UNIVERSITE DE MARNE LA VALLEE
FILIERE INFORMATIQUE RESEAU
ANNEE 2002-2003

ADRIEN MACHADO
FABIEN LOCUSSOL

EXPOSE RESEAU
CLIENT LEGER

SOMMAIRE

1. ARCHITECTURE 5

1.1 PRESENTATION 5
1.1.1 Le modèle Client/Serveur 5
1.1.2 Architecture Client/Serveur traditionnelle 6
1.1.3 Architecture Client-Léger/Serveur 7
1.2 FONCTIONNEMENT 9
1.3 ELEMENTS D'ARCHITECTURE 9
1.3.1 Vocabulaire 9
1.3.2 Deux architectures possibles 10

2. TECHNOLOGIE 12

2.1 MULTIWIN 12
2.2 ICA 12
2.2.1 Présentation des paquets ICA 13
2.2.2 Les différentes commandes 14
Les commandes de canaux virtuels permettent la transmission des informations concernant les différents canaux virtuels entre le client et le serveur. 14
2.2.3 Encapsulation de paquet ICA 15
2.2.4 Canaux virtuels 16
2.3 TECHNOLOGIE SPEEDSCREEN 17
2.4 IMA 18
2.4.1 Citrix Management Console 18
2.4.2 Sous-systèmes IMA 19
2.4.3 Magasin de données (Data Store) 19
2.4.4 Cache de l'hôte local 20
2.4.5 Zones 20
2.4.6 Collecteur de données (Data Collector) 21
2.4.7 Priorité 21

3. AVANTAGES 23

4. ELEMENTS FINANCIERS 25

4.1 COUT DE POSSESSION DES APPLICATION - TCO 25
4.1.1 Capital matériel, réseau et logiciel 25
4.1.2 Gestion des systèmes et des réseaux 25
4.1.3 Support Technique 26
4.1.4 Utilisateurs finaux et coûts afférents 26
4.1.5 Répartition du TCO (GartnerGroup) 27
4.2 SOLUTION – JUSTIFICATIONS ECONOMIQUES – APPROCHE TCO 28
4.2.1 Réduction du TCO avec l'apport d'une solution client léger/serveur 29
4.2.2 Capital matériel, réseau et logiciel 29
4.2.3 Administration des systèmes et réseaux, support technique 29
4.2.4 Utilisateurs finaux et coûts associés 30
4.2.5 Autres éléments de TCO 30
4.2.6 Conclusion 31

5. SECURITE EN ARCHITECTURE CENTRALISEE CITRIX 32

5.1 IDENTIFICATION DES FLUX D'INFORMATIONS UTILISES 32
5.1.1 Gestion des sessions ICA 32
5.1.2 Explorateur ICA 32
5.2 ETABLISSEMENT DES CONNEXIONS 33
5.2.1 Architecture simple 33
5.2.2 Architecture portail 34
5.3 CONTRAINTES SUR L'APPLICATION D'UNE POLITIQUE DE SECURITE 35
5.3.1 Traversée d'un pare-feu 35
5.3.2 Translation d'adresses 36
5.4 ETAT DE L'ART DES SOLUTIONS DE SECURITE 37
5.4.1 Critères communs 37
5.4.2 Authentification 38
5.4.3 Filtrage 44
5.4.4 Sécurisation des échanges 52

6. CONCURENTS 59

6.1 MICROSOFT 59
6.2 NEW MOON 60
CONCLUSION 61

Introduction

L'idée clé de Citrix était de transposer le modèle graphique X-Window propre aux systèmes UNIX vers un environnement Microsoft Windows tout en gardant une compatibilité totale du parc applicatif Windows. C'est aujourd'hui chose faite, grâce au protocole ICA (Independent Computing Architecture).

L'architecture ICA® permet à tout type de poste client de faire passer l'exécution des applications du poste individuel au serveur.
Cela se traduit par une gestion des applications centralisée permettant de simplifier les tâches d'installation, d'améliorer le support technique et la sécurité en ne demandant qu'une quantité minimale de bande passante.

Dotés d'une solution Citrix, les responsables informatiques sont en mesure de gérer l'ensemble de leurs applications à partir d'un point unique centralisé. Cette approche offre une simplicité et une efficacité sans pareil, même dans les environnements informatiques les plus complexes.

La famille de produits Citrix se compose de solutions **serveur d'applications (MétaFrame)** et de **serveurs portails (Nfuse)**. Ces solutions permettent un accès Internet sécurisé à des applications Windows®, UNIX® et Java™ à partir de tout poste client, et via tout type de connexion, tout en offrant une facilité de gestion et une extensibilité inégalée.

1. ARCHITECTURE

1.1 PRESENTATION

Le potentiel d'une entreprise à gagner en productivité et en compétitivité se mesure par sa capacité à rendre ses applications accessibles de la manière la plus simple, la plus rapide possible, au plus grand nombre d'utilisateurs, au moindre coût et en toute sécurité. On peut distinguer aujourd'hui deux modèles d'architecture permettant à une entreprise de mettre ses applications à disposition des utilisateurs :

- Le modèle de base Client/Serveur,
- Le modèle dérivé Client Léger/Serveur.

1.1.1 LE MODELE CLIENT/SERVEUR

L'informatique client/serveur résulte de l'évolution logique des environnements réseau actuels et offre la possibilité aux entreprises d'étendre les ressources, de simplifier le déploiement et la gestion des applications et de réduire les frais liés à l'acquisition des applications. Le modèle client/serveur répartit le traitement d'applications entre les différents ordinateurs d'un réseau.

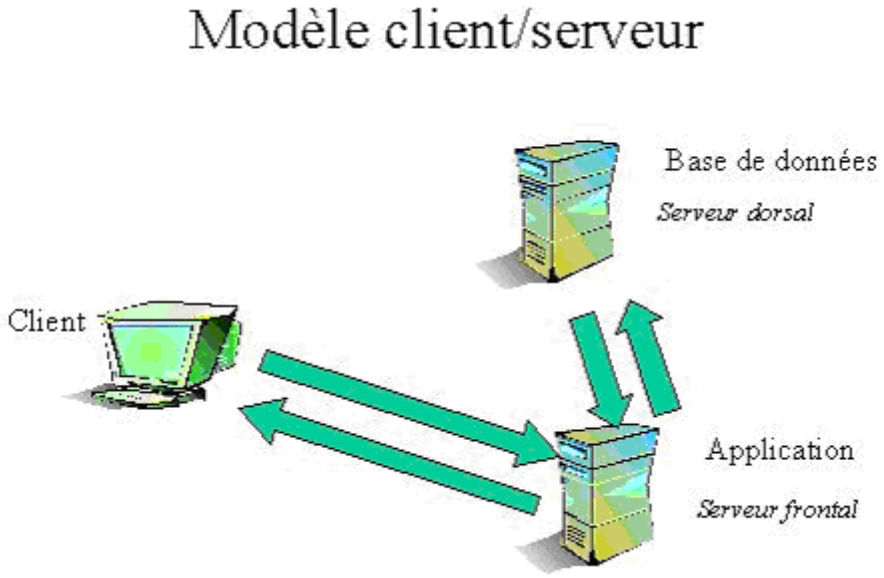


FIGURE 1 : MODELE CLIENT/SERVEUR

Une application client/serveur est constituée d'un logiciel serveur et d'un logiciel client.

Le logiciel client est responsable de l'interface avec l'utilisateur. L'utilisateur entre des données à l'écran qui sont transformées en une requête par le logiciel client. Cette requête est écrite dans un langage spécifique comme par exemple le protocole HTTP pour le Web. Cette requête est envoyée par le logiciel client au logiciel serveur.

Le logiciel serveur récupère les requêtes des logiciels clients qui s'adressent à lui. Il exécute la requête et renvoie le résultat au logiciel client demandeur. Le logiciel client reçoit le résultat et modifie l'affichage en conséquence du côté utilisateur.

Le logiciel serveur est généralement installé sur un ordinateur puissant et dédié à ce service car il est destiné à traiter toutes les requêtes des utilisateurs souhaitant utiliser le service. Souvent l'informatique client/serveur est utilisée pour interroger une base de données et la modifier. La machine hébergeant le logiciel serveur est appelé serveur frontal ; ce service reçoit les requêtes des clients et les traite en collaboration avec une base de données. Un serveur appelé serveur dorsal est chargé de la gestion et de l'hébergement de la base de données.

1.1.2 ARCHITECTURE CLIENT/SERVEUR TRADITIONNELLE

Les applications d'une entreprise, quelle que soit son architecture, sont de deux types :

- Les applications locales, c'est à dire les applications dont le traitement s'effectue entièrement sur un ordinateur,
- Les applications dites client/serveur, c'est à dire les applications dont le traitement est réparti entre différents ordinateurs du réseau : elles sont en effet constituées d'un logiciel serveur spécifique installé sur un serveur d'applications et d'un logiciel client spécifique installé sur un autre ordinateur.

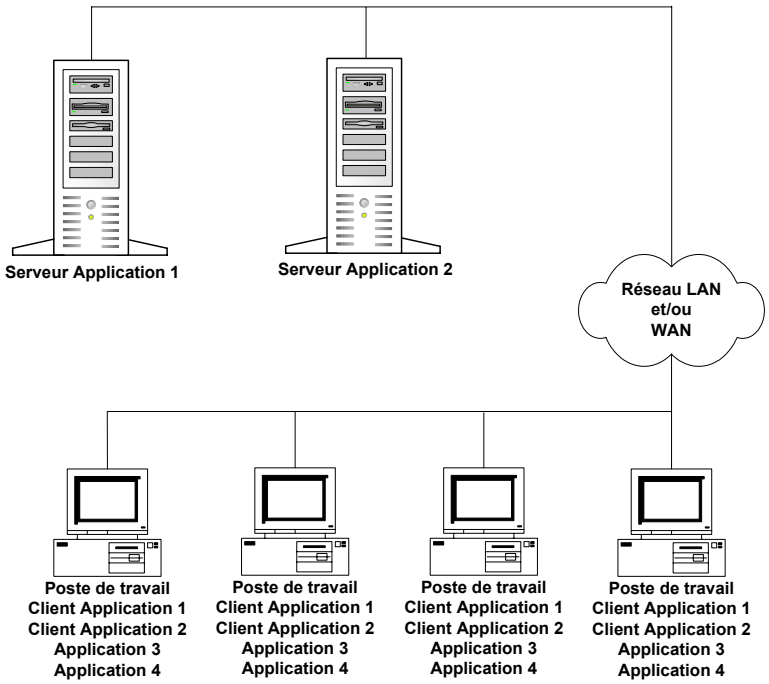


FIGURE 2 : ARCHITECTURE CLIENT/SERVEUR TRADITIONNELLE

Les applications 1 et 2 sont des applications client/serveur alors que les applications 3 et 4 sont des applications locales.
Dans ce type d'architecture, toutes les applications sont installées sur chaque poste de travail utilisateur: les applications 3 et 4 et le logiciel client des applications 1 et 2.

1.1.3 ARCHITECTURE CLIENT-LEGER/SERVEUR

L'architecture en question est dite « Architecture Client Léger/Serveur » parce que tout le traitement des applications ou presque est pris en charge par des serveurs; les postes client, qu'ils soient "lourds" ou "légers", accèdent aux applications via ces serveurs, sans qu'il soit nécessaire de télécharger ou de réécrire les applications.

