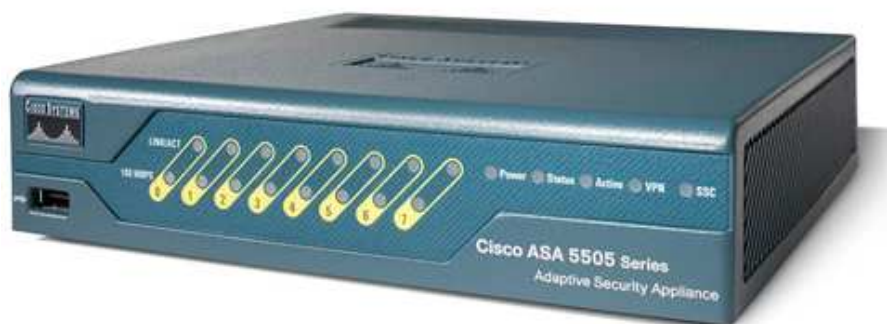


VPN SSL sur ASA

Projet

Réalisation d'un VPN SSL Host to LAN sur un Cisco ASA 5505 (v8.0.4)



Introduction	p 4
I) Différences entre Cisco PIX et Cisco ASA	p 5
a. Présentation de la gamme ASA	p 5
1) Cisco ASA 5505	p 5
2) Cisco ASA 5540	p 7
3) Cisco ASA 5580-40	p 8
b. Présentation de la gamme PIX	p 9
1) Cisco PIX 501	p 9
2) Les modules FWSM	p 10
c. Différences des gammes	p 11
II) Virtual Private Network : VPN	p 12
a. Principe	p 12
b. Types de VPN	p 12
1) VPN Host to Host	p 12
2) VPN Host to LAN	p 13
3) VPN LAN to LAN	p 13
c. Protocoles	p 14
d. Utilisation	p 15
e. Avantages / Inconvénients	p 15
III) Réalisation du projet	p 17
a. ASDM	p 17
b. Connexion au VPN	p 19
c. Problèmes rencontrés	p 23
Conclusion	p 24
Sources	p 24
Illustrations	p 25
Annexes	

Introduction

Dans le cadre du projet nous avons choisis le sujet « VPN SSL avec un Cisco ASA », proposé par M. M'hamed MOSTEFAI. Nous avons choisis ce projet car il nous apparaissait comme une bonne occasion d'approfondir les TP que nous avons pu réaliser lors du module Sécurité des Réseaux, avec M. François AUTIN.

De plus nous avons saisi l'occasion de pouvoir travailler sur un ASA, et donc le nouvel OS de Cisco, ce que nous n'avions pas pu faire en TP, ce qui dans l'optique de notre cursus scolaire et futur professionnel était une excellente occasion pour acquérir ces connaissances.

Le cahier des charges de ce projet était d'une part d'établir une comparaison entre les gammes Cisco PIX et ASA, et dans un second temps l'établissement de la maquette permettant l'accès à une application à distance à travers le VPN.

Nous allons donc voir dans ce dossier, tout d'abord une présentation des gammes PIX et ASA, pour dans un premier temps voir avec quel matériel nous avons travaillé, et établir une base pour pouvoir dans un second temps comparer ces deux familles. Ensuite nous allons étudier le concept de VPN, ses différents types, protocoles, applications... Et pour finir nous allons aborder notre réalisation de la maquette en s'attardant plus particulièrement sur la configuration de l'ASA, ainsi que les modalités d'utilisation.

Remerciements

Avant de commencer, nous aimerions remercier M. M'hamed MOSTEFAI pour nous avoir confié son Cisco ASA afin que nous puissions réaliser ce projet, Mme Béatrice BOUCHOU-MARKHOFF pour nous avoir permis d'utiliser une salle de l'IUT, M. François AUTIN pour la séance de Travaux Pratique su laquelle nous avons pu découvrir les PIX ainsi que son aide pour récupérer des éléments indispensables pour la maquette (Cf. Problèmes rencontrés) ainsi que M. Ludovic FONTAINE pour nous avoir prêté sa salle et pour nous avoir aidé lorsque nous rencontrions quelques difficultés.

Les mots en **rouge** sont définis dans le lexique en annexe

a. Présentation de la gamme ASA

Le matériel Cisco **ASA** de la série 5500 (*Adaptive Security Appliances*) est un système de sécurité s'appuyant sur une plate-forme modulaire. Les ASA peuvent être employés dans différents cadres suivant la gamme que l'on choisit. Les plus petits modèles seront plutôt dédiés à un usage à domicile ou dans les petites entreprises, alors que les gros modèles seront orientés pour les grosses entreprises voir les **Datacenters** nécessitant une sécurité renforcé tout en assurant un service et une rapidité de connexion optimum.

L'OS des ASA est devenu différent de celui des PIX depuis la version 8.x, il utilise depuis un « **kernel** » Linux en lieu et place du PIX OS.

Les différentes familles de Cisco ASA :

La gamme étant assez large, sept références différentes (sans compter les versions Security Plus de certain modèles), nous allons juste voir trois références, bas, milieu et haut de gamme.

1) Cisco ASA 5505

L'ASA 5505 est le plus petit modèle de la gamme. Il y a plus exactement deux modèles, le 5505 *Base* et la version *Security Plus*, qui accepte plus de connexions, de sessions VPN, et liens **VLANs** et point plus intéressant supporte les services de haute disponibilité en **Stateless** Actif/Passif. C'est sur la version de base que nous avons travaillé.

Caractéristiques techniques :

Modèle : 5505



Illustration n°1

Introduit dans la gamme en 2006

Matériel :

- CPU : AMD Geode LX @ 500MHz
- Chipset : Geode CS5536
- Chipset Réseau : Marvell 88E6095
- RAM (par défaut) : 256 Mo
- Périphérique Flash de boot : ATA CompactFlash
- Flash (par défaut) : 64 Mo
- Version minimale de l'OS : 7.2.1
- Interfaces Max : 3 (trunk désactivé) / 20 (trunk activé)
- Supporte les VPN SSL : Oui, 25

Performances :

Bande passante maximale du firewall : 150 Mbps
Connexions maximales : 1 000 / 25 000 (pour la version Security Plus)
Connexions maximales par secondes : 4 000
Paquets par secondes (64 octets) : 85 000
Bande passante maximale VPN 3DES/AES : 100 Mbps
Nombre de sessions VPN maximales (site à site et accès distant) : 10 / 25 (pour la version Security Plus)
Nombre maximale de sessions utilisateur VPN SSL : 25
Nombres de sessions VPN SSL comprises à l'achat : 2

Possibilité d'extensions :

Extension SSC/SSM/IC : 1 SSC
Support SSC/SSM/IC : AIP, SSC
Prévention des intrusions : Oui (avec AIP SSC)
Version de l'ASA OS supportée : 8.2
Haute disponibilité supportée : Non, Actif/Passif (pour la version Security Plus)
VPN **clustering** et équilibrage de charge : Non

Ce modèle est donc intéressant pour les petites structures, aussi bien au vu de ses capacités que de son prix.
De plus un point qui peut être intéressant pour les particulier ou petites sociétés, il n'est pas rackable, donc facile à mettre en œuvre au vu de sa petite taille.

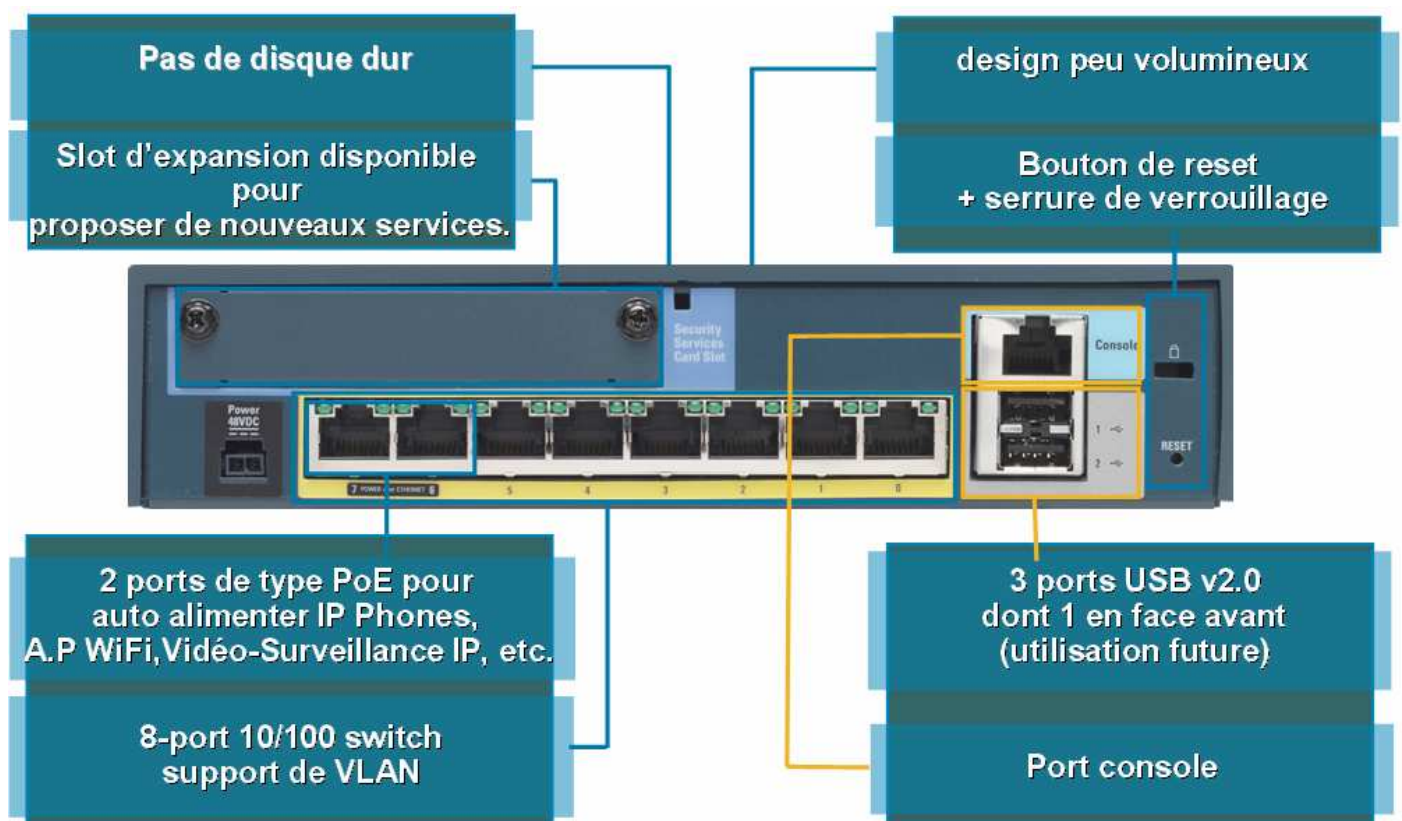


Illustration n°2

2) Cisco ASA 5540

Au vu de ses caractéristique et performances impressionnante cette Appliance est vraiment dédiée aux très grands groupes ayants de très nombreux collaborateurs nomades, ou la base de leur méthode de travail est le télétravail.

Modèle : 5540



Illustration n°3

Introduit dans la gamme en 2005

Matériel :

- CPU : Intel Pentium 4 @ 2,0 GHz
- RAM (par défaut) : 1 Go
- Périphérique Flash de boot : ATA CompactFlash
- Flash (par défaut) : 64 Mo
- Version minimale de l'OS : 7.0.1
- Interfaces Max : 200
- Supporte les VPN SSL : Oui, 2500

Performances :

- Bande passante maximale du firewall : 650 Mbps
- Connexions maximales : 400 000
- Connexions maximales par secondes : 25 000
- Paquets par secondes (64 octets) : 500 000
- Bande passante maximale VPN 3DES/AES : 325 Mbps
- Nombre de sessions VPN maximales (site à site et accès distant) : 5 000
- Nombre maximale de sessions utilisateur VPN SSL : 2 500
- Nombres de sessions VPN SSL comprises à l'achat : 2

Possibilité d'extensions :

- Extension SSC/SSM/IC : 1 SSM
- Support SSC/SSM/IC : CSC SSM, AIP SSM, 4GE SSM
- Prévention des intrusions : Oui (avec AIP SSM)
- Version de l'ASA OS supportée : 8.2
- Haute disponibilité supportée : Actif/Passif, Actif/Actif
- VPN clustering et équilibrage de charge : Oui

3) Cisco ASA 5580-40

Cette référence de la gamme ASA est le plus gros équipement possible. Il est dédié aux Datacenter ou pour les très grands campus, et au vu de ses performances il serait totalement inutile hors de ce rôle.

