension Id: 2.5.29.19 (id-ce-basicConstraints)
critical: True
BasicConstraints
CA: True
Extension (id-ce-subjectAltName)
Extension Id: 2.5.29.17 (id-ce-subjectAltName)
GeneralNames: 1 item
GeneralName: dNSName (2)
dNSName: Router.IFIAG.com



On peut remarquer dans le certificat le nom du DNS « router.ifiag.com» l'algorithme utilisé pour le cryptage « RSA » la clé publique du routeur, la clé d'authentification …etc.

PLANING du travail :

	Nom de la tâche	Duration	Start	Finish
1	**LaRecherche**	25 days	Tue 6/1/10	Mon 7/5/10
2	**Recherche logiciel & IOS**	4 days	Thu 7/1/10	Tue 7/6/10
3	**Installation GNS3 ET IOS c7200-adventerprisek9-mz.124-2.T2**	0 days	Tue 7/6/10	Tue 7/6/10
4	**confifuration du nuage (cloud)**	1 day	Wed 7/7/10	Wed 7/7/10
5	**configuration du routeur**	2 days	Thu 7/8/10	Fri 7/9/10
6	**Test de fonctionnement et capture WIRESHARK**	1 day	Sat 7/10/10	Sat 7/10/10
7	**Redaction du rapport**	20 days	Tue 6/15/10	Sat 7/10/10
8	**Fin du projet**	1 day	Sun 7/11/10	Sun 7/11/10
9	**Preparation soutenance**	1 day	Sun 7/11/10	Sun 7/11/10



CONCLUSION :

Ce rapport vous a montré les rudiments de la mise en place d'un routeur avec un service d'accès à distance WebVPN. Normalement, les routeurs ne sont pas utilisés comme serveurs VPN facile, car la configuration est complexe et les « 3000 VPN concentrateurs » et « PIX » et « ASA security appliances » sont plus renforcé sur les capacités d'accès distant.

Toutefois, il existe de nombreux cas où les routeurs sont utilisés comme dispositifs Remote VPN. La dernière partie du rapport traite d'une nouvelle fonctionnalité sur les routeurs: WebVPN. Grâce à cette fonctionnalité, vous pouvez configurer très basique VPN SSL pour les routeurs Cisco.

WEBOGRAPHIE :

http://www.ciscopress.com/articles/article.asp?p=606584&seqNum=4

http://www.realexam.net/

http://www.gns3.net/

http://www.gns3-labs.com

http://www.internet-computer-security.com

BIBLIOGRAPHIE:

The Complete Cisco VPN Configuration Guide; By Richard Deal

Cisco IOS Cookbook, 2nd Edition; By Kevin Dooley, Ian Brown

Les Réseaux - 6éme Ed - Eyrolles

GLOSSAIRE:

VPN = virtual private network

SSL = Secure Sockets Layer

WAN = Wide Area Network

IPSec = internet protocol security

L2TP = Layer 2 Tunneling Protocol.

DES = Data Encryption Standard

AES = Advanced Encryption Standard

MD5 = Message-Digest algorithm 5

SHA = Secure Hash Algorithm

FAI = Fournisseur d'Accès à Internet

RNIS = réseau numérique à intégration de services

xDSL = x Digital Subscriber Line

LS = Lignes Spécialisées

RLE = run-length encoding

OSI = Open Systems Interconnection

PPTP = Point-to-Point Tunneling Protocol

GRE = General Routing Encapsulation

ISDN = Integrated Services Digital Network

EAP = Extensible Authentication Protocol

CHAP = Challenge Handshake Authentication Protocol

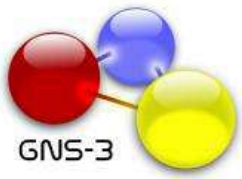
HMAC = Hash-based Message Authentication Code

XAUTH = X Authentication

NAT = Network Address Translation

ANNEXE:

GNS3 est un simulateur d'équipements Cisco. Cet outil permet donc de charger de véritable IOS Cisco et de les utiliser en simulation complète sur un simple ordinateur. Pour caractériser, GNS3 permet d'avoir un routeur Cisco virtuel sur son ordinateur. A noter simplement que GNS3 ne fournit pas d'IOS, il faut se les procurer à l'aide d'un compte Cisco CCO par exemple.



Afin de permettre des simulations complètes, GNS3 est fortement lié avec:

- Dynamips, un émulateur d'image IOS qui permet de lancer des images binaires IOS provenant de Cisco Systems.
- Dynagen, une interface en mode texte pour Dynamips.

GNS3 est un logiciel libre qui fonctionne sur de multiples plateformes, incluant Windows, Linux, et MacOS X.

Il y a 4 plateformes supportées actuellement:

- C2600 (2610, 2611, 2620, 2621, 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691)
- C3600 (3620, 3640, 3660)
- C3700 (3725, 3745)
- C7200

GNS3 n'émule pas encore de switch Catalyst, mais il semblerait qu'avec l'aide de Cisco, rien ne soit impossible.