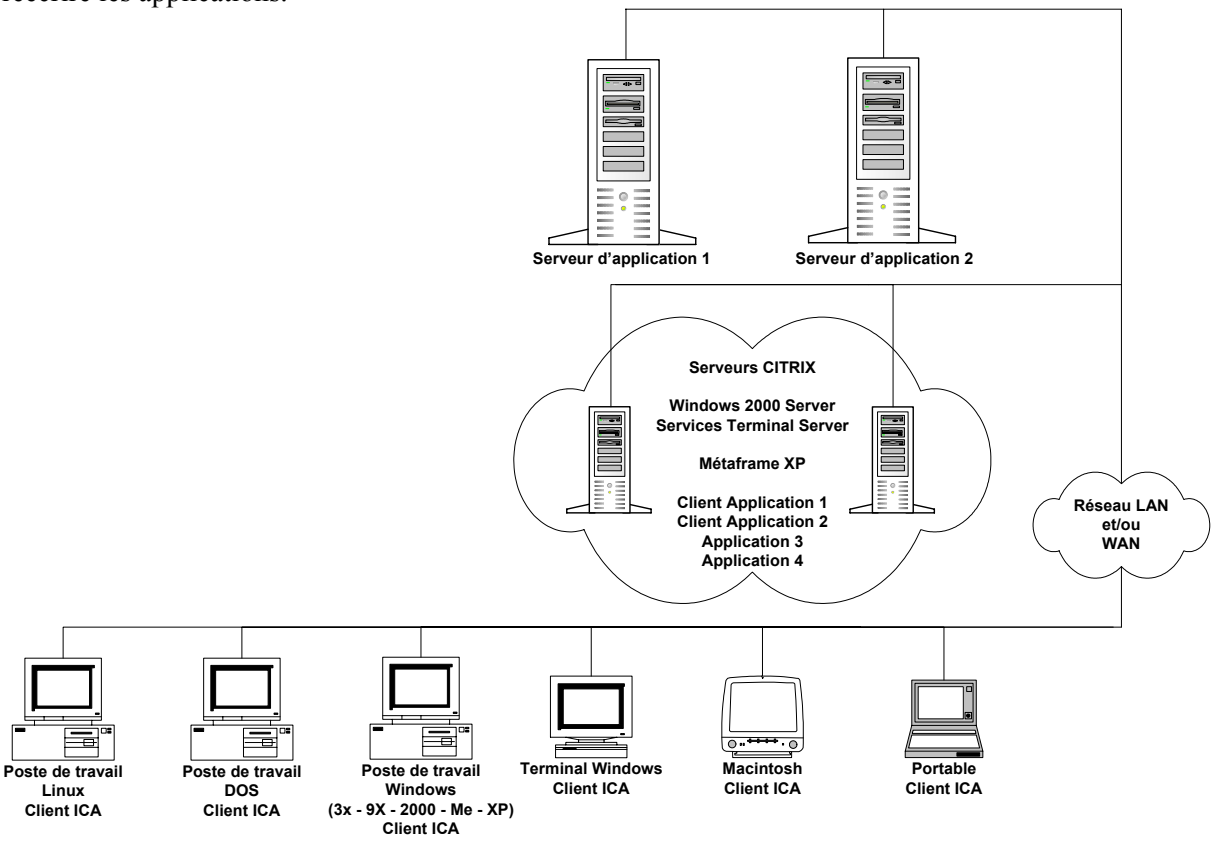


Figure 3 : Architecture Client-Léger/Serveur

L'architecture "Client Léger/Serveur" comporte trois composants essentiels :

- Un système d'exploitation multi-utilisateur

Comme le montre la figure 2, des serveurs sont regroupés en "batterie" et supportent chacun un système d'exploitation Windows 2000 avec le composant Services Terminal Server.
Ce composant permet à Windows 2000 d'avoir la fonctionnalité multi-utilisateur. Cela signifie que, lorsqu'il est installé sur un serveur Windows 2000, chaque utilisateur dispose sur ce serveur d'une émulation Windows 2000 sur laquelle tournent ses applications. Ainsi plusieurs utilisateurs peuvent se connecter en même temps sur ces serveurs et exécuter des applications dans des sessions indépendantes et protégées.

- La technologie MétaFrame

C'est un élément capable de séparer la logique d'une application de son interface utilisateur, de telle sorte que seules les frappes clavier, les clics souris et les différences d'affichage écran transitent sur le réseau. Ainsi, la batterie Citrix distribue la présentation de chaque interface utilisateur vers les postes clients.
Cette technologie s'appuie sur un composant logiciel serveur (le logiciel MétaFrame), un composant protocole de réseau (le protocole ICA) et un composant logiciel client (le client ICA).

- Le logiciel MétaFrame

MétaFrame XP 1.0 est la dernière version du composant logiciel serveur. Il s'agit d'une couche logicielle ajoutée au système d'exploitation multi-utilisateurs sur chaque serveur de la batterie Citrix.

- Le protocole ICA

La communication entre le logiciel serveur MétaFrame et le logiciel client est réalisé au moyen du protocole propriétaire ICA de Citrix. Ce protocole permet à n'importe quel périphérique client d'accéder à n'importe quelle application par n'importe quel type de connexion réseau. ICA est un protocole de services de présentation distant grâce auquel seules les frappes clavier, les clics de souris et les mises à jour d'écran circulent sur le réseau.

- Le client ICA

Il s'agit d'un client universel.
Comme le montre la figure 2, chaque utilisateur informatique de l'entreprise dispose d'un seul logiciel client installé sur son poste de travail, et ce quel qu'il soit. Il s'agit du client ICA de Citrix. Grâce à lui, les utilisateurs ont accès à l'ensemble des applications de l'entreprise.

- La gestion centralisée des applications et des postes clients

Dans l'architecture que montre la Figure 1, toutes les applications de l'entreprise sont installées sur chaque poste de travail des utilisateurs informatiques. Alors que dans l'architecture que montre la Figure 2, toutes les applications de l'entreprise sont installées uniquement en un point central qui est la batterie de serveurs Citrix. Dans le cas d'applications Client/Serveur, seul le logiciel client spécifique à l'application est installé.

Le bon fonctionnement des applications de l'entreprise est assuré avec une bande passante considérablement réduite et une station de travail plus légère en termes de puissance de calcul.

1.2 FONCTIONNEMENT

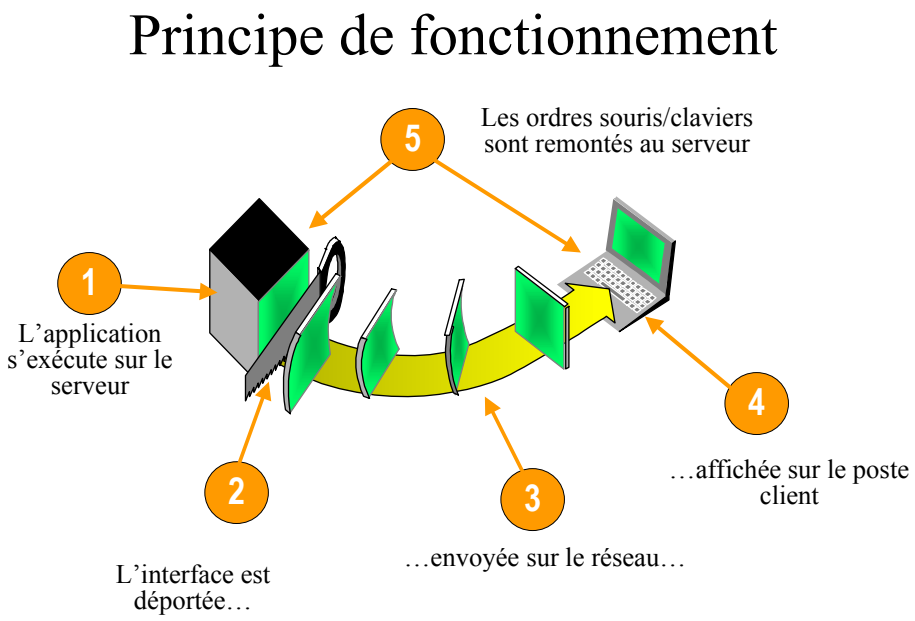


FIGURE 4 : PRINCIPE DE FONCTIONNEMENT DE LA TECHNOLOGIE CITRIX

1.3 ELEMENTS D'ARCHITECTURE

1.3.1 VOCABULAIRE

1.3.1.1 APPLICATION PUBLIEE

Une application publiée est une application accessible via la technologie Citrix. Cette application est exécutée sur le serveur MétaFrame et est accessible en utilisant un logiciel client ICA.

1.3.1.2 FERME DE SERVEURS

Une ferme de serveurs est un ensemble de serveurs sur lesquels sont publiées des applications. L'utilité principale d'une ferme de serveurs est de réaliser de la répartition de charge (« load balancing ») entre les différents serveurs en fonction des applications publiées sur chacun d'eux.

1.3.2 DEUX ARCHITECTURES POSSIBLES

On distingue principalement deux types d'architectures centralisées basées sur la technologie Citrix :

- L'architecture simple : l'accès aux applications publiées est effectué par l'intermédiaire d'un client ICA.
- L'architecture portail : l'accès aux applications publiées est réalisé par l'intermédiaire d'une page web.

1.3.2.1 L'ARCHITECTURE SIMPLE

L'architecture simple est composée de clients ICA reliés à une ferme de serveurs d'applications (serveurs Citrix MetaFrame). L'utilisateur accède aux applications sur Metaframe via un programme spécifique (Program Neighborhood) permettant la gestion locale des paramètres de connexion (fichiers ICA). Le contrôle d'accès et l'autorisation d'accès aux applications sont effectués sur le serveur Metaframe. La saisie du login et du mot de passe (si nécessaire) est réalisée à l'ouverture de la session avec le serveur mais peut être automatisée dans le logiciel Neighborhood.
Une variante est possible en accédant aux paramètres de connexions par le navigateur web. L'utilisateur accède aux applications sur le serveur Metaframe via le chargement http d'un fichier de paramètres de connexion ICA exécuté par le programme ActiveX WFICA32.EXE. Le contrôle d'accès et l'autorisation d'accès aux applications sont effectués sur le serveur Metaframe. La saisie du login et du mot de passe (si nécessaire) est réalisée à l'ouverture de la session avec le serveur.
Ces deux architectures supportent la fonctionnalité de « Load Balancing » au travers du protocole TCPIP port UDP 1604. Une fois connecté, le client Citrix, quel qu'il soit utilisant toujours le port TCP 1494.

1.3.2.2 L'ARCHITECTURE PORTAIL

1.3.2.2.1 PRESENTATION

L'adoption d'Internet par les entreprises constitue le moteur d'entraînement du concept de réseau universel, c'est-à-dire l'intégration transparente des réseaux locaux (LAN), des réseaux étendus (WAN), de l'Internet, des intranets et des extranets qui permet aux entreprises d'optimiser leurs communications. Toutefois, aujourd'hui, peu d'applications critiques sont conçues pour être déployées via le Web. De nombreuses entreprises sont en train de réécrire leurs applications existantes pour la publication sur le réseau en utilisant du code HTML, des scripts Java et d'autres moyens propriétaires.
Mais cette approche nécessite un investissement de temps et d'argent considérable. Pour tirer parti du réseau rapidement et dans de bonnes conditions de rentabilité, les entreprises ont besoin d'une solution qui leur permette d'intégrer et de publier les applications nouvelles et existantes dans tout navigateur Web standard. Et cela instantanément.
Les produits de portails applicatifs de Citrix fonctionnent en toute transparence avec les solutions Citrix de gestion et de déploiement d'applications, ce qui permet aux entreprises de regrouper leurs applications et les informations dans une seule vue de portail. Les utilisateurs peuvent alors y accéder à partir de tout navigateur Web, de tout type de poste client, via tout type de connexion, et en tout lieu. En outre, tout contenu de portail peut être personnalisé de telle sorte que les utilisateurs reçoivent les applications et les informations dont ils ont besoin pour travailler efficacement. Citrix NFuse est le portail applicatif de Citrix pour environnement MétaFrame.
Il est téléchargeable gratuitement dans sa version 1.6.

1.3.2.2.2 FONCTIONNEMENT

L'architecture portail est composée de clients ICA, d'un service Web auquel on a ajouté l'extension NFuse de Citrix et d'une ferme de serveurs d'applications. L'utilisateur accède aux applications via une page HTML de son navigateur.
Le service Web est utilisé pour récupérer l'identité et le mot de passe puis afficher, dans une page HTML, les liens d'accès aux applications autorisées à cet utilisateur. Ce dernier clique sur l'application désirée ce qui déclenche le transfert d'un fichier ICA personnalisé qui est ensuite interprété et exécuté par le client ICA ActiveX.

2. TECHNOLOGIE

2.1 MULTIWIN

MultiWin est une technologie Citrix qui permet à plusieurs utilisateurs de partager simultanément l'unité centrale, les cartes réseau, les ports d'Entrée/Sortie et autres ressources figurant sur la console du serveur. Ainsi, plusieurs utilisateurs peuvent se connecter et lancer des applications dans des sessions protégées distinctes sur le serveur sans être gênés par les autres utilisateurs. A l'origine, Citrix a développé la technologie MultiWin pour sa gamme de produits WinFrame.