Modèle : 5580-40



Illustration n°4

Introduit dans la gamme en 2008

Matériel :

- CPU : 4 AMD Opteron (4 x 2 cœurs) @ 2,6 GHz
- RAM (par défaut) : 12 Go
- Périphérique Flash de boot : ATA CompactFlash
- Flash (par défaut) : 1 Go
- Version minimale de l'OS : 8.1.1
- Interfaces Max : 250
- Supporte les VPN SSL : Oui, 10 000

Performances :

- Bande passante maximale du firewall : 10 Gbps (en application http standard par exemple)
20 Gbps (en Jumbo Frames)
- Connexions maximales : 2 000 000
- Connexions maximales par secondes : 150 000
- Paquets par secondes (64 octets) : 4 000 000
- Bande passante maximale VPN 3DES/AES : 1 Gbps
- Nombre de sessions VPN maximales (site à site et accès distant) : 10 000
- Nombre maximale de sessions utilisateur VPN SSL : 10 000
- Nombres de sessions VPN SSL comprises à l'achat : 2

Possibilité d'extensions :

- Extension SSC/SSM/IC : 6 IC
- Support SSC/SSM/IC : 4 10/100/1000, 4 GE SR LC, 2 10GE SR LC
- Prévention des intrusions : NA
- Version de l'ASA OS supportée : 8.2
- Haute disponibilité supportée : Actif/Passif, Actif/Actif
- VPN clustering et équilibrage de charge : Oui (Avec la version Security Plus)

b. Présentation de la gamme PIX

Les Cisco PIX, pour *Private Internet eXchange*, sont des appliances prenant en charge les fonctions de pare-feu et **NAT**. Les PIX ont fait partis des premiers produits de ce segment de marché. Les produit de la gamme PIX ne sont plus vendus depuis juillet 2008, remplacés par les ASA. La technologie demeure en vente mais sous la forme de **blade** (lame), sous le nom de *FireWall Services Module (FWSM)*, et sont destinés aux Switchs *Cisco Catalyst 6500* et aux routeurs de la gamme 7600.

Les ASA sont donc passés à un noyau Linux, les PIX quant à eux continuent à utiliser un système d'exploitation propriétaire appelé *Finesse* (Fast InterNET Server Executive) mais plus couramment appelé PIX OS.

A l'origine le PIX OS n'était pas vraiment aligné avec la syntaxe de l'ISO Cisco, ce qui a été revu à partir de la version 7.0 même si certaines particularités restent il est bien plus abordable pour quiconque connais l'IOS classique.

Comme pour la famille des ASA, les PIX avaient une gamme assez large. La puissance entre PIX et ASA est assez difficilement comparable étant donné que le matériel à en moyenne 4 à 5 ans de plus dans les PIX, et comme tout le monde le sait le matériel évolue à une vitesse impressionnante.

1) Cisco PIX 501 :



Illustration n°5

Il s'agit du modèle le plus proche de l'ASA sur lequel nous avons travaillé, ses caractéristiques sont légèrement plus modestes vu son âge.

Introduit dans la gamme en 2001

Fin de commercialisation en 2008

Hardware :

CPU : AMD SC520 x86 @ 133MHz

RAM (par défaut) : 16 Mo

Périphérique Flash de boot : Sur la carte mère

Flash (par défaut) : 8 Mo

Version minimale de l'OS : 6.1

Interfaces Max : 2

Supporte les VPN SSL : non

Performances :

Bande passante maximale du firewall : 60 Mbps (en application http standard par exemple)

Connexions maximales : 7 500

Bande passante maximale VPN 3DES/AES : 1 Gbps

Nombre maximale de sessions utilisateur VPN SSL : 10

Possibilité d'extensions :

Non

Version de l'ASA OS supportée : 6.3.x

Haute disponibilité supportée : Non



Illustration n°6

Les versions les plus haut de gamme ont pour principales différences la partie matérielle, les 506^e et 515^e passent respectivement à l'Intel Celeron @ 300 MHz et 433MHz, à 32 et 64 Mo de RAM. L'atout majeur du 515 est de supporter la version 8 du PIX OS et de permettre l'ajout de cartes d'extension (5 ports FE, et un 1000baseSX).

Les version 525 et 535 passent quant à elle à l'Intel Pentium III à 600MHz et 1GHz, et généralisent les mêmes ports d'extensions que le 515.

2) Les modules FWSM :



Illustration n°7

Ces modules d'extensions destinés aux routeurs internet 7600 et Switchs de la gamme Catalyst 6500 sont les seuls représentants de la famille PIX encore commercialisés. Les modules d'extensions FWSM n'ont pas à proprement parler d'interfaces physiques, ils se connectent directement à fond de panier et profitent donc de débit important, évitant ainsi des baisses de performances sur le réseau.

Le principe de ces modules est de faire passer les flux de VLANs complets par l'interface virtuel du FWSM et permettre ainsi la sécurisation du réseau grâce à la technologie du PIX.

c. Différences des gammes

A sa sortie le PIX était un excellent firewall, et un des premiers sur le marché, mais le paysage de la sécurité a bien changé depuis. Pour protéger un réseau un PIX n'est aujourd'hui plus suffisant au vu du nombre de type d'attaques possibles comme les virus, vers, ainsi que des applications non désirées (P2P, jeux, messageries instantanées...). Les PIX n'offrent pas de protection « **multi-threat** » ou « **Anti X** ».

D'un point de vue financier il serait extrêmement désavantageux d'avoir une Appliance PIX pour le firewall à filtrage actif, ainsi qu'un ou plusieurs autres Appliances pour effectuer le filtrage concernant les autres types d'attaques. Il est donc bienvenu d'avoir une Appliance « tout en un », aussi appelée UTM pour *Unified Threat Management*.

L'ASA est quant à lui prévu pour effectuer ce rôle, bien qu'il faille ajouter un module CSC SSM, *Content Security and Control Security Service Module* pour ajouter ces fonctions « Anti X ». Sans ce module l'ASA est assez similaire à un PIX.

Pour résumer le Cisco ASA regroupe trois éléments de la gamme Cisco en une seule plate-forme, le *Cisco PIX firewall*, le *Cisco VPN 3000 Series Concentrator*, et le *Cisco IPS 4000 Series Sensor*, alors que le PIX n'était que firewall avec quelques fonctions VPN et sonde IPS assez limitées il est donc important de choisir l'appliance en fonction de ses besoins.

a. Principe

Comme son nom l'indique le VPN est une méthode pour créer un réseau virtuel et privé, c'est-à-dire qu'il est constitué d'un tunnel permettant d'assurer la confidentialité des données transmises.

Comme nous le savons, Internet n'a pas été créé dans un optique de confidentialité, c'est pour cela qu'ont été mis au point ces fameux VPN, ils permettent de créer une liaison entre deux points (deux pairs connectés à l'Internet) tout en rendant cette connexion privée et cryptée donc inaccessible à autrui qui ne serait pas autorisé afin de protéger ces données.

Ils existent plusieurs types de VPN et plusieurs protocoles qui permettent la réalisation de ceux-ci.

b. Types de VPN

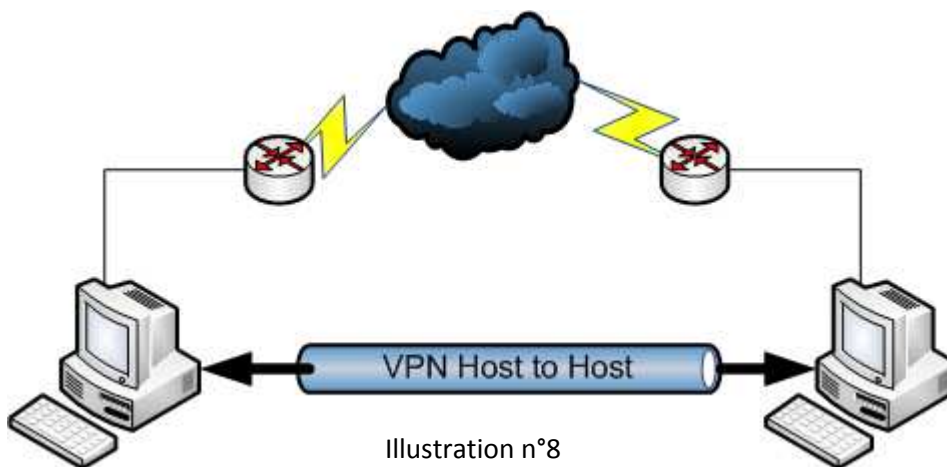
Parmi ces différents types on peut citer les :

- VPN Host to Host
- VPN Host to LAN
- VPN LAN to LAN

Chacun ont leurs particularités, c'est ce que nous allons voir dans cette partie.

1) VPN Host to Host

Les VPN *Host to Host* sont des tunnels entre deux hôtes (souvent deux machines) dont les utilisateurs désirent échanger des fichiers de manière sécurisée et anonyme. Les équipements réseaux ne savent pas ce qui transite à l'intérieur du tunnel, ils « voient » juste des flux cryptés.



2) VPN Host to LAN

Les VPN *Host to LAN* sont des tunnels créés entre un hôte A et un « réseau local » B, l'hôte A se connecte en fait à un matériel dédié à créer le VPN afin qu'il puisse accéder aux ressources du réseau B, c'est ce type de VPN que nous allons mettre en place. Les VPN *Host to LAN* sont souvent mis en place pour du télétravail, ou par exemple un employé en déplacement désirant récupérer une ressource dont il a besoin à travers l'Internet et de manière sécurisée.

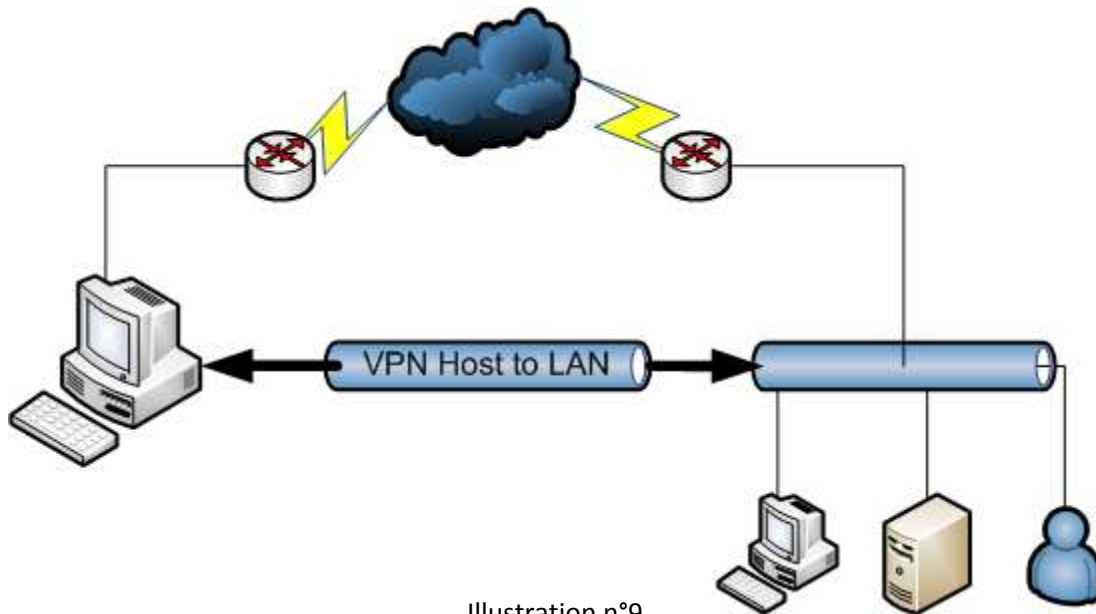


Illustration n°9

3) VPN LAN to LAN

Les VPN *LAN to LAN* sont mis en place entre deux Réseaux Locaux par exemple entre deux routeurs (Cisco PIX ou ASA ou toutes autre marques et modèles supportant les VPN). Ils sont créés afin que les usagers d'un côté puissent atteindre les ressources de l'autre réseau et vice-versa.