En mai 1997, Microsoft a acquis une licence d'exploitation de la technologie MultiWin pour l'incorporer à son produit Windows NT Server 4.0, Terminal Server Edition (TSE), permettant ainsi à plusieurs utilisateurs d'accéder simultanément au même produit.

Aujourd'hui, Microsoft a intégré la technologie MultiWin au service Terminal Server de ses produits Windows 2000 Server.

2.2 ICA

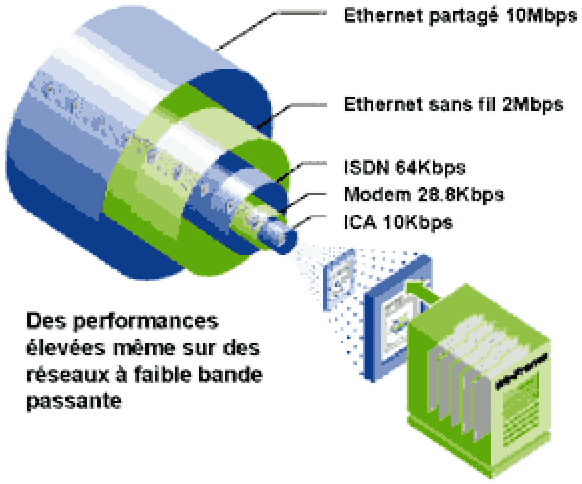


FIGURE 5 : FLUX ICA

L'architecture ICA Independant Computing Architecture) est le protocole de services de présentation à distance multicanal développé par Citrix. Le protocole ICA utilise généralement 10 à 20kbps de la bande passante pour transférer des données entre le serveur et le client ICA.

Sur le serveur, le protocole ICA sépare la logique d'une application de son interface utilisateur et envoie l'interface utilisateur ainsi que les données audio à la machine cliente.

Sur le client ICA, l'utilisateur peut ainsi voir l'interface utilisateur de l'application et entendre les données audio. Le client ICA utilise le protocole ICA pour renvoyer les frappes clavier et les clics souris au serveur. Le protocole ICA permet :

- exécute la logique de toutes les applications sur le serveur;
- réduit le trafic en transférant les rafraîchissements d'écran, les données audio, les frappes clavier et les clics souris entre le serveur et le client;
- utilise comme protocole de transport les protocoles LAN et WAN standards (IPX, SPX, TCP/IP, NetBIOS et NetBEUI) ainsi que les connexions réseau traditionnelles (asynchrone, RNIS, relais de trames, ATM et autres);
- permet aux applications d'être exécutées rapidement, comme sur un réseau local, même avec des connexions à très faible débit;
- permet aux applications 16 et 32 bits les plus récentes de fonctionner sur des ordinateurs clients anciens qui normalement ne pourraient pas les exécuter.

2.2.1 PRESENTATION DES PAQUETS ICA

Un paquet ICA est composé d'une commande d'un octet obligatoire et de données optionnelles. Le paquet peut comporter comme préfixe des préambules qui sont négociés au moment de la connexion afin de gérer la transmission du paquet. La nature du support de transmission (réseau local et connexion asynchrone) et les options définies par l'utilisateur (telles que la compression) ont une incidence sur la définition globale du paquet.

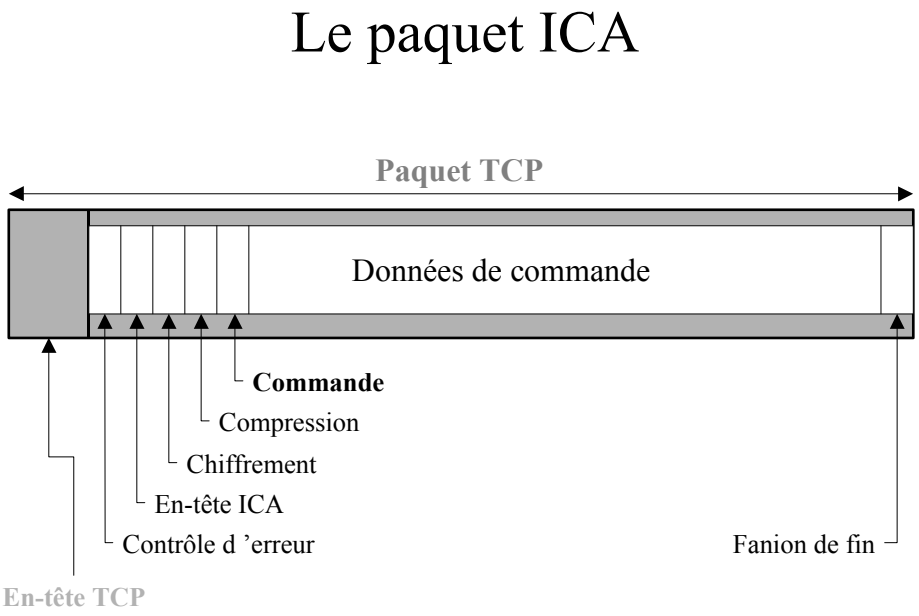


FIGURE 6 : PAQUET ICA

Les cinq premiers champs et le dernier ont une taille de un octet. Ils sont tous facultatifs sauf le champ de « commande ».
L'en-tête et le fanion sont présents dans le cas où le protocole de transport n'assure pas lui-même la fragmentation comme TCP.
Le champ de contrôle d'erreur est utilisé pour la détection d'erreur, la garantie de livraison et le séquencement des paquets. Il n'est présent que si le protocole de couche inférieure est non fiable.
Les champs relatifs au chiffrement et à la compression sont également optionnels. Ils servent respectivement à la gestion d'un paquet ICA chiffré et à la gestion de données compressées.
Le champ « commande » est le seul champ obligatoire. C'est l'en-tête du paquet ICA de base.
Le champ « données de commande » contient les attributs associés au champ « commande ». La longueur de ce champ dépend de la commande et peut être vide. Ce champ est destiné à contenir les paquets des canaux virtuels.

2.2.2 LES DIFFERENTES COMMANDES

2.2.2.1 LES COMMANDES DE CONTROLE

Les commandes de contrôle permettent la gestion de la relation entre l'application qui s'exécute sur le serveur et l'affichage au niveau du client. On trouve notamment les commandes suivantes :

- Initialisation de la connexion et négociation des paramètres entre le client et le serveur,
- Contrôle de l'affichage sur le client,
- Parcours de l'arborescence du serveur par le client,
- Gestion de la souris et du clavier

2.2.2.2 LES COMMANDES SOURIS ET CLAVIER

Les commandes souris et clavier sont transmises du client vers le serveur. Un même paquet ICA peut contenir plusieurs codes de touche. Pour la souris, ces commandes permettent non seulement de transmettre la position de la souris en coordonnées normalisées mais également l'état des boutons.

2.2.2.3 LES COMMANDES DE CANAUX VIRTUELS

Les commandes de canaux virtuels permettent la transmission des informations concernant les différents canaux virtuels entre le client et le serveur.

2.2.3 ENCAPSULATION DE PAQUET ICA

Le paquet ICA encapsule les données en les faisant passer par une série de pilotes tels que le cryptage, la compression et la mise en trame. Les paquets, en traversant la pile de protocoles, adaptent les paquets en fonction du support de transmission utilisé. Ces fonctionnalités correspondent à la couche présentation du modèle OSI.

Exemples d'encapsulation :

- Le protocole de transport IPX n'étant pas fiable, un pilote gérant la fiabilité du protocole de transport IPX est ajouté au-dessus du pilote de transport IPX. IPX étant un protocole basé sur des trames, le pilote de mise en trame n'est pas inclus dans le paquet ICA correspondant.
- Le protocole de transport TCP est un protocole de transport orienté flux. Le pilote de mise en trame est ajouté au paquet ICA au-dessus du pilote de transport TCP. TCP étant un protocole de transport fiable, le pilote de contrôle d'erreur n'est pas ajouté au paquet ICA.

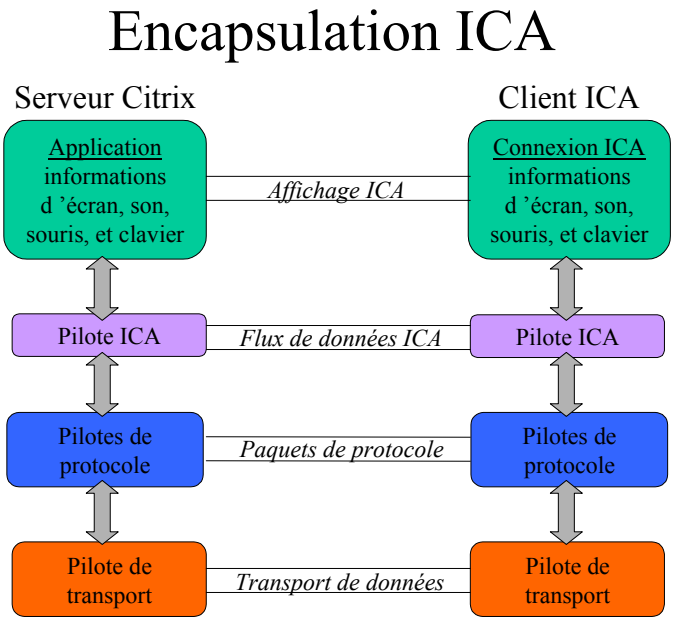


FIGURE 7 : ENCAPSULATION ICA

Lorsque les données sont encapsulées dans les pilotes nécessaires, le paquet ICA est placé sur a couche transport et envoyé au client ICA. Sur le client ICA, le paquet ICA passe à travers les mêmes couches dans l'ordre inverse. Cette opération permet d'extraire les informations du pilote ICA et d'envoyer les données à la couche de destination.

2.2.4 CANAUX VIRTUELS

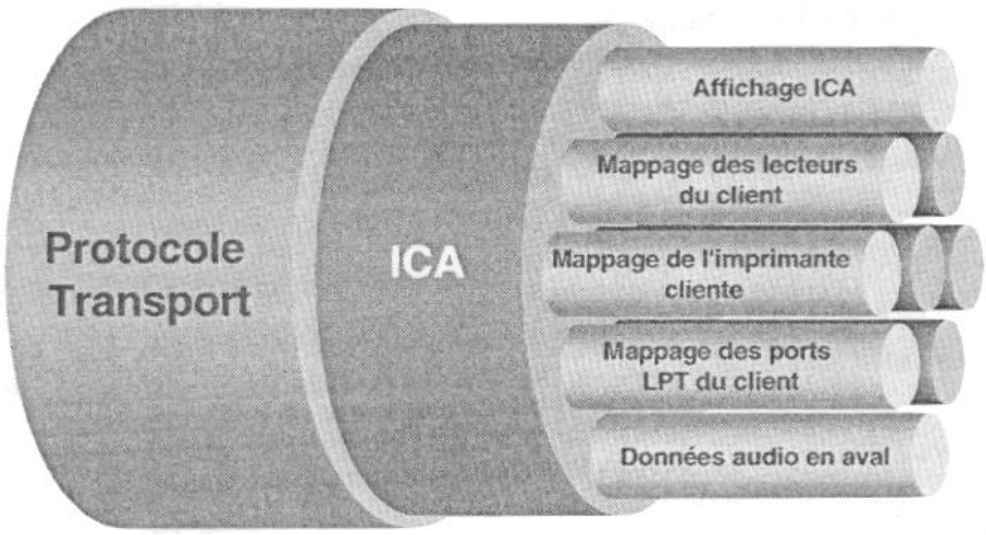


FIGURE 8 : CANAUX VIRTUELS

Le protocole ICA utilise des canaux virtuels pour étendre ses fonctionnalités et inclure divers type de données (audio et vidéo par exemple) et périphériques clients (lecteurs de badge, crayons lecteurs et scanners).

Le protocole ICA peut prendre en charge 32 canaux virtuels et les routeurs intelligents sur le réseau peuvent les classer par ordre de priorité.

En cas d'utilisation de plusieurs canaux virtuels, le protocole ICA intègre les canaux dans un paquet ICA au lieu d'envoyer un paquet par chaîne virtuelle. Ainsi, le protocole ICA n'est pas surchargé et reste efficace.