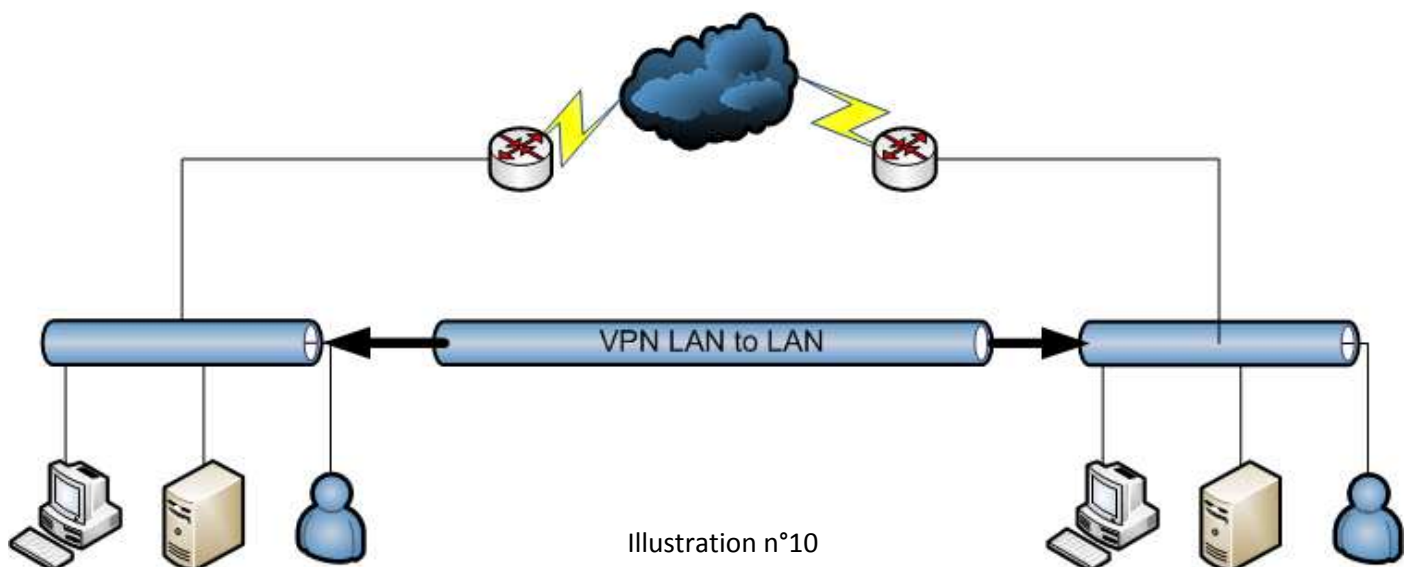


Illustration n°10

c. Protocoles

Il existe plusieurs protocoles permettant la mise en place de VPN, de plus certains se situe plus ou moins haut dans l'architecture OSI.

Par exemple :

- GRE (pour *Generic Routing Encapsulation* ou *Encapsulation Générique de Routage* développé par Cisco) encapsule la couche réseau.
- L2TP (pour *Layer 2 Tunneling Protocol* ou *Protocole de Tunnelisation de Niveau 2* développé par Cisco) encapsule la couche réseau en utilisant L2F et PPTP et est basé sur PPP.
- L2F (pour *Layer Two Forwarding* ou *Transfert de couche 2* développé par Cisco Systems, Northern Telecom (Nortel) et Shiva) est basé sur UDP.
- PPTP (pour *Point-to-Point Tunneling Protocol* ou *Protocole d'encapsulation Point à point* développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics) utilisant GRE.
- IPsec (pour *Internet Protocol Security* définit par l'IETF) basé sur la couche Réseau utilise ISAKMP, IKE, RSA, PSK, etc.
- SSL/TLS (pour Secure Sockets Layer/Transport Layer Security développé par Netscape puis par IETF) nous mettrons ce protocole en place pour le projet.



I E T F

IETF : Internet Engineering Task Force.

"L'Internet Engineering Task Force, abrégée IETF, littéralement traduit de l'anglais en « Détachement d'ingénierie d'Internet » est un groupe informel, international, ouvert à tout individu, qui participe à l'élaboration de standards pour Internet. L'IETF produit la plupart des nouveaux standards d'Internet."

Wikipédia.org

Illustration n°11

d. Utilisation

La plupart des VPN mis en place sont des VPN *Host to LAN* ou des VPN *LAN to LAN*.

Comme nous l'avons déjà vu Internet n'est pas orienté sécurité ni confidentialité il est donc tout à fait possible de pister et de retrouver des traces d'une navigation passée ou en cours. Les VPN sont donc une des solutions afin d'empêcher ou de réduire ces risques.

Il existe de nombreux VPN gratuits (ou payants) proposés sur l'Internet, ce sont des VPN *Host to Host* entre votre ordinateur et un serveur dédié à cette tâche, ils servent la plupart du temps afin de garantir une navigation anonyme.

Ou par exemple une entreprise disposant de plusieurs sites (par exemple un à Tours et un à Blois), elle peut par le biais d'un VPN *LAN to LAN* faire partager des données entre ses deux sites de manière sécurisé, et cette solution est moins coûteuse qu'une liaison spécialisée louée à un prestataire de Télécommunications.

e. Avantages / Inconvénients

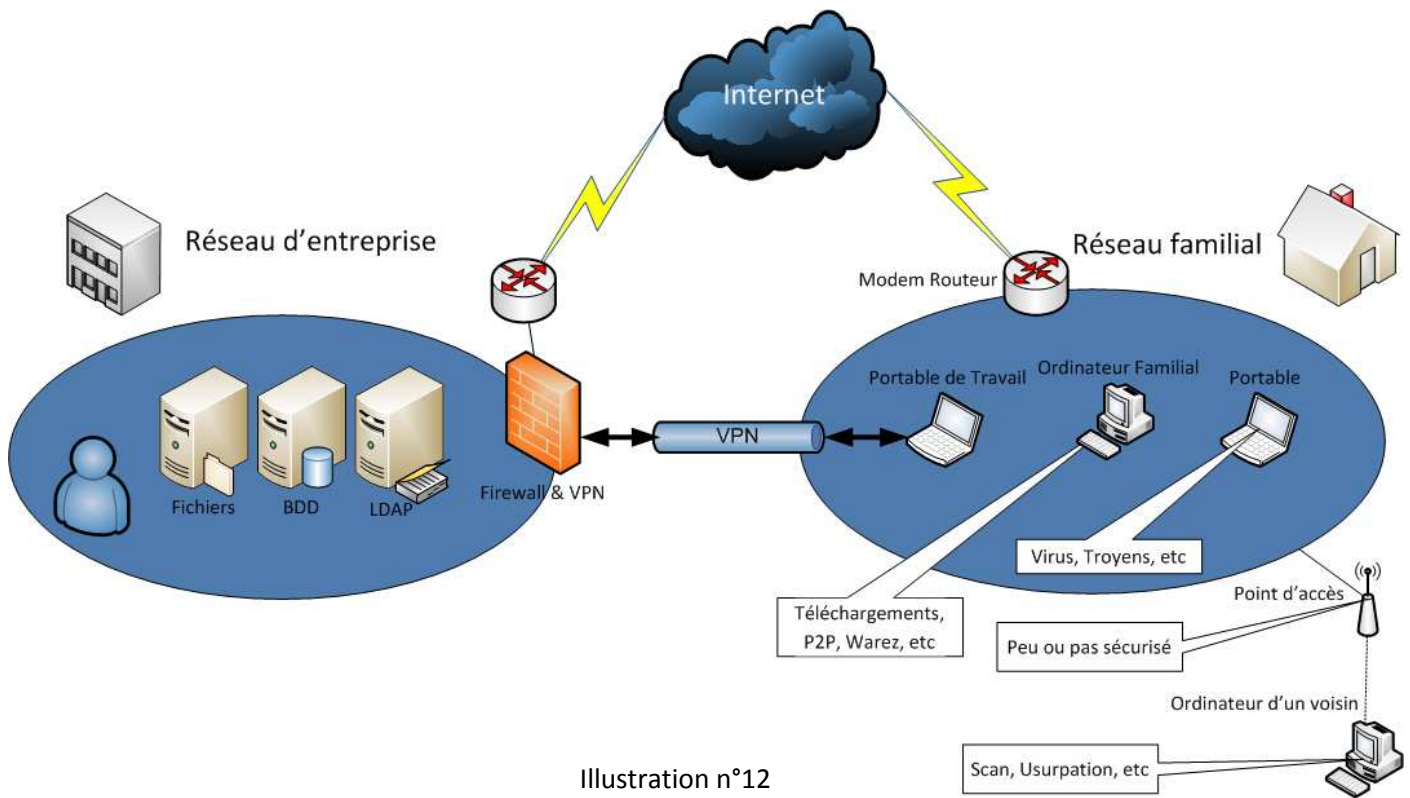
Comme nous venons de le voir les VPN disposent de nombreux avantages :

- Gratuité ou coût assez faible
- Confidentialité
- Sécurité
- Simplicité de mise en place
- Utilisation (quasiment) invisible pour l'utilisateur Lambda

Cependant ils peuvent aussi représenter quelques inconvénients :

- Faille de sécurité (si mal sécurisé)
- Utilisation de ressources matérielles importantes
- Du matériel dédié peut être obligatoire

Par exemple sur le schéma ci-dessous, on peut voir aisément les diverses failles de sécurité que peut représenter du télétravail :



Différentes hypothèses :

Si le réseau du client n'est pas sûr et le VPN mal configuré de nombreuses données non légitimes peuvent transiter vers le réseau d'entreprises tel que des virus, des troyens ou tout autres *malware*.

Si le réseau sans fil n'est pas sécurisé ou mal, il est tout à fait possible à n'importe quelle personne malveillante de récupérer des données ou même usurper l'identité afin de récupérer des informations.

Dans cette partie nous ne n'aborderons, pas à proprement parler, de la configuration de l'ASA car celle-ci a été réalisée en ligne de commande et le fichier est joint en annexe et a été commenté.

a. ASDM

Côté administration, nous avons réalisé la configuration de l'ASA en ligne de commande (plus facile de notre point de vue) il est cependant tout à fait possible de l'effectuer via l'interface graphique nommée ASDM (*Cisco Adaptive Security Device Manager*) disponible soit en l'installant soit par machine Java.

Par l'installation :



Illustration n°13



Illustration n°14

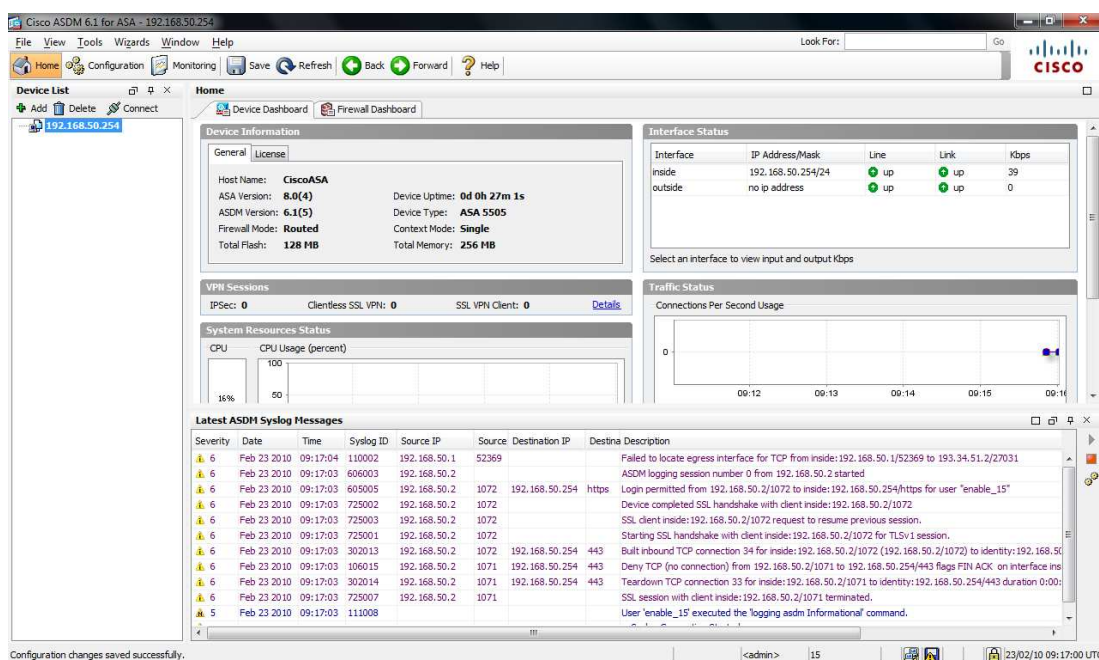


Illustration n°15

Par un navigateur web : A l'adresse <https://192.168.50.254>



Cisco ASDM 6.1(5) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or Java Web Start.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

[Install ASDM Launcher and Run ASDM](#)

Running Cisco ASDM as Java Web Start

You can run Cisco ASDM as Java Web Start that is dynamically downloaded from the device to which you connect.

- Click **Run ASDM** to run Cisco ASDM.
- Click **Run Startup Wizard** to run Startup Wizard. Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

[Run ASDM](#) [Run Startup Wizard](#)

Copyright © 2006-2008 Cisco Systems, Inc. All rights reserved.

Illustration n°16

Sans l'installer il est possible de manager l'ASA par ASDM : *Run ASDM*

Authentification requise

Le serveur 192.168.50.254:443 à l'adresse Authentication requiert un nom d'utilisateur et un mot de passe.

Nom d'utilisateur :

Mot de passe :

[Se connecter](#) [Annuler](#)

Illustration n°17

Ouverture de asdm.jnlp

Vous avez choisi d'ouvrir

asdm.jnlp
qui est un fichier de type : JNLP File
à partir de : https://192.168.50.254

Que doit faire Firefox avec ce fichier ?

☒ Ouvrir avec [Java\(TM\) Web Start Launcher \(défaut\)](#)

☐ Enregistrer le fichier

☐ Toujours effectuer cette action pour ce type de fichier.

[OK](#) [Annuler](#)

Illustration n°18

b. Connexion au VPN

Afin de se connecter au VPN voici les manipulations à effectuer quel que soit le système d'exploitation (Windows, MacOS ou Linux) :

Avec un navigateur (quel qu'il soit), aller à l'adresse <https://78.X.X.X>

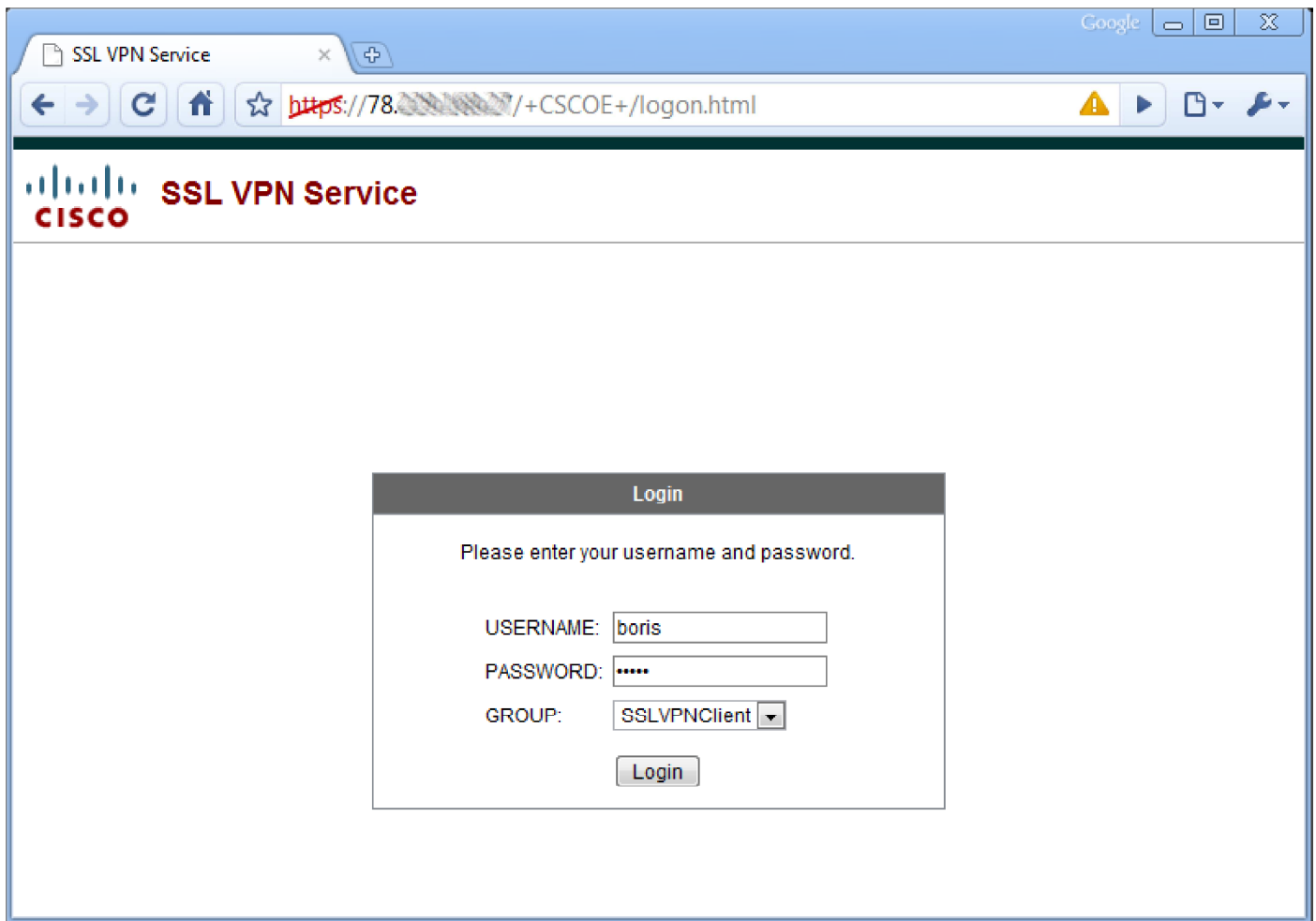


Illustration n°19

Entrer vos login et mot de passe

Soit : boris / boris

Soit : gael / gael

L'installation du client Cisco Any Connect devrait se lancer automatiquement après les messages d'avertissement de sécurité.



Illustration n°20

Le certificat de l'ASA étant auto-signé des messages apparaissent :

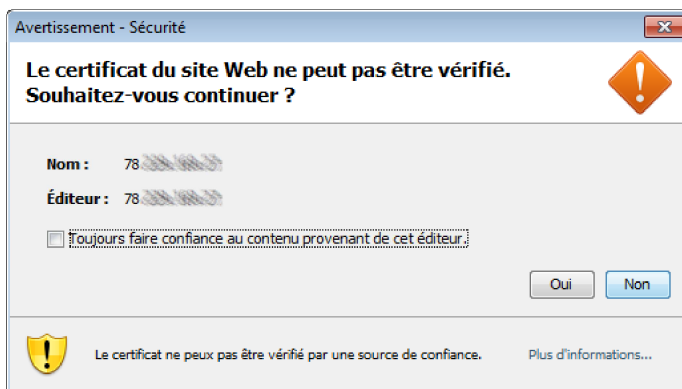


Illustration n°21

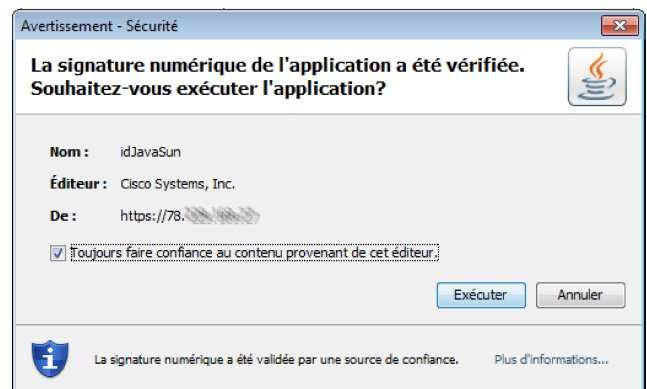


Illustration n°22

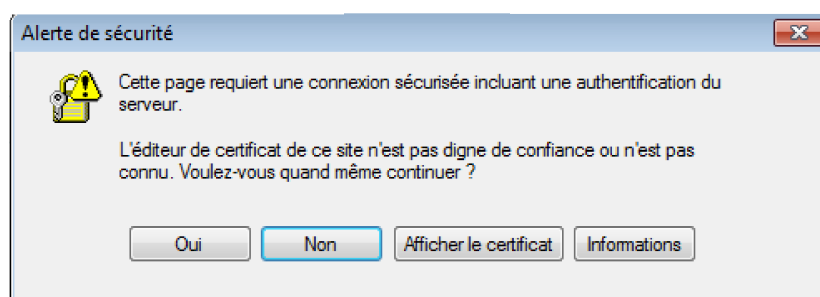


Illustration n°23

L'installation se lance de manière automatique



Illustration n°24

! Attention !

Si vous êtes sous Windows Vista il y a une petite manipulation à effectuer.
(Désactivation du service Bonjour ou celui appelé "##Id_String...")

Une fois connecté il est possible de voir le statut de la connexion VPN ainsi que les caractéristiques de cette dernière.

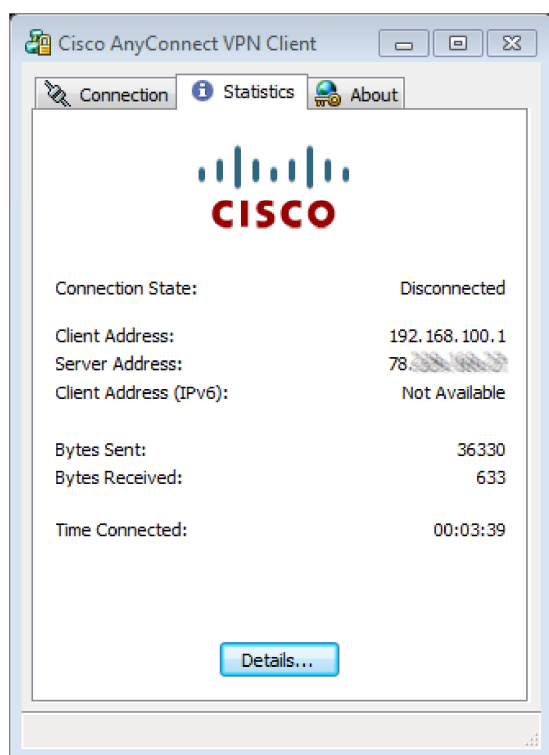


Illustration n°25

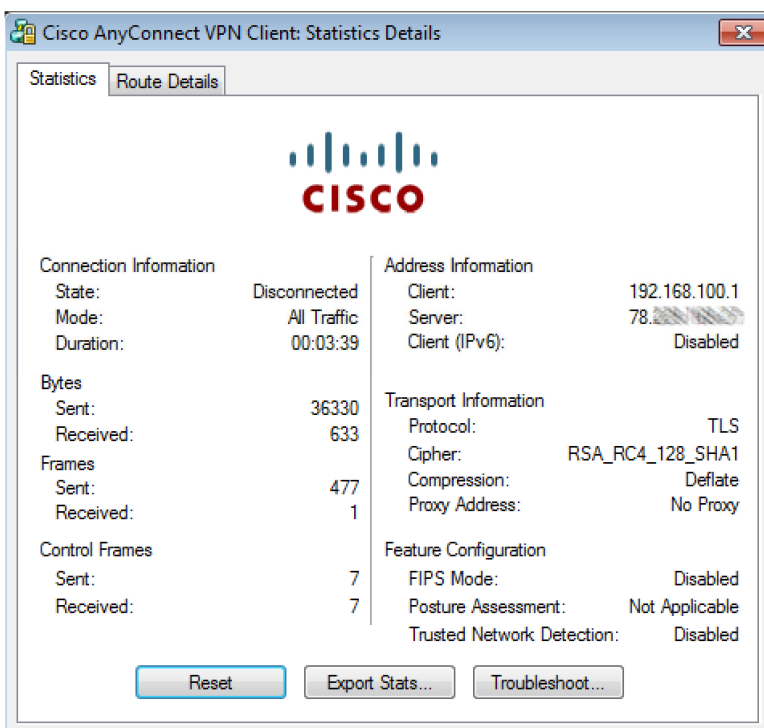


Illustration n°26

Exemple de connexion à partir d'un Mac :