Voici ci-dessous des exemples de canaux virtuels utilisés par le protocole ICA :

- **Audio** : transmet au client les données audio d'une application exécutée sur le serveur.
- **Presse-papiers** : transmet au client les données du Presse-papiers du serveur et inversement.
- **Mappage des lecteurs** : transmet au client les fonctions du système de fichiers des applications exécutées sur le serveur.
- **Polices et disposition du clavier** : envoie au client la table de clavier et les glyphes de polices qui se trouvent sur le serveur s'ils ne figurent pas dans le cache du disque du client
- **Mappage des ports parallèles** : permet d'accéder aux ports parallèles du client depuis une application ou un spooler exécutés sur le serveur.

- **Mise en file d'attente de l'imprimante** : transmet au client les données à imprimer des applications exécutées sur le serveur.

- **Mappage des ports série** : offre un accès bidirectionnel simultané aux ports série du client depuis une application ou un spooler exécutés sur le serveur.

- **Canal de contrôle de SpeedScreen** : transmet les données de la fonction Réduction de latence SpeedScreen entre le client et le serveur.

- **Affichage ICA** : exporte les images graphiquues de l'application vers le client. La chaîne virtuelle Affichage ICA réduit la bande passante utilisée par MétaFrame XP en envoyant, lorsque cela est possible, uniquement les rafraîchissements d'écran au lieu de l'écran ou du bitmap entier.

2.3 TECHNOLOGIE SPEEDSCREEN

SpeedScreen est l'agent de protocole ICA qui permet de réduire la latence et d'améliorer l'apparence des applications basées sur le serveur en limitant la quantité de bande passante consommée.
La technologie SpeedScreen est constituée de plusieurs composants :

- Reducer 1 et Reducer 2 : il s'agit des algorithmes utilisés pour la compression des flux de données.
- Cache permanent des images bitmap : cache créé sur le disque local du client pour y enregistrer les bitmaps fréquemment utilisés afin de ne pas avoir à les retransmettre.
- Autre méthode de mise en cache : algorithme qui fractionne l'écran en petits éléments et les stocke en mémoire. Lorsque l'écran est modifié, seules les mises à jour incrémentielles et non plus l'intégralité de l'écran sont envoyées au client depuis le serveur.
- Mise en file d'attente et suppression : algorithme qui examine les éléments graphiques envoyés au client. Les données qui ne sont plus valides sont supprimées.
- Réduction de latence SpeedScreen : réduit le délai lorsqu'une action est effectuée au niveau du client ICA et que les informations sont renvoyées par le serveur MétaFrame XP. Cette fonction s'avère particulièrement utile sur les réseaux étendus et les connexions entrantes. La fonction Réduction de latence SpeedScreen traite ces délais de deux façons :

  Retour des cliques souris : transforme temporairement le pointeur de la souris afin d'indiquer qu'une action est en cours. La durée de la transformation du pointeur de la souris dépend de la latence de la connexion réseau.

  Le pointeur de souris reprend sa forme initiale dès réception de la réponse du serveur.
  Echo local du texte : renvoie immédiatement l'information à l'utilisateur en réponse aux données (sur une connexion très lente) en anticipant la réponse du serveur MétaFrame XP. Le résultat réellement fourni par le serveur est appliqué dès qu'il est disponible.
  La fonction Réduction de latence SpeedScreen réduit la latence des connexions nécessitant entre 150 ms et 500 ms pour être établies. Cette fonction apporte une nette amélioration aux connexions nécessitant entre 250 ms et 500 ms. En revanche, son bénéfice n'est pas perceptible pour les connexions à latence inférieure à 150 ms.
  Par défaut, la fonction Réduction de latence SpeedScreen est désactivée pour les connexions ICA sur un réseau local.

2.4 IMA

L'architecture IMA (Independant Management Architecture) constitue l'ossature de MétaFrame XP. Elle fournit la structure des communications de serveur à serveur. L'architecture IMA est un système de gestion centralisée articulé autour de plusieurs sous-systèmes fondamentaux qui définissent et contrôlent l'exécution de produits sur un serveur MétaFrame XP. L'architecture IMA :

- centralise toutes les tâches d'administration dans une seule application avec interface utilisateur appelée Citrix Management Console,
- déploie des sous-systèmes fondamentaux qui assurent ensemble la fonctionnalité des produits Citrix actuels et à venir.

L'architecture IMA peut être exécutée sur tous les serveurs MétaFrame XP et les serveurs fonctionnent selon un modèle homologue. Les communications entre les sous-systèmes IMA sont établies au moyen de messages envoyés sur le protocole TCP/IP depuis des serveurs homologues ou la CMC.

2.4.1 CITRIX MANAGEMENT CONSOLE

La Citrix Management Console remplace les utilitaires d'administration de serveurs Citrix et d'administration de l'équilibrage de charge, ainsi que le gestionnaire d'applications publiées et Citrix Licensing disponibles dans MétaFrame1.8.

La CMC permet aux administrateurs de gérer les serveurs MétaFrame XP. Elle peut aussi être exécutée sur tout système disposant de Java Runtime Environment (JRE) version 1.3 ou supérieure, du protocole TCP/IP et de l'un des systèmes d'exploitation suivants :

Microsoft Windows 2000 (Professional, Server, Advanced Server ou Data Center);
Microsoft Windows NT 4.0 (Server ou Workstation);
Microsoft Windows NT Server 4.0, Terminal Server Edition.

Remarque : Un client ICA doit être installé sur le système afin que la CMC puisse observer les sessions ICA.

2.4.2 SOUS-SYSTEMES IMA

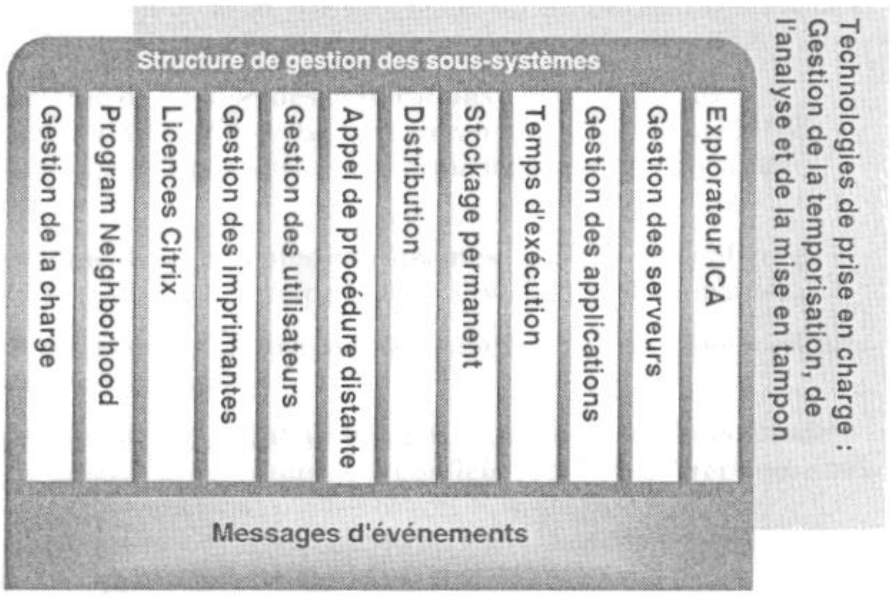


FIGURE 9 : SOUS-SYSTEMES IMA

L'architecture IMA est constituée de sous-systèmes. Un sous-système est un fichier DLL (bibliothèque de liaison de données). Grâce à ces sous-systèmes, l'architecture IMA est modulaire et extensible. Il est possible d'ajouter de nouveaux sous-systèmes et de remplacer des sous-systèmes par des versions plus récentes.

Les sous-systèmes interagissent via une couche de messagerie qui achemine les données à travers les sous-systèmes des serveurs MétaFrame XP de la batterie.

2.4.3 MAGASIN DE DONNEES (DATA STORE)

Le Magasin de données stocke les données de configuration statiques et assure le suivi des informations de la batterie de serveurs MétaFrame XP qui ne changent pas fréquemment. Ce magasin est une base de données qui utilise Microsoft Access, SQL Server ou une base de données Oracle. Le sous-système de stockage permanent met à jour les données du magasin par l'envoi de messages.
Avec MétaFrame XP, les serveurs n'envoient pas les données à tous les serveurs de la batterie. Les informations sont centralisées dans le magasin de données.

Le magasin de données contient les informations suivantes :

- Les informations relatives aux applications publiées, y compris les propriétés de la connexion ICA, le nom de l'application, les utilisateurs autorisés à se connecter à cette application, la taille de la fenêtre, le nombre de couleurs, le niveau de cryptage et le paramétrage audio;
- Les informations sur la configuration du serveur pour la batterie;
- Les informations sur la configuration utilisateur pour la batterie;
- Les informations relatives au pilote d'imprimante et à l'imprimante.

2.4.4 CACHE DE L'HOTE LOCAL

Le cache de l'hôte local est présent sur chacun des serveurs MétaFrame XP de la batterie. Il contient un sous-ensemble des données de configuration stockées dans le magasin. La première fois qu'un serveur est attaché à la batterie, il reçoit une copie des informations du magasin de données et les enregistre dans le cache de l'hôte local.

Lorsqu'un serveur est réinitialisé, il consulte son cache d'hôte local afin d'obtenir les informations requises pour pouvoir être rattaché à la batterie. Une fois le serveur en ligne, le magasin de données informe le cache de l'hôte local des changements. Le cache de l'hôte local reçoit uniquement les données qui ont été modifiées, ce qui permet de réduire le volume de données échangées sur le réseau et de limiter la fréquence des consultations du magasin pour les mises à jour. Au cours de cette opération, le cache de l'hôte local est vérifié toutes les 15 minutes pour assurer la cohérence. Une actualisation peut être provoquée par l'arrêt, puis le redémarrage du service IMA serveur. Remarque : l'interruption et le redémarrage du service IMA du serveur n'ont aucune incidence sur les sessions des utilisateurs connectés. Toutefois, les utilisateurs essayant de se connecter au serveur de l'arrêt ou du redémarrage du service IMA se verront refuser l'accès.
Le cache de l'hôte local peut émunérer les serveurs ainsi que les applications et effectuer un filtrage avec Citrix Program Neighborhood. En cas de défaillance du magasin de données, le serveur continue ainsi à fonctionner en utilisant les informations locales. Le cache de l'hôte local se trouve dans le fichier Program Files\Citrix\IndependantManagementArchitecture\IMALHC.MDB.