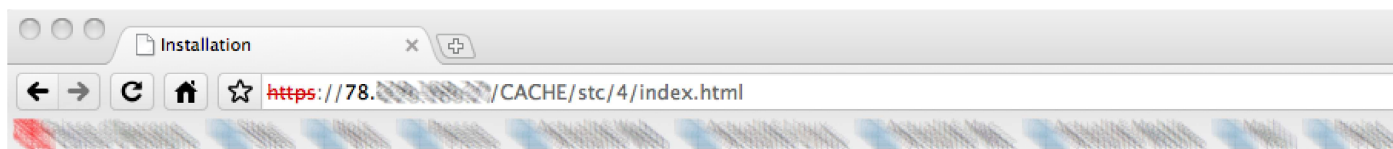


Illustration n°27



Illustration n°28

Ce message apparaît si MacOS X a été mis à jour à la dernière version (AnyConnect Mac n'étant pas à jour Cf Problèmes rencontrés)

Une fois connecté vous pouvez accéder au réseau local (192.168.50.0/24) par exemple le serveur XAMPP de test :

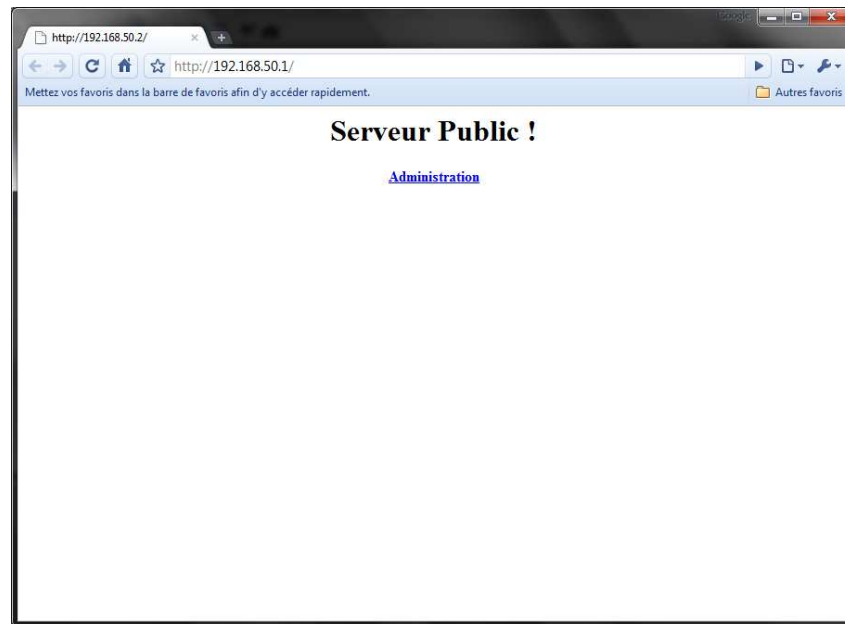


Illustration n°29

c. Problèmes rencontrés

- Compte CCNA Technicien : Nous ne disposions pas de compte ayant des droits suffisant sur le site Cisco pour pouvoir télécharger les clients AnyConnect, ou ASDM. Nous avons donc dû demander à M. MOSTEFAI et M. AUTIN de nous les fournir.
- Licence VPN : 2 sessions maximum : La licence de base vendue avec les ASA ne compte que deux sessions VPN SSL au maximum. Ce problème est apparu en même temps que les sessions fantôme que nous développons ensuite.
- Sessions fantôme : Il nous est apparu un souci de session dite fantôme. Lorsque la session VPN n'était pas quittée correctement, la session de l'utilisateur restait ouverte pour l'ASA, ce qui au vu de la limitation de licence nous a bloqué rapidement. La solution consiste simplement à forcer la fermeture des sessions grâce à l'ASDM.
- Accès à une IP Publique : Pour pouvoir tester la maquette il nous fallait une connexion Internet et avoir accès à l'IP publique, nous avons donc du finir le projet chez nous, avec notre propre accès ADSL.
- Client MacOS : Lors des tests nous avons eu des erreurs pour l'accès au VPN à partir de MacOS, la version du client que nous avons n'étant pas à jour.
- Salle de projet : Il a été difficile de travailler efficacement car d'un point de vu logistique il n'y a pas de salle prévue pour les projets. Nous devons donc à chaque fois démonter la maquette, et ce parfois plusieurs fois par jour si il y avait cours dans la salle.

Conclusion

Le regard que nous portons sur ce projet une fois terminé est à notre avis extrêmement positif. Dans le cadre de notre formation ce projet nous a permis d'approfondir un domaine qui nous avait intéressés au cours de l'année, et qui s'avèrera très probablement utile au quotidien dans la suite de notre parcours.

Malgré quelques problèmes inhérents à tout projet nous avons la satisfaction d'avoir rempli le cahier des charges qui nous a été fournis. Nous aurions aimé avoir plus de temps pour explorer plus en avant les possibilités offertes par le matériel, notamment le partage d'application à partir d'une interface web.

Pour conclure nous restons sur une très bonne impression et sommes pleinement satisfait d'avoir fait ce projet tout à fait dans l'esprit de la licence professionnelle QSSI.

Sources

Ci-dessous vous trouverez les différentes sources qui nous ont permis de réaliser ce projet ainsi que le dossier l'accompagnant.

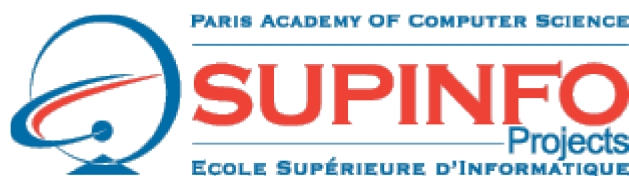


Cisco.com



WIKIPEDIA
L'encyclopédie libre

Wikipedia.org



Supinfo-projects.com



Cisco.netacad.net

Illustration n°1 : Cisco ASA 5505 - Source : Cisco.com
Illustration n°2 : Schéma Cisco ASA 5505 - Source : Cisco.com
Illustration n°3 : Cisco ASA 5540 - Source : Cisco.com
Illustration n°4 : Cisco ASA 5580-40 - Source : Cisco.com
Illustration n°5 : Cisco PIX 501 - Source : Cisco.com
Illustration n°6 : Cisco PIX 515 - Source : Cisco.com
Illustration n°7 : Exemple de module FWSM - Source : Cisco.com
Illustration n°8 : VPN Host to Host - Source : Boris PASCAULT
Illustration n°9 : VPN Host to LAN - Source : Boris PASCAULT
Illustration n°10 : VPN LAN to LAN - Source : Boris PASCAULT
Illustration n°11 : Logo de l'IETF - Source : ietf.org
Illustration n°12 : Dangers des VPN - Source : Boris PASCAULT
Illustration n°13 : Connexion au ASDM
Illustration n°14 : Certificat ASA
Illustration n°15 : Accueil ASDM
Illustration n°16 : Accueil Web ASDM
Illustration n°17 : Authentification ASDM
Illustration n°18 : asdm.jnlp (Machine Java)
Illustration n°19 : Connexion au VPN par l'IP public
Illustration n°20 : Informations à propos de Java
Illustration n°21 : Certificat ASA
Illustration n°22 : Signature du certificat
Illustration n°23 : Alerte de sécurité
Illustration n°24 : Installation de Cisco AnyConnect
Illustration n°25 : Etat de la connexion
Illustration n°26 : Détails de la connexion
Illustration n°27 : Installation de AnyConnect sur MacOS
Illustration n°28 : Erreur version Mac
Illustration n°29 : Serveur Web de test

ANNEXES

- I) Lexique
- II) Fichier de configuration
- III) Schéma global
- IV) Fiche Cisco
- V) Diagrammes de Gantt
 - a. Gantt – Diagramme de Janvier
 - b. Gantt – Diagramme de Février
 - c. Gantt – Diagramme Final

Anti X	Anti-Malware, Anti-Virus, Anti-Spyware, etc.
ASA	Adaptive Security Appliance Gamme de pare-feu de Cisco Systems
Blade	Lame Dans le cadre des Appliances Cisco il s'agit de modules d'extension ayant une apparence similaire aux serveurs lames appelés blades.
Datacenters	Centre de données Lieu protégé regroupant de grandes quantités de données et de serveurs souvent loués (Hébergeurs Web, ...)
Firewall	Pare-feu Logiciel ou Matériel séparant plusieurs réseaux et régissant leurs accès respectifs
GRE	Generic Routing Encapsulation Protocole d'encapsulation IPv4
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange Informations de sécurité partagées pour IPsec
IPsec	Internet Protocol SECurity Protocole d'encapsulation (IPv6 et retro compatible IPv4)
ISAKMP	Internet Security Associations and Key Management Permet l'établissement d'un canal permettant l'échange des clés du cryptage pour les VPN IpSec
Kernel	Noyau Cœur d'un système d'exploitation permettant aux matériels de communiquer et gérant les ressources
L2F	Layer Two Forwarding Protocole d'encapsulation basé sur UDP
L2TP	Layer 2 Tunneling Protocole Protocole d'encapsulation
LAN	Local Area Network Réseau Local
Malware	Logiciel développé dans le but de nuire à un système informatique
Multi-threat	Menaces multiples
NAT/PAT	Network Address Translation « Mécanisme informatique permettant de faire communiquer un réseau local avec l'Internet. » [Wikipédia] Port Address Translation Translation de port contrairement au NAT avec l'adresse
OS	Operating System Système d'Exploitation
PIX	Private Internet eXchange Gamme de are-feu de Cisco Systems
PPTP	Point-to-Point Tunneling Protocol Protocole d'encapsulation basé sur IP

PSK	Phase-Shift Keying Modulation par déplacement de phase
RSA	Rivest Shamir Adleman Algorithme cryptographique
SSL / TLS	Secure Socket Layer / Transport Layer Security Protocole de sécurisation d'échange sur Internet
Statefull (FireWall)	En opposition aux Firewalls Stateless
Stateless (FireWall)	Pare-feu ne prenant pas en compte l'état de la connexion lors du filtrage.
Troyens	Cheval de Troie Logiciel développé dans le but d'exécuter de manière invisible des actions à l'insu de l'utilisateur
VLAN	Virtual Local Area Network Permet de créer un réseau informatique logique indépendant. [Wikipedia]
VPN	Virtual Private Network Réseau Privé Virtuel

```
en

conf t
hostname CiscoASA
enable password jacky
exit

exit
en
jacky

configure terminal

! Parametrage des VLANS
interface vlan 1
shutdown
exit

interface vlan 2
nameif outside
description Vlan Ouside
security-level 0
ip address dhcp setroute
!ip address 78.229.169.27 255.255.255.0
no shutdown
exit

interface vlan 3
nameif inside
description Vlan Inside
security-level 100
ip address 192.168.50.254 255.255.255.0
no shutdown
exit

! Parametrage des interfaces
interface Ethernet 0/0
switchport mode access
switchport access vlan 2
no shutdown
exit

interface Ethernet 0/1
switchport mode access
switchport access vlan 3
no shutdown
exit

interface Ethernet 0/2
switchport mode access
switchport access vlan 3
no shutdown
exit

interface Ethernet 0/3
switchport mode access
switchport access vlan 3
no shutdown
exit
```

```

interface Ethernet 0/4
switchport mode access
switchport access vlan 3
no shutdown
exit

interface Ethernet 0/5
switchport mode access
switchport access vlan 3
no shutdown
exit

interface Ethernet 0/6
switchport mode access
switchport access vlan 3
no shutdown
exit

interface Ethernet 0/7
switchport mode access
switchport access vlan 3
no shutdown
exit

! Parametrage du serveur DHCP : Pool et DNS
dhcpd dns 8.8.8.8
dhcpd address 192.168.50.1-192.168.50.100 inside
dhcpd enable inside

! Parametrage du NAT
global (outside) 1 interface
nat (inside) 1 0 0

! Activation du serveur HTTP
http server enable
http 192.168.50.0 255.255.255.0 inside

! Mise en place des ACL
access-list acl-icmp extended permit icmp any any
access-group acl-icmp in interface inside

access-list acl-out extended permit ip 192.168.50.0 255.255.255.0 any
access-list acl-out extended permit ip 192.168.100.0 255.255.255.0 any
access-list acl-vpn extended permit ip 192.168.100.0 255.255.255.0 any

access-group acl-out in interface inside
access-group acl-vpn in interface outside

! Generation des certificats
crypto key generate rsa label sslvpnkeypair
crypto ca trustpoint localtrust
enrollment self
fqdn sslvpn.cisco.com
subject-name CN=sslvpn.cisco.com
keypair sslvpnkeypair
crypto ca enroll localtrust noconfirm
ssl trust-point localtrust outside