2.4.5 ZONES

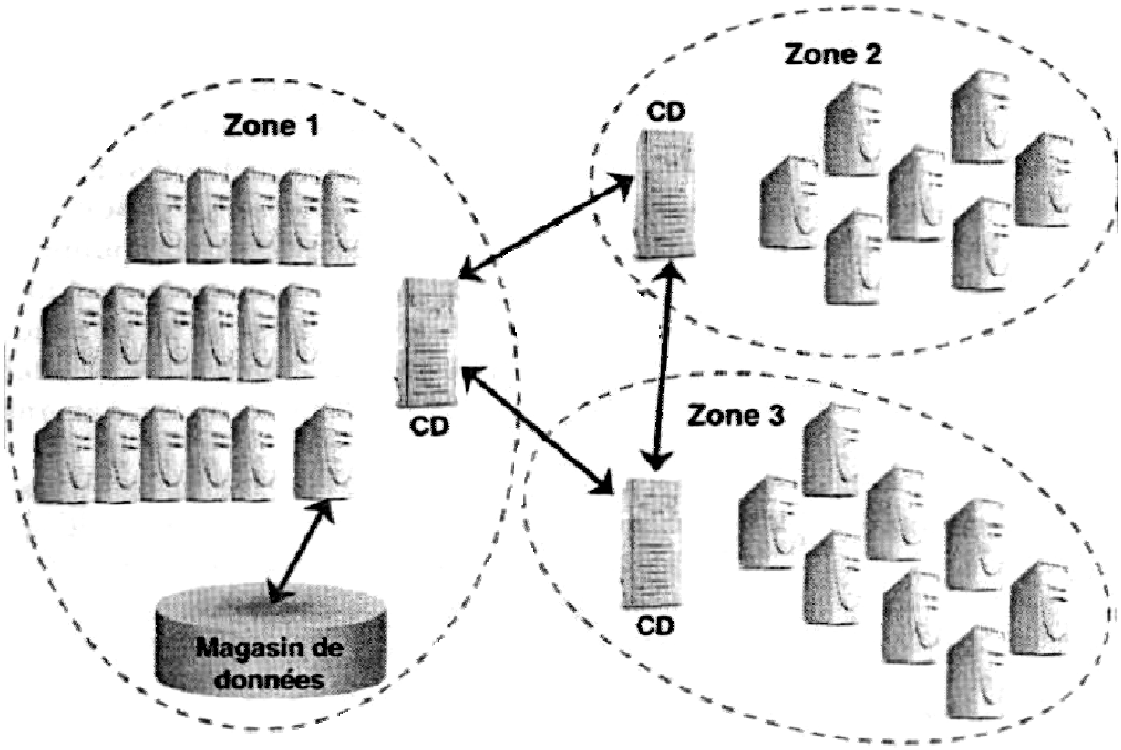


Figure 10 : Zones

Une zone contient un sous-ensemble de serveurs à l'intérieur d'une batterie de serveurs. Chaque zone dispose d'un collecteur de données qui rassemble et diffuse les informations aux serveurs de la zone et aux collecteurs de données des autres zones.
Une zone sert à améliorer les performances d'une batterie de serveurs MétaFrame XP en permettant aux serveurs liés géographiquement d'être rassemblés, qu'ils soient connectés au même sous-réseau ou non.
Par défaut, la zone est l'équivalent du sous-réseau TCP/IP et tous les serveurs sont ajoutés à la zone par défaut.
Si les serveurs de la batterie se trouvent dans des zones, régions ou pays différents, un administrateur peut utiliser la CMC pour créer des zones et configurer les serveurs en fonction des zones auxquelles ils appartiennent.
La séparation des serveurs en zones en fonction de leur situation géographique peut rendre l'administration de la batterie de serveurs plus efficace et améliorer les performances car les collecteurs de données sont moins éloignés de serveurs.

Remarque : les zones peuvent recouvrir plusieurs sous-réseaux et un sous-réseau peut faire partie de plusieurs zones.

2.4.6 COLLECTEUR DE DONNEES (DATA COLLECTOR)

Un collecteur de données est une base de données en mémoire qui met à jour les données spécifiques aux zones.
Les collecteurs de données reçoivent les mises à jour de données incrémentielles et les requêtes en provenance des serveurs de la zone. Les collecteurs de données stockent les informations dynamiques qui ne sont pas liées à la configuration, telles que les charges du serveur, les sessions, actives et déconnectées ainsi que les utilisateurs et les licences en cours d'utilisation. Ils communiquent entre eux afin que chaque zone soit notifiée des mises à jour importantes effectuées dans les autres zones. Grâce à cette `communication entre` les différents collecteurs de données d'une batterie, les serveurs de cette batterie n'ont pas besoin de communiquer entre eux.
Dans chaque zone, un serveur MétaFrame XP fait office de collecteur de données pour cette zone. Ce collecteur de données est l'explorateur ICA principal de cette zone (en mode mixte). Par défaut, le collecteur de données est le premier serveur de la zone. En cas de défaillance du serveur faisant office de collecteur de données, un autre serveur de la zone le remplace en fonction de son niveau de priorité. Un administrateur peut utiliser la CMC pour attribuer un niveau de priorité à chaque serveur.

2.4.7 PRIORITE

Le niveau de priorité permet de déterminer quel serveur MétaFrame XP deviendra Collecteur de données de cette zone.
Les informations relatives à la priorité sont enregistrées avec les notes de version et les fonctionnalités dans le magasin de données. Lorsqu'un serveur collecteur de données tombe en panne, est déconnecté du réseau ou déplacé vers une autre zone, l'un des serveurs de la zone est sélectionné comme collecteur de données par le protocole TCP.
Ce choix est basé sur le niveau de priorité. Dès qu'un serveur est désigné comme collecteur de données, il envoie un message aux autres serveurs de la zone pour les informer de sa nouvelle identité. Tous les messages destinés au collecteur de données seront désormais envoyés à ce nouveau collecteur.

Un administrateur peut utiliser la CMC pour attribuer un niveau de priorité à chaque serveur. Les niveaux de priorité sont les suivants :

- Plus haute priorité : indique que ce serveur devient le collecteur de données pour cette zone. Un seul serveur de la zone doit avoir ce niveau de priorité.

- Prioritaire : inique que ce serveur devient le collecteur de données pour cette zone si aucun serveur n'est sélectionné en tant que Plus haute priorité.

- Priorité par défaut : indique que ce serveur essaie de devenir le collecteur de données pour cette zone, si aucun serveur n'a le niveau de priorité Plus haute priorité ou Prioritaire. Il s'agit du choix par défaut.
  Tous les serveurs qui sont rattachés à une zone sont initialement définis sur Priorité par défaut.

- Sans priorité : indique que ce serveur devient le collecteur de données pour cette zone uniquement si aucun serveur n'a le niveau de priorité Plus haute priorité, Prioritaire ou Priorité par défaut.

Remarque : MétaFrame XP n'utilise pas de collecteur de données de secours. En cas de défaillance du collecteur de données, un nouveau collecteur de données est sélectionné et tous les serveurs de la zone envoient leurs données spécifiques à la zone du nouveau collecteur.

3. AVANTAGES

Les avantages d'une architecture Client Léger/Serveur, apportés par la technologie Citrix, par rapport à une architecture Client/Serveur traditionnelle sont indéniables et multiples.

- **Réduction du Coût de Propriété *TCO***

Avec sa capacité à simplifier le déploiement et l'administration des applications, à faciliter le support technique et à réduire le temps que passent les utilisateurs à maintenir leurs propres ordinateurs, la solution centralisée client léger de Citrix peut permettre d'économiser entre 25% et 30% des coûts afférents aux réseaux.

- **Contrôle centralisé**

En général, le déploiement des applications d'entreprise est onéreux et complexe et demande beaucoup de temps. Il oblige les administrateurs systèmes de l'entreprise à distribuer physiquement les applications sur chaque poste client, à contrôler la présence éventuelle de plusieurs versions, à se charger du support utilisateur, à prendre en compte les nombreuses configurations systèmes. Le logiciel MétaFrame XP de Citrix améliore la gestion des applications en permettant le déploiement quasi instantané, l'administration et le support de ces dernières pour des centaines d'utilisateurs à partir d'un point central. Les mises à jour ne sont effectuées qu'une seule fois : sur le serveur Citrix.

- **Des performances indépendantes de la bande-passante**

Les applications d'entreprise conçues pour des réseaux à large bande passante et des machines de bureau puissantes congestionnent les réseaux et n'offrent que des performances limitées sur des lignes à faible débit.
Le logiciel MétaFrame XP de Citrix est optimisé pour des connexions avec un débit aussi faible que 14400 bps.
Pour cette raison, tout utilisateur distant peut compter sur des performances dans l'utilisation des applications équivalentes à celles d'un réseau local, même lorsque la bande passante est réduite ou le trafic réseau élevé. Cette indépendance par rapport à la bande passante augmente l'efficacité du réseau et réduit de ce fait ses coûts.

- **Intégration dans des environnements informatiques hétérogènes**

L'hétérogénéité des environnements informatiques est un état de chose indéniable pour l'entreprise d'aujourd'hui, avec un large éventail de postes clients, de systèmes d'exploitation, de protocoles et de connexions réseaux.
Le logiciel MétaFrame XP de Citrix offre un accès universel aux applications Windows, indépendamment de la nature du poste client, du système d'exploitation, du type de connexion réseau ou du protocole.

- Hétérogénéité des postes clients

Pratiquement tout poste client peut accéder aux serveurs Citrix MétaFrame sans réécriture de code, sans modification du matériel client ou reconfiguration de ce dernier. Ces postes peuvent être des PC à base de processeur x86 ou de pentium, des terminaux Windows, des portables et des périphériques d'information, aussi bien que des clients DOS, UNIX, OS/2 Warp, Mac OS ...

- Hétérogénéité des connexions réseaux

Les utilisateurs peuvent se connecter au réseau à travers des lignes téléphoniques standards, des liaisons WAN (T1, T3, X.25), des connexions à large bande (RNIS, relais de trame, ATM), des

connexions sans fil, via l'Internet ou des intranets. Les utilisateurs disposent de performances équivalentes à celles des réseaux locaux quelle que soit la connexion réseau utilisée. Pour cette raison, les entreprises évitent des mises à niveau coûteuses de leur structure réseau.

- Hétérogénéité des protocoles de réseaux

Le logiciel Citrix MétaFrame XP supporte tous les protocoles usuels des *LANs* et des *WAN*s, dont TCP/IP, IPX, SPX, NetBIOS.

- Gestion des systèmes

Il n'y a donc pas de limite dans la puissance pouvant être mise en oeuvre côté serveurs. Au fur et à mesure que la taille de l'entreprise passe de quelques dizaines à des centaines voire des milliers d'utilisateurs, les administrateurs réseaux de celle-ci peuvent simplement ajouter de nouveaux serveurs Citrix MétaFrame à la batterie de serveurs en répartition de charge.

- Gestion des applications

Le logiciel MétaFrame XP permet aux administrateurs systèmes de l'entreprise de gérer et d'étendre l'utilisation des applications à toute l'entreprise.

- Intégration transparente des ordinateurs de bureau

Les utilisateurs ont un accès complet à toutes leurs ressources systèmes locales, alors même que les applications tournent à distance sur le serveur Citrix MétaFrame.
Ils n'ont donc pas besoin d'une formation spécifique puisqu'ils continuent à travailler dans leur environnement de travail habituel.

4. ELEMENTS FINANCIERS

4.1 COUT DE POSSESSION DES APPLICATION - TCO

TCO signifie Total Cost of Ownership.

Le TCO d'une organisation englobe quatre domaines principaux :

- Coûts en capital matériel, réseau et logiciel pour les nouvelles acquisitions et mises à niveau,
- Coûts de gestion des systèmes et réseaux,
- Coûts de support technique,
- Coûts des systèmes d'information et coûts liés aux utilisateurs finaux.

De récentes analyses du TCO ont également permis d'identifier d'autres catégories importantes de coûts : dépenses en développement de logiciels, frais de communications réseau et coûts indirects de non-activité résultant des périodes de panne du système.

4.1.1 CAPITAL MATERIEL, RESEAU ET LOGICIEL

Les coûts en capital matériel et logiciel constituent l'élément du TCO le lus palpable et le plus facilement identifiable. Bien que pouvant être significatifs, ils représentent moins du tiers du coût total d'un ordinateur de bureau client. Toutefois, ces coûts ne constituent qu'une partie des coûts totaux. Il faut en effet y ajouter les mises à jour du processeur, de la mémoire physique, de la mémoire de masse et périphériques de stockage, du matériel de connectivité qui peuvent largement dépasser le coût d'acquisition initial.

La plupart des analyses de TCO supposent que le nouveau matériel ou les solutions de gestion ont été achetés à leur coût minimum. Néanmoins, le remplacement à grande échelle des environnements informatiques représente un coût prohibitif.

4.1.2 GESTION DES SYSTEMES ET DES RESEAUX

Bien que moins palpables, les coûts de gestion et d'administration d'un environnement informatique demeurent pourtant un élément à part entière du TCO ; ceux-ci peuvent s'élever à 6275 dollars par ordinateur de bureau Windows 95 au bout de cinq ans d'exploitation. Le déploiement régulier d'applications, c'est-à-dire notamment l'installation, la configuration et la gestion des logiciels, est souvent une activité laborieuse et onéreuse. Non seulement les administrateurs doivent distribuer physiquement les applications à chaque client, mais ils doivent également gérer les problèmes de contrôle des versions, l'administration à distance, les multiples configurations système et la duplication des données.

Les coûts de gestion des systèmes et des réseaux englobent également les coûts de mise en place des technologies d'information et de sous-traitance qui sont associées à la gestion des réseaux, des systèmes et des supports de données. Ces coûts concernent notamment les activités de sauvegarde, de maintenance du matériel, de gestion de la sécurité informatique et celle d'administration des serveurs et des réseaux. Malgré les défis que cela représente, il existe peu de solutions pour répondre aux problèmes sous-jacents de gestion

4.1.3 SUPPORT TECHNIQUE

Comme le coût de gestion, le coût du support technique est moins palpable mais bien réel. Ils englobent les dépenses en main d'œuvre, systèmes et logiciels qui sont engagées pour le support des utilisateurs, les contrats associés, le personnel technique, la formation des utilisateurs finaux et les services annexes. D'après les données du GartnerGroup, le coût du support technique peut s'élever à 8165 dollars sur cinq ans, soit environ 16% du TCO. Des solutions permettent aujourd'hui d'automatiser la procédure de support aux utilisateurs, mais elles n'ont pas résolu les problèmes fondamentaux liés à la nécessité d'administrer des centaines, voire des milliers d'ordinateurs de bureau clients dispersés à travers une organisation.

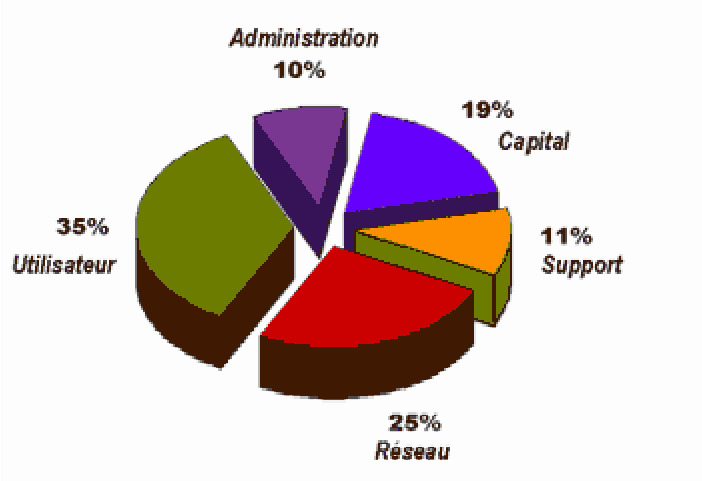
4.1.4 UTILISATEURS FINAUX ET COUTS AFFERENTS

Les coûts indirects liés aux utilisateurs finaux sont les plus difficiles à quantifier et correspondent souvent à l'élément le plus controversé du TCO. Ils englobent les coûts et l'inefficacité des utilisateurs finaux lorsque ceux-ci essaient de résoudre eux-mêmes les problèmes et ceux de leurs collègues au lieu de recourir au service de support. De tels coûts sont quantifiés en temps perdu ou en baisse de productivité résultant d'activités telles que la gestion de fichiers, le développement d'applications personnelles ou de macros et l'auto-formation.

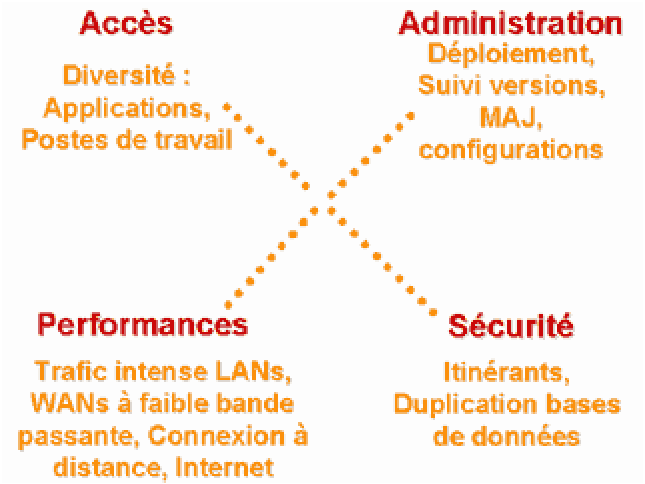
Bien que les environnements PC et client/serveur aient fourni aux utilisateurs finaux les applications dont ils avaient besoin, ils ont malheureusement accentué les contraintes techniques. Par ailleurs, la création de ces environnements s'est faite aux dépens du contrôle et de la sécurité. Dans une architecture c/s traditionnelle, les applications et les données vitales de l'entreprise résident à la fois sur le serveur et les postes clients disséminés en différents lieux. Les risques de détournement (ou accès non autorisés) et de perte d'information sont accrus. Tous ces facteurs représentent 40% du TCO réel d'une organisation.

4.1.5 REPARTITION DU TCO (GARTNERGROUP)

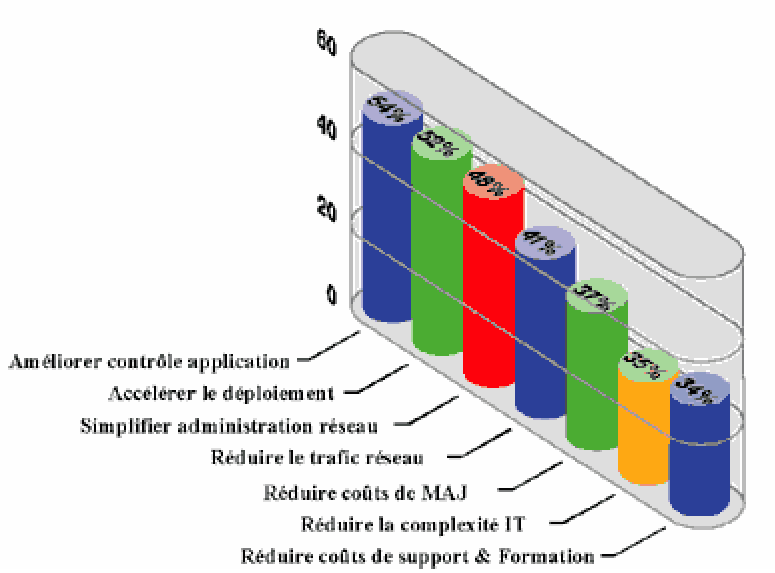
D'après une étude du GartnerGroup, le coût de possession d'une application classique (déployée sur un PC) peut être réparti ainsi :



Le principal challenge que les entreprises doivent relever est le suivant (source Citrix) :



La maîtrise, le déploiement et la facilité d'administration des applications sont les trois facteurs essentiels au choix logiciels dans les entreprises. La diminution du trafic réseau, la simplicité de mise à jour et les nombreuses possibilités MetaFrame (support, formation utilisateur) sont des points auxquels répond parfaitement l'offre Citrix basée sur le concept du client léger. Le schéma suivant détaille les souhaits des directeurs informatiques :



4.2 SOLUTION – JUSTIFICATIONS ECONOMIQUES – APPROCHE TCO

La solution de Citrix est une solution globale, fédérant la diversité logicielle et matérielle existante, et laissant la liberté de choix pour les investissements futurs. Elle préserve les investissements engagés sur les produits logiciels "Microsoft Windows compliant" acquis et déployés dans votre société . Elle ne nécessite aucune mise à jour de ce parc. Le problème de l'évolution des configurations (nouveaux runtimes) disparaît puisque le poste ne gère plus que le simple pilote d'affichage ICA (Independent Computing Architecture, protocole de présentation de Citrix permettant, entre autres, la gestion des événements graphiques de type Windows).

L'adoption d'une telle solution simplifie considérablement la gestion du parc micro de votre société et contribue à réduire les coûts à tous les niveaux (déploiement, administration, gestion des configurations, …).

En effet, le coût réel d'acquisition, de déploiement et d'administration des applications informatiques pour un ensemble d'utilisateurs finaux est bien supérieur au coût d'achat initial d'un PC et des logiciels. Il reste cependant à en déterminer le plus précisément dans quelles proportions. D'après le GartnerGroup, le coût total d'un PC en réseau sous Windows® 95 s'élève à près de 50000$ au bout de cinq ans. Le résultat net d'un passage à la solution client léger proposée par Citrix est une réduction du TCO pouvant aller jusqu'à 57%.

4.2.1 REDUCTION DU TCO AVEC L'APPORT D'UNE SOLUTION CLIENT LEGER/SERVEUR

Dans le modèle client léger/serveur, le déploiement, la gestion, le support et l'exécution des applications se font intégralement sur serveur. Il utilise un système d'exploitation multi-utilisateurs qui permet à plusieurs utilisateurs de se connecter et d'exécuter des applications sur le serveur en sessions indépendantes et protégées. Il emploie une méthode qui consiste à séparer l'application du poste client. Ce dernier est cantonné à traiter les ordres d'affichage qui reçoit au format ICA et à envoyer ses événements clavier/souris au serveur en utilisant le même protocole ICA.

Les sessions client léger/serveur fonctionnent à partir de l'infrastructure et des normes informatiques actuelles ainsi que des produits Windows présents ou à venir. Cela signifie une meilleure rentabilité des investissements informatiques ordinateurs de bureau, réseaux, applications et formation. Les sessions client léger/serveur permettent une réduction des coûts dans les quatre postes clés du TCO.

4.2.2 CAPITAL MATERIEL, RESEAU ET LOGICIEL

Les sessions client léger/serveur offrent une solution basée sur les terminaux Windows qui, de par leur rentabilité, peuvent contribuer à réduire le coût moyen du capital en ordinateurs de bureau de 21%. Par exemple, le déploiement d'une solution client léger/serveur à partir d'une nouvelle génération de matériel client léger comme les terminaux Windows Wyse® Winterm™ – a permis à une société américaine située à San Francisco d'économiser environ 1 million de dollars sur un cycle de vie de cinq ans.
En permettant de préserver l'intégralité de l'infrastructure existante et d'utiliser les applications Win32 les plus performantes, la banque de Walnut Creek (Californie) a réalisé une économie de 40% grâce à la solution client léger/serveur de Citrix. Cette solution lui a permis d'éviter l'achat de nouveaux serveurs et l'embauche d'administrateurs réseau pour chaque succursale, tout en donnant accès aux applications vitales de l'entreprise avec des PC et des anciennes bornes interactives à travers un réseau WAN.

Parce que les applications résident et s'exécutent à 100% sur le serveur, les architectures client léger/serveur offrent un moyen aux compagnies d'utiliser ces dernières à partir des postes existants. En outre, il existe une parfaite intégration entre l'ordinateur de bureau, les ressources, les applications locales et distantes de l'utilisateur, et ceci avec des performances exceptionnelles.

4.2.3 ADMINISTRATION DES SYSTEMES ET RESEAUX, SUPPORT TECHNIQUE

L'architecture client léger résout les problèmes de gestion et de support technique en permettant un contrôle des applications et des fichiers de données à partir d'un point unique. Elle inclut des outils de gestion d'entreprise qui permettent aux administrateurs de déployer, configurer, gérer et supporter les applications d'un seul endroit. L'installation de nouvelles applications ou les mises à jour des applications existantes est réalisée uniquement sur le serveur et mise instantanément à la disposition de tous les ordinateurs de bureau clients. Ainsi, la solution client léger/serveur de Citrix a permis à Hewlett-Packard de déployer un logiciel de ressources humaines vers plus de 25000 employés disséminés dans toute l'Europe. Cette solution a permis de gérer de façon centrale les applications et les données, tout en donnant à chacun des employés la possibilité d'accéder en temps réel aux données vitales afin de leur permettre de procéder à des mises à jour et des recherches d'information.

Les spécialistes du support technique peuvent prendre le contrôle à distance d'une session utilisateur (mode shadow) afin de visualiser l'écran de ce dernier et prendre le contrôle de sa souris et de son clavier. Cela simplifie considérablement le support, le diagnostic des problèmes et la formation. Selon Otto Folprecht, administrateur de réseaux pour Tree Island, société basée en Colombie britannique avec des filiales en Californie et à Washington, « une solution client léger/serveur appliquée à des terminaux Windows s'est avérée être la solution la plus simple et la plus économique pour le déploiement d'applications à travers notre entreprise. Pour moi, cette solution d'ensemble correspond à l'idée que je me fais du Zero Administration. »
Les données du GartnerGroup indiquent qu'une solution Citrix peut abaisser les coûts du support technique de 25% et les coûts d'administration d'environ 60%. Une étude réalisée par Zona Research a révélé qu'une solution client léger/serveur présentait des avantages bien plus conséquents ; en effet, les coûts d'administration et de gestion de 15 ordinateurs personnels dans un réseau Windows NT® sont approximativement 500% supérieurs aux coûts d'administration et de gestion de 15 postes Winterm fonctionnant dans une architecture client léger/serveur.