```

```

! Configuration du VPN SSL
! Sur les clients Vista ARRETER services Bonjour (dans services.msc =>
"##Id_String...")
webvpn
svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1 regex Windows_NT
svc image disk0:/anyconnect-dart-win-2.4.1012-k9.pkg 2 regex Windows_DART
svc image disk0:/anyconnect-macosx-powerpc-2.4.0202-k9.pkg 3 regex Mac_Power_Pc
svc image disk0:/anyconnect-macosx-i386-2.4.0202-k9.pkg 4 regex Mac_i386
svc image disk0:/anyconnect-linux-2.4.1012-k9.pkg 5 regex Linux
svc image disk0:/anyconnect-wince-ARMv4I-2.4.0202-k9.pkg 6 regex Wince_ARM

enable outside
svc enable
ip local pool SSLClientPool 192.168.100.1-192.168.100.10 mask 255.255.255.0
group-policy SSLClientPolicy internal
group-policy SSLClientPolicy attributes
dns-server value 8.8.8.8
vpn-tunnel-protocol svc
default-domain value vpn.projet.local
address-pools value SSLClientPool
sysopt connection permit-vpn
tunnel-group SSLClientProfile type remote-access
tunnel-group SSLClientProfile general-attributes
default-group-policy SSLClientPolicy
tunnel-group SSLClientProfile webvpn-attributes
group-alias SSLVPNClient enable
webvpn
tunnel-group-list enable
access-list no_nat extended permit ip 192.168.50.0 255.255.255.0 192.168.100.0
255.255.255.0
nat (inside) 0 access-list no_nat
username boris password boris
username boris attributes
service-type remote-access
username gael password gael
username gael attributes
service-type remote-access
exit

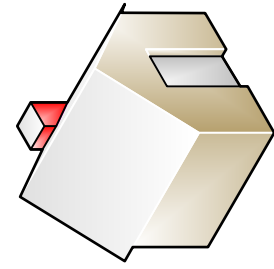
! Sauvegarde dans la memoire flash
write memory

```

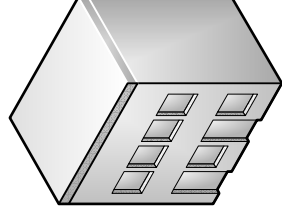
VPN SSL

Host to LAN

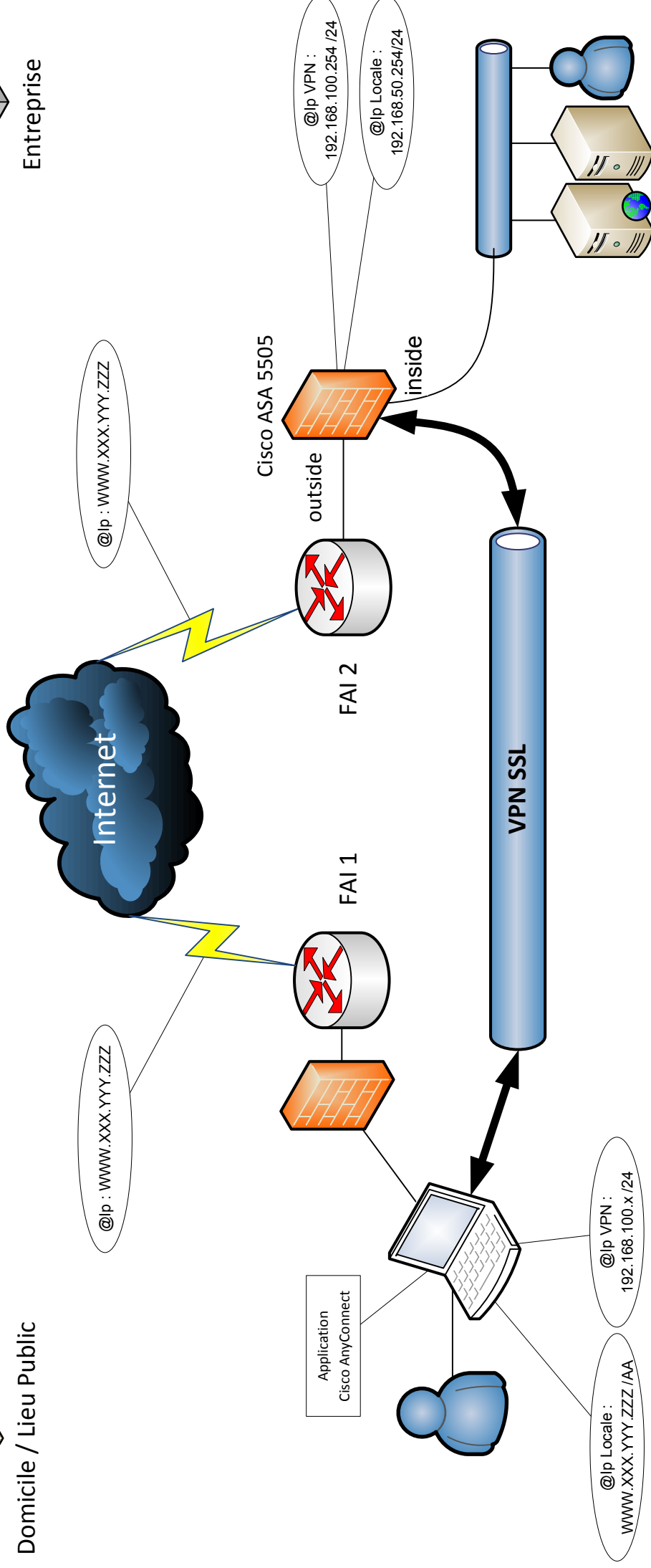
Cisco ASA 5505 (8.0.4)



Domicile / Lieu Public



Entreprise



ASA 8.x: VPN Access with the AnyConnect VPN Client Using Self-Signed Certificate Configuration Example

Document ID: 99756

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configure

- Step 1. Configure a Self-Issued Certificate
- Step 2. Upload and Identify the SSL VPN Client Image
- Step 3. Enable Anyconnect Access
- Step 4. Create a new Group Policy
- Configure Access List Bypass for VPN Connections
- Step 6. Create a Connection Profile and Tunnel Group for the AnyConnect Client

Connections

- Step 7. Configure NAT Exemption for AnyConnect Clients
- Step 8. Add Users to the Local Database

Verify

Troubleshoot

- Troubleshooting Commands (Optional)

Related Information

Introduction

This document describes how to use self-signed certificates to allow remote access SSL VPN connections to the ASA from the Cisco AnyConnect 2.0 client.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic ASA configuration that runs software version 8.0
- ASDM 6.0(2)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 8.0(2), ASDM 6.0 (2)
- Cisco AnyConnect 2.0

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

The Cisco AnyConnect 2.0 client is an SSL-based VPN client. The AnyConnect client can be utilized and installed on a variety of operating systems, such as Windows 2000, XP, Vista, Linux (Multiple Distros) and MAC OS X. The AnyConnect client can be installed manually on the remote PC by the system administrator. It can also be loaded onto the security appliance and made ready for download to remote users. After the application is downloaded, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections. This example makes the AnyConnect client ready to download upon successful browser-based SSL authentication.

For more information on the AnyConnect 2.0 client, refer to AnyConnect 2.0 Release Notes.

Note: MS Terminal Services is not supported in conjunction with the AnyConnect client. You cannot RDP to a computer and then initiate an AnyConnect session. You cannot RDP to a client that is connected via AnyConnect.

Note: The first installation of AnyConnect requires the user to have admin rights (whether you use the standalone AnyConnect msi package or push the pkg file from the ASA). If the user does not have admin rights, a dialog box appears that states this requirement. Subsequent upgrades will not require the user that installed AnyConnect previously to have admin rights.

Configure

In order to configure the ASA for VPN access using the AnyConnect client, complete these steps:

1. Configure a Self-Issued Certificate.
2. Upload and Identify the SSL VPN Client Image.
3. Enable Anyconnect Access.
4. Create a new Group Policy.
5. Configure Access List Bypass for VPN Connections.
6. Create a Connection Profile and Tunnel Group for the AnyConnect Client Connections.
7. Configure NAT Exemption for AnyConnect Clients.
8. Add Users to the Local Database.

Step 1. Configure a Self-Issued Certificate

By default, the security appliance has a self-signed certificate that is regenerated every time the device is rebooted. You can purchase your own certificate from vendors, such as Verisign or EnTrust, or you can configure the ASA to issue an identity certificate to itself. This certificate remains the same even when the device is rebooted. Complete this step in order to generate a self-issued certificate that persists when the device is rebooted.

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **Certificate Management**, and then choose **Identity Certificates**.
3. Click **Add**, and then click the **Add a new identity certificate** radio button.
4. Click **New**.

5. In the Add Key Pair dialog box, click the **Enter new key pair name** radio button.
6. Enter a name to identify the keypair.

This example uses *sslvpnkeypair*.

7. Click **Generate Now**.
8. In the Add Identity Certificate dialog box, ensure the newly created key pair is selected.
9. For Certificate Subject DN, enter the fully qualified domain name (FQDN) that will be used to connect to the VPN terminating interface.

CN=sslvpn.cisco.com

10. Click **Advanced**, and enter the FQDN used for the Certificate Subject DN field.

For example, **FQDN**: sslvpn.cisco.com

11. Click **OK**.
12. Check the **Generate Self Signed Certificate** check box, and click **Add Certificate**.
13. Click **OK**.
14. Click **Configuration**, and then click **Remote Access VPN**.
15. Expand **Advanced**, and choose **SSL Settings**.
16. In the Certificates area, choose the interface that will be used to terminate the SSL VPN (outside), and click **Edit**.
17. In the Certificate drop-down list, choose the self-signed certificate that you generated earlier.
18. Click **OK**, and then click **Apply**.

Command Line Example

ciscoasa
<pre>ciscoasa(config)#crypto key generate rsa label sslvpnkeypair INFO: The name for the keys will be: sslvpnkeypair Keypair generation process begin. Please wait... !--- Generate an RSA key for the certificate. (The name should be unique. !--- For example, sslvpnkeypair.) ciscoasa(config)#crypto ca trustpoint localtrust !--- Create a trustpoint for the self-issued certificate. ciscoasa(config-ca-trustpoint)#enrollment self ciscoasa(config-ca-trustpoint)#fqdn sslvpn.cisco.com ciscoasa(config-ca-trustpoint)#subject-name CN=sslvpn.cisco.com !--- The fully qualified domain name is used for both fqdn and CN. !--- The name should resolve to the ASA outside interface IP address. ciscoasa(config-ca-trustpoint)#keypair sslvpnkeypair !--- The RSA key is assigned to the trustpoint for certificate creation. ciscoasa(config-ca-trustpoint)#crypto ca enroll localtrust noconfirm % The fully-qualified domain name in the certificate will be: sslvpn.cisco.com ciscoasa(config)# ssl trust-point localtrust outside !--- Assign the trustpoint to be used for SSL connections on the outside interface.</pre>

Step 2. Upload and Identify the SSL VPN Client Image

This document uses the AnyConnect SSL 2.0 client. You can obtain this client at the Cisco Software Download Website. A separate Anyconnect image is required for each operating system that remote users plan to use. For more information, refer to Cisco AnyConnect 2.0 Release Notes.

Once you obtain the AnyConnect client, complete these steps:

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **Network (Client) Access**, and then expand **Advanced**.
3. Expand **SSL VPN**, and choose **Client Settings**.
4. In the SSL VPN Client Images area, click **Add**, and then click **Upload**.
5. Browse to the location where you downloaded the AnyConnect client.
6. Select the file, and click **Upload File**.

Once the client uploads, you receive a message that states the file was uploaded to flash successfully.

7. Click **OK**.

A dialog box appears to confirm that you want to use the newly uploaded image as the current SSL VPN client image.

8. Click **OK**.
9. Click **OK**, and then click **Apply**.
10. Repeat the steps in this section for each operating system-specific Anyconnect package that you want to use.

Command Line Example

```
ciscoasa
ciscoasa(config)#copy tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg flash
Address or name of remote host [192.168.50.5]?
Source filename [anyconnect-win-2.0.0343-k9.pkg]?
Destination filename [anyconnect-win-2.0.0343-k9.pkg]?

Accessing tftp://192.168.50.5/anyconnect-win-2.0.0343-k9.pkg...!!!!!!!!!!!!!!
Writing file disk0:/anyconnect-win-2.0.0343-k9.pkg...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
2635734 bytes copied in 4.480 secs (658933 bytes/sec)

!--- AnyConnect image is downloaded to ASA via TFTP.

ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1

!--- Specify the AnyConnect image to be downloaded by users. The image that is
!--- downloaded the most should have the lowest number. This image uses 1 for the
!--- AnyConnect Windows image.
```

Step 3. Enable Anyconnect Access

In order to allow the AnyConnect client to connect to the ASA, you must enable access on the interface that terminates SSL VPN connections. This example uses the outside interface in order to terminate Anyconnect

connections.

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **Network (Client) Access**, and then choose **SSL VPN Connection Profiles**.
3. Check the **Enable Cisco AnyConnect VPN Client** check box.
4. Check the **Allow Access** check box for the outside interface, and click **Apply**.

Command Line Example

ciscoasa
<pre>ciscoasa(config)#webvpn ciscoasa(config-webvpn)#enable outside ciscoasa(config-webvpn)#svc enable !--- Enable AnyConnect to be downloaded to remote computers.</pre>

Step 4. Create a new Group Policy

A group policy specifies the configuration parameters that should be applied to clients when they connect. This example creates a group policy named *SSLClientPolicy*.

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **Network (Client) Access**, and choose **Group Policies**.
3. Click **Add**.
4. Choose **General**, and enter **SSLClientPolicy** in the Name field.
5. Uncheck the Address Pools **Inherit** check box.
6. Click **Select**, and then click **Add**.

The Add IP Pool dialog box appears.

7. Configure the address pool from an IP range that is not currently in use on your network.

This example uses these values:

- ◆ **Name:** SSLClientPool
- ◆ **Starting IP Address:** 192.168.25.1
- ◆ **Ending IP Address:** 192.168.25.50
- ◆ **Subnet Mask:** 255.255.255.0

8. Click **OK**.
9. Choose the newly created pool, and click **Assign**.
10. Click **OK**, and then click **More Options**.
11. Uncheck the Tunneling Protocols **Inherit** check box.
12. Check **SSL VPN Client**.
13. In the left pane, choose **Servers**.
14. Uncheck the DNS Servers **Inherit** check box, and enter the IP address of the internal DNS server that the AnyConnect clients will use.

This example uses *192.168.50.5*.

15. Click **More Options**.
16. Uncheck the Default Domain **Inherit** check box.

17. Enter the domain used by your internal network. For example, *tsweb.local*.
18. Click **OK**, and then click **Apply**.

Command Line Example

ciscoasa
<pre> ciscoasa(config)#ip local pool SSLClientPool 192.168.25.1-192.168.25.50 mask 255.255.255.0 !--- Define the IP pool. The IP pool should be a range of IP addresses !--- not already in use on the internal network. ciscoasa(config)#group-policy SSLClientPolicy internal ciscoasa(config)#group-policy SSLClientPolicy attributes ciscoasa(config-group-policy)#dns-server value 192.168.50.5 !--- Specify the internal DNS server to be used. ciscoasa(config-group-policy)#vpn-tunnel-protocol svc !--- Specify VPN tunnel protocol to be used by the Group Policy. ciscoasa(config-group-policy)#default-domain value tsweb.local !--- Define the default domain assigned to VPN users. ciscoasa(config-group-policy)#address-pools value SSLClientPool !--- Assign the IP pool created to the SSLClientPolicy group policy. </pre>

Configure Access List Bypass for VPN Connections

When you enable this option, you allow the SSL/IPsec clients to bypass the interface access list.

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **Network (Client) Access**, and then expand **Advanced**.
3. Expand **SSL VPN**, and choose **Bypass Interface Access List**.
4. Ensure the **Enable inbound SSL VPN and IPSEC Sessions to bypass interface access lists** check box is checked, and click **Apply**.

Command Line Example

ciscoasa
<pre> ciscoasa(config)#sysopt connection permit-vpn !--- Enable interface access-list bypass for VPN connections. !--- This example uses the vpn-filter command for access control. ciscoasa(config-group-policy)# </pre>

Step 6. Create a Connection Profile and Tunnel Group for the AnyConnect Client Connections

When VPN clients connect to the ASA, they connect to a connection profile or tunnel group. The tunnel group is used to define connection parameters for specific types of VPN connections, such as IPsec L2L, IPsec

remote access, clientless SSL, and client SSL.

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **Network (Client) Access**, and then expand **SSL VPN**.
3. Choose **Connection Profiles**, and click **Add**.
4. Choose **Basic**, and enter these values:
 - ◆ **Name:** SSLClientProfile
 - ◆ **Authentication:** LOCAL
 - ◆ **Default Group Policy:** SSLClientPolicy
5. Ensure the **SSL VPN Client Protocol** check box is checked.
6. In the left pane, expand **Advanced**, and choose **SSL VPN**.
7. Under Connection Aliases, click **Add**, and enter a name to which users can associate their VPN connections. For example, *SSLVPNClient*.
8. Click **OK**, and then click **OK** again.
9. At the bottom of the ASDM window, check the **Allow user to select connection, identified by alias in the table above at login page** check box, and click **Apply**.

Command Line Example

```

ciscoasa
ciscoasa(config)#tunnel-group SSLClientProfile type remote-access

!--- Define tunnel group to be used for VPN remote access connections.

ciscoasa(config)#tunnel-group SSLClientProfile general-attributes
ciscoasa(config-tunnel-general)#default-group-policy SSLClientPolicy
ciscoasa(config-tunnel-general)#tunnel-group SSLClientProfile webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias SSLVPNClient enable

!--- Assign alias for tunnel group.

ciscoasa(config-tunnel-webvpn)#webvpn
ciscoasa(config-webvpn)#tunnel-group-list enable

!--- Enable alias/tunnel group selection for SSL VPN connections.
```

Step 7. Configure NAT Exemption for AnyConnect Clients

NAT exemption should be configured for any IP addresses or ranges you want to allow the SSL VPN clients to access. In this example, the SSL VPN clients need access to the internal IP 192.168.50.5 only.

Note: If NAT-control is not enabled, this step is not required. Use the **show run nat-control** command to verify. In order to verify through ASDM, click **Configuration**, click **Firewall**, and choose **Nat Rules**. If the **Enable traffic through the firewall without address translation** check box is checked, you can skip this step.

ASDM Procedure

1. Click **Configuration**, and then click **Firewall**.
2. Choose **Nat Rules**, and click **Add**.
3. Choose **Add NAT Exempt Rule**, and enter these values:

- ◆ **Action:** Exempt
 - ◆ **Interface:** inside
 - ◆ **Source:** 192.168.50.5
 - ◆ **Destination:** 192.168.25.0/24
 - ◆ **NAT Exempt Direction:** NAT Exempt outbound traffic from interface 'inside' to lower security interfaces (Default)
4. Click **OK**, and then click **Apply**.

Command Line Example

```

ciscoasa
ciscoasa(config)#access-list no_nat extended permit
                    ip host 192.168.50.5 192.168.25.0 255.255.255.0

!--- Define access list to be used for NAT exemption.

ciscoasa(config)#nat (inside) 0 access-list no_nat

!--- Allow external connections to untranslated internal
!--- addresses defined by access list no_nat.

ciscoasa(config)#

```

Step 8. Add Users to the Local Database

If you use local authentication (the default), you must define user names and passwords in the local database for user authentication.

ASDM Procedure

1. Click **Configuration**, and then click **Remote Access VPN**.
2. Expand **AAA Setup**, and choose **Local Users**.
3. Click **Add**, and enter these values:
 - ◆ **Username:** matthewp
 - ◆ **Password:** p@ssw0rd
 - ◆ **Confirm Password:** p@ssw0rd
4. Select the **No ASDM, SSH, Telnet or Console Access** radio button.
5. Click **OK**, and then click **Apply**.
6. Repeat this step for additional users, and then click **Save**.

Command Line Example

```

ciscoasa
ciscoasa(config)#username matthewp password p@ssw0rd
ciscoasa(config)#username matthewp attributes
ciscoasa(config-username)#service-type remote-access

!--- Assign user remote access only. No SSH, Telnet, ASDM access allowed.

ciscoasa(config-username)#write memory

!--- Save the configuration.

```


Verify

Use this section in order to verify that the SSL VPN configuration is successful

Connect to the ASA with the AnyConnect Client

Install the client directly on a PC, and connect to the ASA outside interface, or enter https and the FQDN/IP address of the ASA in a web browser. If you use a web browser, the client installs itself upon successful login.

Verify SSL VPN Client Connections

Use the **show vpn-sessiondb svc** command in order to verify connected SSL VPN clients.

```
ciscoasa(config-group-policy)#show vpn-sessiondb svc

Session Type: SVC

Username      : matthewp                      Index      : 6
Assigned IP   : 192.168.25.1                 Public IP   : 172.18.12.111
Protocol      : Clientless SSL-Tunnel        DTLS-Tunnel
Encryption    : RC4 AES128                   Hashing     : SHA1
Bytes Tx      : 35466                        Bytes Rx    : 27543
Group Policy   : SSLClientPolicy             Tunnel Group : SSLClientProfile
Login Time    : 20:06:59 UTC Tue Oct 16 2007
Duration      : 0h:00m:12s
NAC Result    : Unknown
VLAN Mapping  : N/A                          VLAN        : none

ciscoasa(config-group-policy)#
```

The **vpn-sessiondb logoff name username** command logs off users by user name. An *Administrator Reset* message is sent to the user when disconnected.

```
ciscoasa(config)#vpn-sessiondb logoff name matthewp
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "matthewp" logged off : 1

ciscoasa(config)#
```

For more information about the AnyConnect 2.0 client, refer to Cisco AnyConnect VPN Administrator Guide.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands (Optional)

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug webvpn svc 255** Displays debug messages about connections to SSL VPN clients over WebVPN.