4.2.4 UTILISATEURS FINAUX ET COUTS ASSOCIES

Avec l'architecture client léger/serveur, les administrateurs et les employés du service de support basé au siège, peuvent assurer leur fonction vis à vis des filiales sans qu'il soit nécessaire de recourir à des techniciens dans chaque agence. Par exemple, Kein Smith, directeur du service de support de Pro Staff, une société possédant 130 filiales explique :
« À terme, nous réduirons de façon substantielle les coûts annuels de possession des applications, puisque leur déploiement, leur configuration et le support des utilisateurs seront assurés en central depuis les serveurs situés au siège de la société. »
Parce qu'une solution client léger/serveur maintient les applications et les données sur le serveur, les utilisateurs peuvent accéder aux informations et aux applications dont ils ont besoin en toute sécurité sans que les administrateurs s'exposent aux risques liés au téléchargement de données et d'applications. La gestion de fichiers et des applications est confiée aux professionnels. Les sauvegardes pratiquées au niveau des serveurs assurent que toutes les données vitales de la société sont archivées. En fin de compte, les coûts de l'utilisateur final sont réduits d'un tiers.

4.2.5 AUTRES ELEMENTS DE TCO

L'architecture client léger/serveur offre de nombreux autres avantages pour la maîtrise du TCO. Plutôt que d'avoir à développer de nouvelles applications orientées réseau, le modèle client léger/serveur utilise les applications Windows actuelles 16 et 32-bit. Ce modèle permet également aux administrateurs de publier des applications Windows via des pages HTML sans réécrire une seule ligne de code. Par exemple, d'après Allen Hewes, ingénieur chez Standard Forms Inc., « une solution client léger/serveur nous a permis de réduire considérablement le coût total de possession de nos applications d'entreprise puisqu'elle nous a dispensé de l'obligation de réécrire 5 Go de code. »

Les architectures client léger/serveur minimisent le trafic réseau, y compris pour les applications Win32 actuelles. Ainsi pour une entreprise, la mise à niveau structurelle d'un WAN n'est plus une nécessité. Par ailleurs, les modèles client léger/serveur constituent une solution très fiable qui permet de diminuer les coûts liés à l'indisponibilité d'un serveur, notamment grâce à la fonctionnalité de répartition de charge qui permet à un ensemble de serveurs identiques (ferme ou grappe) de simuler un mode cluster évolué.

.

Les architectures client léger/serveur réduisent le TCO des organismes qui :

- Ont besoin de préserver et d'amortir leur investissement réalisé,
- Ont besoin d'utiliser des applications Win32 dans un environnement hétérogène,
- Possèdent un parc important de PC 286/386/486,
- Ont un besoin croissant en personnel de support technique et d'administration,
- Ont besoin de déployer et de gérer des applications pour des milliers d'ordinateurs clients/serveur,
- Doivent fournir un support technique à des filiales ou agences,
- Ont besoin d'améliorer le contrôle et la sécurité dans leur environnement informatique,
- Développent ou réécrivent des applications afin de les publier via leur intranet,
- Se trouvent devant la nécessité de mettre à niveau un réseau étendu afin de bénéficier d'une bande passante à plus haut débit et de performances plus élevées.

4.2.6 CONCLUSION

Selon le GartnerGroup, l'avantage offert par les solutions client léger/serveur en matière de coût de capital, de gestion, de support et utilisateur final s'élève à 22%. D'après Zona Research, l'avantage atteint 57%. L'avantage devient encore plus important lorsqu'une organisation amortit et augmente son parc informatique et ses réseaux existants. Aujourd'hui, les solutions client léger/serveur de Citrix garantissent une réduction importante des coûts et sont en passe de devenir le moyen le plus fiable de réduire la complexité et le coût global de l'informatique d'entreprise.

5. SECURITE EN ARCHITECTURE CENTRALISEE CITRIX

Cette partie à pour but de mettre en évidence les contraintes liées à l'utilisation de la technologie Citrix sur l'application d'une politique de sécurité.

5.1 IDENTIFICATION DES FLUX D'INFORMATIONS UTILISES

L'identification des flux d'informations utilisés par Citrix MetaFrame permet de mettre en évidence les services et les échanges qu'il faut sécuriser.
On distingue deux services nécessaires au bon fonctionnement des applications s'exécutant dans l'environnement Citrix MetaFrame :

- La gestion des sessions clientes (sessions ICA).
- L'explorateur ICA (ICA Browser).

5.1.1 GESTION DES SESSIONS ICA

Lorsqu'un utilisateur souhaite accéder à une application, il clique sur une icône ou un lien hypertexte pointant vers l'application souhaitée. Un mécanisme de création de session entre le client et le serveur est alors lancé. Ce service permet d'accéder aux applications publiées par l'intermédiaire du protocole ICA correspondant au port TCP 1494 sur le serveur d'applications.

5.1.2 EXPLORATEUR ICA

Chaque serveur Citrix exécute le service Explorateur ICA. L'explorateur principal gère la liste des explorateurs et reçoit régulièrement des mises à jour des explorateurs membres.
L'explorateur principal collecte les informations suivantes :

- Les serveurs Citrix disponibles,
- Les applications disponibles,
- Les licences communes,
- Les informations relatives aux performances et à la charge des serveurs Citrix.

Les clients Citrix ICA interrogent le service Explorateur ICA pour obtenir la liste des serveurs et des applications publiées et l'adresse des serveurs et des applications publiées lors du lancement d'une session. Les clients Citrix ICA doivent donc rechercher l'explorateur principal pour obtenir l'adresse d'un serveur ou d'une application publiée.
Le service Explorateur ICA utilise le port UDP 1604 du côté client et du côté serveur.

5.2 ETABLISSEMENT DES CONNEXIONS

5.2.1 ARCHITECTURE SIMPLE

Dans une architecture simple une session ICA est établie de la manière suivante (cf. Figure):

1. Le client Citrix ICA envoie un paquet au port 1494 du serveur Citrix en demandant une connexion. Un port libre supérieur à 1023 est attribué aléatoirement du côté du client.
2. Le serveur Citrix répond en envoyant des paquets au client Citrix ICA avec le port de destination demandé à l'étape 1.

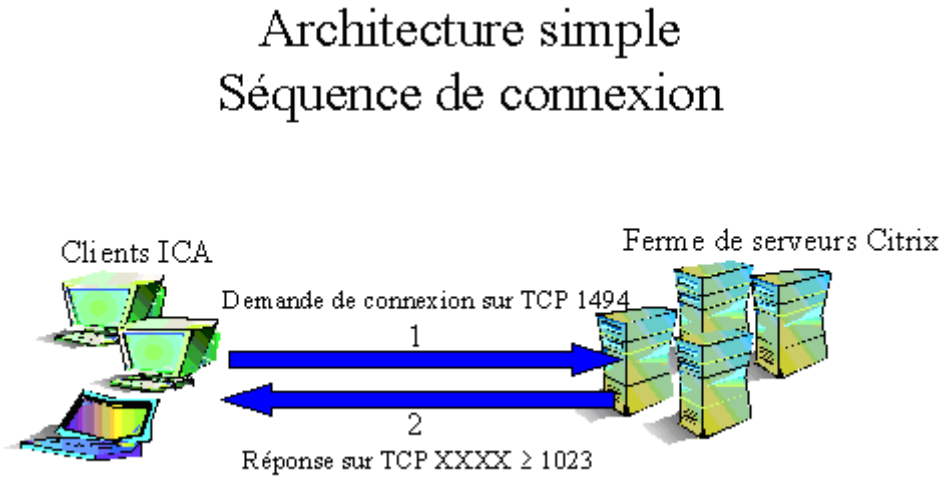


FIGURE 12 : ETABLISSEMENT D'UNE CONNEXION ICA (ARCHITECTURE SIMPLE)

En cas de demande d'une application en « Load Balancing », le mécanisme de communication « Explorateur ICA » est mis en œuvre. Voir ci-dessus.
Comme indiqué plus haut, les paramètres de connexion peuvent provenir ; soit d'un fichier ICA chargé préalablement via le navigateur, soit au travers du logiciel « Program Neighborhood ».

5.2.2 ARCHITECTURE PORTAIL

Dans une architecture portail une session ICA est établie de la manière suivante (cf. Figure 13) :

1. L'utilisateur se connecte au site web en tapant l'url dans son navigateur. Une page de login apparaît. L'utilisateur tape son login et son mot de passe.
   Une requête HTTP contenant ces informations est alors envoyée au serveur web.
2. Le serveur web reçoit les informations concernant l'utilisateur et les transmet au service Citrix XML(interface entre http (port 80) et l'explorateur ICA) du serveur d'applications Citrix.
3. Le serveur d'applications détermine quelles sont les applications auxquelles l'utilisateur a le droit d'accéder. Ces informations sont envoyées au serveur web via le service XML.
4. Le serveur web génère une page HTML contenant les liens vers les applications de l'utilisateur. Cette page est affichée dans le navigateur web de l'utilisateur.
5. Lorsque l'utilisateur clique sur l'icône d'une application, le navigateur web envoi une requête au serveur web pour retrouver l'application désignée. Cette requête est traitée par le serveur web qui renvoie les paramètres de l'application au navigateur web de l'utilisateur sous la forme d'un fichier ICA paramétré dynamiquement.
6. Le navigateur web reçoit ces paramètres et les transmet au client ICA installé sur la poste de l'utilisateur.
7. Le client ICA reçoit les paramètres de l'application et les utilise pour établir une session ICA avec le serveur d'applications.

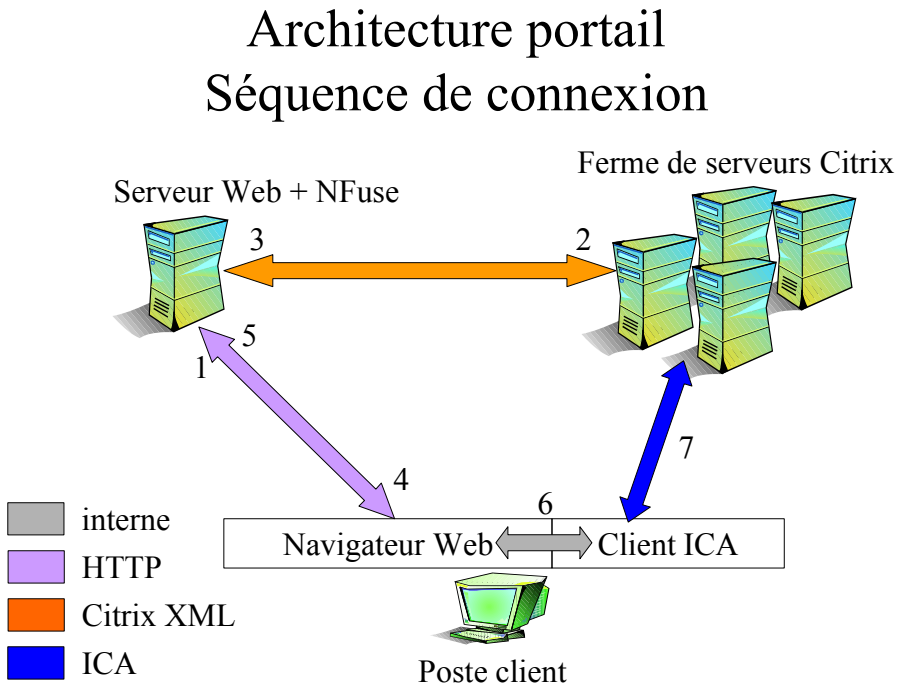


Figure 13 : Etablissement d'une connexion dans le cas d'une architecture portail

5.3 CONTRAINTES SUR L'APPLICATION D'UNE POLITIQUE DE SECURITE

L'utilisation d'une architecture centralisée Citrix permet de réduire les flux liés à l'utilisation des différentes applications client/serveur classique en un seul type de flux grâce à l'utilisation du protocole ICA. Il est difficile de décoder un flux ICA en sniffant le réseau puisque seules les mises à jour sont envoyées sur le réseau.
Toutefois, des contraintes sur l'application de la politique de sécurité de l'entreprise sont introduites par l'utilisation de la technologie Citrix sur le réseau.

5.3.1 TRAVERSEE D'UN PARE-FEU

Un pare-feu permet de laisser passer ou de bloquer les paquets de données en fonction de l'adresse et du port de destination. Pour utiliser ICA via un pare-feu sur le réseau, il faut configurer correctement le pare-feu afin de permettre l'accès aux services suivants : **gestion des sessions ICA** et **explorateur ICA**.