Successful AnyConnect Login

```
ciscoasa(config)#debug webvpn svc 255
INFO: debug webvpn svc enabled at level 255.
ciscoasa(config)#ATTR_FILTER_ID: Name:
```

SSLVPNClientAccess

```
, Id: 1, refcnt: 1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.10.1.5' -
!--- Outside IP of ASA
```

```
Processing CSTP header line: 'Host: 10.10.1.5'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' -
!--- AnyConnect Version
```

```
Processing CSTP header line: 'User-Agent: Cisco AnyConnect
                                VPN Client 2, 0, 0343'
Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=3338474156@28672@1192565782@EFB9042D72C
63CE02164F790435897AC72EE70AE'
Processing CSTP header line: 'Cookie: webvpn=3338474156@28672@119
2565782@EFB9042D72C63CE02164F790435897AC72EE70AE'
Found WebVPN cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C
63CE02164F790435897AC72EE70AE'
WebVPN Cookie: 'webvpn=3338474156@28672@1192565782@EFB9042D72C63CE02
164F790435897AC72EE70AE'
IPADDR: '3338474156', INDEX: '28672', LOGIN: '1192565782'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: wkstation1' -
!--- Client desktop hostname
```

```
Processing CSTP header line: 'X-CSTP-Hostname: wkstation1'
Setting hostname to: 'wkstation1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1206'
Processing CSTP header line: 'X-CSTP-MTU: 1206'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451CB0948AFBE98296FD849
49EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
Processing CSTP header line: 'X-DTLS-Master-Secret: 72B8AD72F327059AE22CBB451C
B0948AFBE98296FD84949EB6CAEDC203865C76BDBD634845FA89634C668A67152ABB51'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.25.1/255.255.255.0 -
!--- IP assigned from IP Pool
```

```
CSTP state = HAVE_ADDRESS
SVC: NP setup
np_svc_create_session(0x7000, 0xD41612C8, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got internal message
Unable to initiate NAC, NAC might not be enabled or invalid policy
```

Unsuccessful AnyConnect Login (Bad Password)

```
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_portal.c:http_webvpn_kill_cookie[627]
webvpn_auth.c:http_webvpn_pre_authentication[1905]
WebVPN: calling AAA with ewsContext (-717386088) and nh (-717388536)!
WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[4380]
WebVPN: AAA status = (REJECT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1808]
ewaFormSubmit_webvpn_login: tgCookie = 0
ewaFormSubmit_webvpn_login: cookie = d53d2990
ewaFormSubmit_webvpn_login: tgCookieSet = 0
ewaFormSubmit_webvpn_login: tgroup = NULL
webvpn_auth.c:http_webvpn_post_authentication[1180]
WebVPN: user: (matthewp) rejected.
http_remove_auth_handle(): handle 9 not found!
webvpn_portal.c:ewaFormServe_webvpn_login[1749]
webvpn_portal.c:http_webvpn_kill_cookie[627]
```

Related Information

- [Cisco AnyConnect VPN Client Administrator Guide, Version 2.0](#)
 - [Release Notes for AnyConnect VPN Client, Release 2.0](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

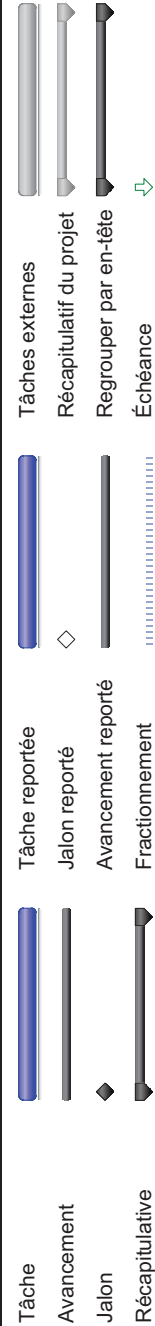
© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

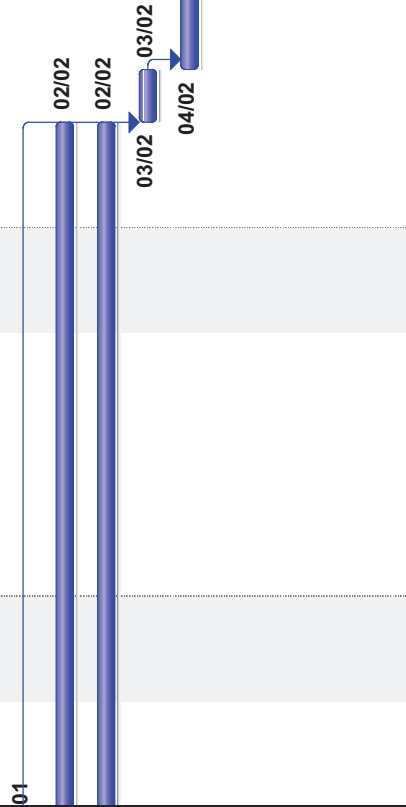
Updated: Nov 06, 2007

Document ID: 99756

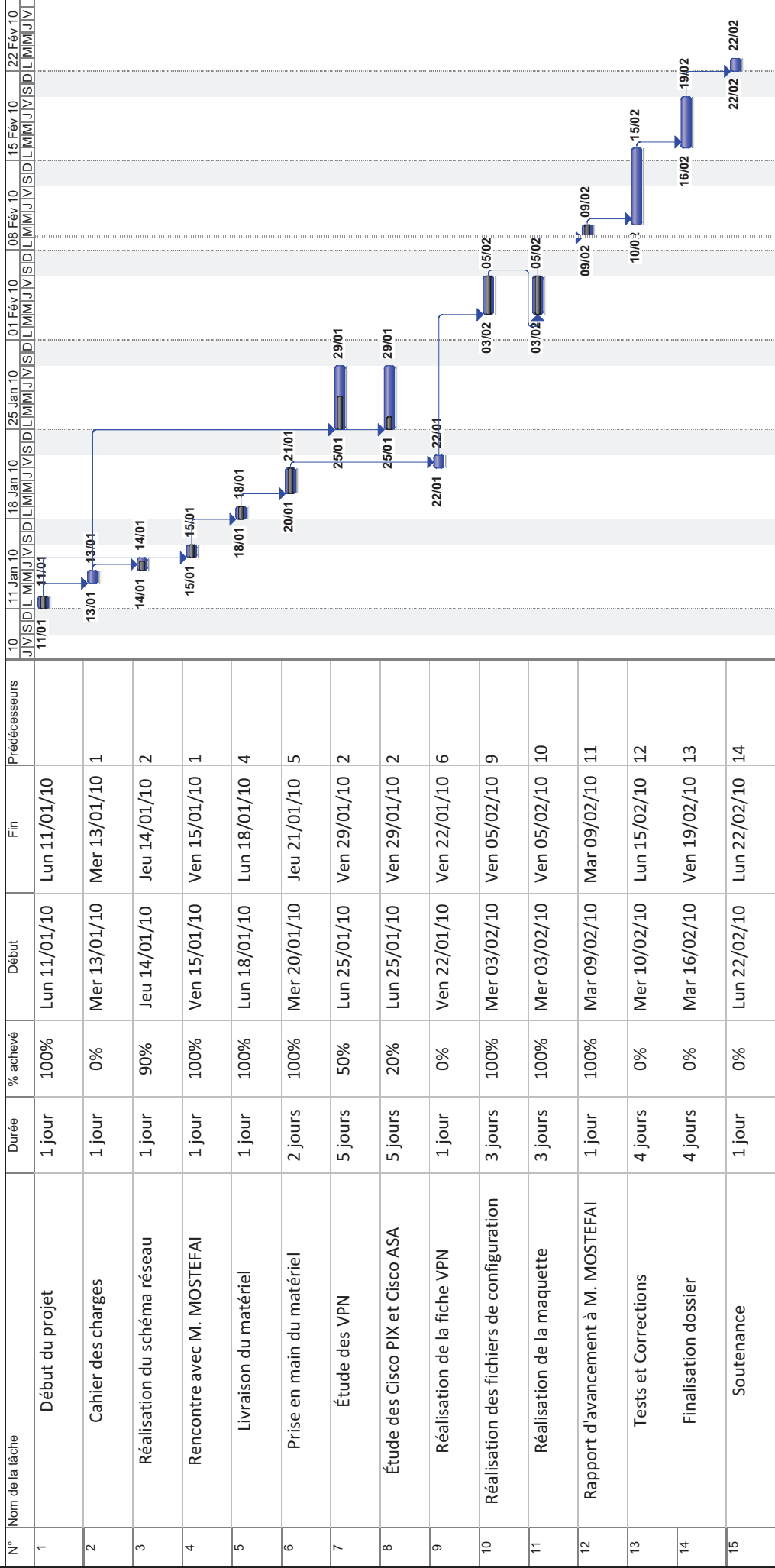
Boris PASCAULT - Gaël RIVOIRAS
LP QSSI - Groupe B
Promotion 2009-2010

N°	Nom de la tâche	Durée	Début	Fin	Prédécesseurs	S	D	L	M	J	V	S	D	L	M	M
1	Début du projet	1 jour	Lun 11/01/10	Lun 11/01/10		11/01										
2	Cahier des charges	1 jour	Mer 13/01/10	Mer 13/01/10	1											
3	Réalisation du schéma réseau	1 jour	Jeu 14/01/10	Jeu 14/01/10	2											
4	Rencontre avec M. MOSTEFAI	1 jour	Ven 15/01/10	Ven 15/01/10	1											
5	Livraison du matériel	1 jour	Lun 18/01/10	Lun 18/01/10	4											
6	Prise en main du matériel	1 jour	Mar 19/01/10	Mar 19/01/10	5											
7	Étude des VPN	10 jours	Mer 20/01/10	Mar 02/02/10	2											
8	Étude des Cisco PIX et Cisco ASA	10 jours	Mer 20/01/10	Mar 02/02/10	2											
9	Réalisation de la fiche VPN	1 jour	Mer 03/02/10	Mer 03/02/10	6											
10	Réalisation des fichiers de configuration	2 jours	Jeu 04/02/10	Ven 05/02/10	9											
11	Réalisation de la maquette	4 jours	Lun 08/02/10	Jeu 11/02/10	10											
12	Tests et Corrections	4 jours	Ven 12/02/10	Mer 17/02/10	11											
13	Finalisation dossier	4 jours	Jeu 18/02/10	Mar 23/02/10	12											
14	Soutenance	1 jour	Mer 24/02/10	Mer 24/02/10	13											
15	Fin du projet	1 jour	Ven 26/02/10	Ven 26/02/10	14											
























Projet : VPN Cisco ASA Date : Mer 20/01/10	
Tâche	Tâche reportée
Avancement	Jalon reporté
Jalon	Avancement reporté
Récapitulative	Fractionnement
	Tâches externes
	Récapitulatif du projet
	Regrouper par en-tête
	Échéance



Projet : VPN Cisco ASA Date : Mar 09/02/10	Tâche Avancement Jalon	Récapitulative Tâche reportée Jalon reporté	Avancement reporté Fractionnement Tâches externes	Récapitulatif du projet Regrouper par en-tête Échéance
---	------------------------------	---	---	--

N°	Nom de la tâche	Durée	% achevé	Début	Fin	Prédécesseurs
1	Début du projet	1 jour	100%	Lun 11/01/10	Lun 11/01/10	
2	Cahier des charges	1 jour	100%	Mer 13/01/10	Mer 13/01/10	1
3	Réalisation du schéma réseau	1 jour	100%	Jeu 14/01/10	Jeu 14/01/10	2
4	Rencontre avec M. MOSTEFAI	1 jour	100%	Ven 15/01/10	Ven 15/01/10	1
5	Livraison du matériel	1 jour	100%	Lun 18/01/10	Lun 18/01/10	4
6	Prise en main du matériel	2 jours	100%	Mer 20/01/10	Jeu 21/01/10	5
7	Étude des VPN	5 jours	100%	Lun 25/01/10	Ven 29/01/10	2
8	Étude des Cisco PIX et Cisco ASA	5 jours	100%	Lun 25/01/10	Ven 29/01/10	2
9	Réalisation de la fiche VPN	1 jour	100%	Ven 22/01/10	Ven 22/01/10	6
10	Réalisation des fichiers de configuration	3 jours	100%	Mer 03/02/10	Ven 05/02/10	9
11	Réalisation de la maquette	3 jours	100%	Mer 03/02/10	Ven 05/02/10	10
12	Rapport d'avancement à M. MOSTEFAI	1 jour	100%	Mar 09/02/10	Mar 09/02/10	11
13	Tests et Corrections	4 jours	100%	Mer 10/02/10	Lun 15/02/10	12
14	Finalisation dossier	4 jours	100%	Mar 16/02/10	Ven 19/02/10	13
15	Soutenance	1 jour	100%	Lun 22/02/10	Lun 22/02/10	14

Projet : VPN Cisco ASA Date : Mar 23/02/10	
Tâche	<div></div> <div></div> <div></div>
Avancement	<div></div> <div></div> <div></div>
Jalon	<div></div> <div></div> <div></div>
Récapitulative	<div></div> <div></div> <div></div>
Tâche reportée	<div></div> <div></div> <div></div>
Jalon reporté	<div></div> <div></div> <div></div>
Avancement reporté	<div></div> <div></div> <div></div>
Fractionnement	<div></div> <div></div> <div></div>
Tâches externes	<div></div> <div></div> <div></div>
Régrouper par en-tête	<div></div> <div></div> <div></div>
Échéance	<div></div> <div></div> <div></div>
Récapitulatif du projet	<div></div> <div></div> <div></div>