5.3.1.1 GESTION DES SESSIONS ICA

Le pare-feu doit être configuré pour permettre aux paquets TCP/IP du port 1494 d'être transmis aux serveurs Citrix sur le réseau. Il faut aussi permettre aux paquets TCP/IP des ports supérieurs à 1023 d'être transmis aux clients Citrix ICA. Cf. **Figure** .
Si le pare-feu n'est pas défini pour transmettre les paquets ICA, les utilisateurs reçoivent le message d'erreur « There is no route to the specified address » (aucune route vers l'adresse indiquée).

5.3.1.2 EXPLORATEUR ICA

De même, le pare-feu doit être configuré pour autoriser les connexions entrantes et sortantes UDP du port 1604 aux serveurs Citrix pour permettre l'accès à l'équilibrage de charge, aux batteries de serveurs et à l'exploration des serveurs ICA de fonctionner correctement (cf. **Figure**). Si ce port n'est pas autorisé au niveau du pare-feu, ces services ne pourront pas fonctionner. L'exploration des serveurs utilisée pour récupérer la liste des applications publiées ne pourra pas être effectuée car le client ne peut pas interroger l'explorateur principal. La répartition de charge ne fonctionnera pas, ainsi si un serveur tombe en panne il faut prévoir un serveur de secours sur lequel l'utilisateur peut se connecter pour continuer à travailler.

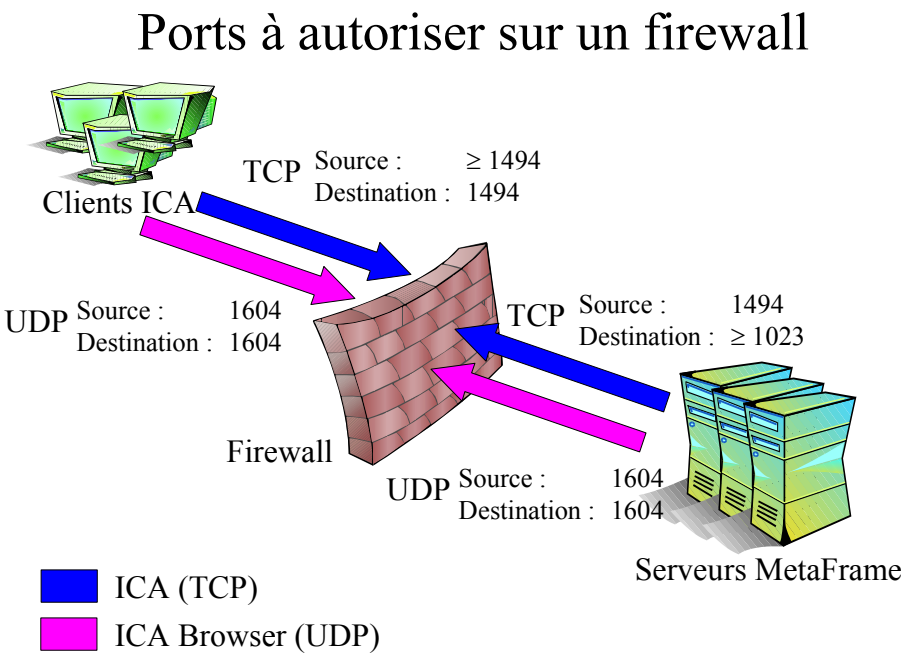


FIGURE 12 : PORTS A AUTORISER SUR UN FIREWALL

Attention : l'autorisation des accès non accrédités au service d'explorateur comporte quelques risques au niveau de la sécurité. On ne permettra la transmission des données Explorateur ICA au travers d'un pare-feu uniquement si l'équilibrage de charge et l'exploration des serveurs via le pare-feu sont essentiels.
Dans le cas d'une architecture portail, il faudra aussi veiller à autoriser le service web (port 80) sur les équipements de filtrage se trouvant entre le client et le serveur web NFuse. De même, si des équipements de filtrage sont présents entre le serveur web NFuse et la ferme de serveurs d'applications, il faut autoriser le port correspondant au service Citrix XML (le plus souvent le port 80 est utilisé mais il peut être différent).

5.3.2 TRANSLATION D'ADRESSES

Les équipements réseaux et de sécurité peuvent utiliser la translation d'adresses IP pour convertir les adresses IP privées en adresses IP publiques. Les adresses publiques permettent de contacter une machine depuis l'extérieur tandis que son adresse IP privée permet de le contacter de l'intérieur.
Cette translation d'adresse est supportée par les logiciels clients ICA et serveur. Il faut indiquer, au niveau des serveurs d'applications, l'adresse publique de chacun des serveurs (en utilisant la commande « altaddr /set @IP »).

5.4 ETAT DE L'ART DES SOLUTIONS DE SECURITE

Pour les besoins d'une entreprise, des applications doivent être mises à disposition des employés nomades, des clients et des partenaires. Une infrastructure réseau commune entre l'entreprise et ses clients, partenaires et fournisseurs ou l'utilisation de l'Internet (par exemple pour les nomades) permet d'accéder aux ressources de l'entreprise. Toutefois, on doit assurer l'authentification des tiers, la confidentialité et l'intégrité des informations échangées. Pour cela il faut mettre en place des solutions d'authentification, de filtrage et de sécurisation des échanges.

Les solutions de sécurité en authentification forte, firewall (techniques de filtrage) et de sécurisation des échanges applicables en environnement Citrix sont présentées par la suite.

Dans cet état de l'art, les solutions techniques (protocole, service) sont tout d'abord présentées puis les principaux produits, utilisables en architecture centralisée Citrix et permettant la mise en œuvre de la solution technique préalablement présentée, sont identifiés.

5.4.1 CRITERES COMMUNS

Pour la sélection des produits et des solutions , les critères suivants communs à toutes les solutions ont été pris en compte:

- Disponibilité en France.
- Compatibilité avec l'environnement Citrix et aussi avec l'environnement client léger si des terminaux sont mis en place.
- Eviter au maximum d'intervenir sur les plates-formes des utilisateurs (impossible dans le cas de l'utilisation de terminaux). Dans le cas de partenaires, il n'est pas possible d'intervenir sur leurs postes.
- Interopérabilité entre les équipements de sécurité existant et nouveaux. Les standards existant (IETF) ou les alliances entre constructeurs sont utilisés comme référence :
  - ➔ Les standards sont définis par l'IETF (Internet Engineering Task Force), l'organisme de normalisation de l'Internet.
  - ➔ L'alliance OPSEC est une initiative de l'éditeur CheckPoint Software, un des principaux acteurs dans le domaine filtrage et de la sécurisation des échanges avec son produit far Firewall-1/VPN-1. Cette alliance a pour but d'assurer l'interopérabilité de l'ensemble des solutions de sécurité membres.
- Haute disponibilité afin d'assurer un service fiable d'accès aux applications et aux données.
- Niveau de sécurité offert.
- Performances.
- Solution globale adaptée au maximum à l'ensemble des besoins de l'entreprise dans le domaine considéré.
- Administration centralisée.
- Administration à distance.
- Coût.

5.4.2 AUTHENTIFICATION

L'authentification permet d'assurer l'identité d'une personne ou d'un serveur.

5.4.2.1 AUTHENTIFICATION FORTE

L'authentification forte encore appelée authentification à deux facteurs est basée sur quelque chose que l'on possède et sur quelque chose que l'on connaît. Un exemple est l'accès à un compte bancaire. Lorsque que l'on souhaite retirer de l'argent à un distributeur on utilise sa carte à puce associée à un numéro à quatre chiffres (code PIN). Ce mécanisme correspond à une authentification forte de l'utilisateur de la carte puisqu'il faut à la fois posséder la carte et aussi connaître le code PIN pour effectuer un retrait.

L'authentification forte combine donc l'utilisation d'un authentificateur (token en anglais) et d'un code secret. Un authentifieur est généralement un objet physique toutefois certains éditeurs utilisent des authentifieurs logiciels.

Pour assurer un niveau de sécurité élevé en ce qui concerne l'authentification, on peut décider de choisir une solution d'authentification forte plutôt qu'une simple authentification par mot de passe.
En effet, une solution de mot de passe statique comporte quelques risques car le couple login / mot de passe peut être découvert. De petits logiciels à la portée de tous et faciles à se procurer par l'intermédiaire du web, permettent de découvrir en quelques minutes les mots de passe les plus simples d'un système. En quelques heures des mots de passe plus complexes seront aussi découverts. Ces outils sont basés sur l'utilisation d'un dictionnaire.

Pour l'accès à des ressources sensibles réseau, on utilisera donc une solution d'authentification forte. Toutefois, dans un environnement local avec peu de risques, une solution d'authentification classique par login/mot de passe suffit si l'on veille à modifier son mot de passe régulièrement et que celui-ci n'est pas facile à deviner.

5.4.2.2 PROTOCOLE D'AUTHENTIFICATION

Dans une organisation où des personnes travaillent à distance, il est nécessaire de protéger les réseaux et les services des accès non autorisés des utilisateurs distants. L'authentification des utilisateurs est souvent réalisée par un service spécifique appelé AAA pour Authentication, Authorization et Accounting (authentification, contrôle d'accès et suivi d'activités). Ce service d'authentification est généralement mis en place au travers l'utilisation d'un protocole spécifique.
Les principaux protocoles d'authentification sont les suivants :

- RADIUS
- TACACS
- TACACS+
- XTACACS
- Kerberos

Les protocoles de la famille TACACS sont assez répandus et utilisent le protocole TCP contrairement à RADIUS qui s'appuie sur UDP. Toutefois, ne ce sont pas des standards définis par un organisme de standardisation comme l'IETF. Seuls RADIUS et Kerberos sont des standards.
Kerberos est mis en place dans l'authentification Windows 2000 au sein d'Active Directory (annuaire Microsoft). Ce protocole permet l'authentification des entités communicantes (clients et serveurs) et des utilisateurs. Dans le cas où le service Citrix d'accès aux applications est mis en place uniquement pour les membres d'un domaine Windows 2000, cette solution est la plus simple à mettre en place.
Pour des accès distants soit par modem en appelant un serveur d'accès, soit par l'Internet (via la solution portail de Citrix : NFuse), l'authentification Kerberos est difficile à mettre en place si on n'est pas dans le même domaine Windows (ou dans un sous-domaine de ce domaine), elle est complexe à déployer car des éléments doivent être mis en place du côté utilisateur et l'interopérabilité n'est pas évidente entre deux systèmes d'authentification différents basés sur Kerberos.
Pour ces raisons, RADIUS est le plus approprié pour un accès distant aux applications utilisant Citrix. Le protocole RADIUS est décrit ci-dessous. Pour obtenir des informations sur les autres protocoles, il est possible de consulter les RFC disponibles sur le site web de l'IETF (www.ietf.org).

5.4.2.2.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) est un protocole de transport des informations d'authentification développé par Livingston Enterprises. C'est un standard normalisé par l'IETF, il est défini dans les RFC 2138 et RFC 2139 : (la RFC 2138 traite de l'aspect authentification de RADIUS et la RFC 2139 traite l'aspect accounting (suivi des activités).
Contrairement aux autres protocoles d'authentification comme TACACS et ses successeurs(TACACS+, XTACACS), RADIUS est un standard. RADIUS est gratuit, son code est public et c'est un protocole ouvert (il est possible de lui rajouter des fonctionnalités supplémentaires). Il supporte de nombreux mécanismes d'authentification. Les échanges entre client et serveur sont chiffrés. Ce protocole est interopérable avec d'autres protocoles d'authentification comme TACACS, TACACS+ et XTACACS. De nombreuses solutions commerciales d'authentification offrent la compatibilité RADIUS.

5.4.2.2.2 PRINCIPE DE FONCTIONNEMENT

RADIUS est basé sur un modèle client/serveur, l'authentification est réalisée de manière centralisée. RADIUS utilise le protocole UDP. Les numéros de ports qui lui sont attribués sont le port UDP 1645 pour l'authentification et le port 1646 pour le suivi des activités. La fiabilité du transport des informations est réalisée par RADIUS et non par le protocole de transport car RADIUS s'appuie sur UDP. Le serveur RADIUS tourne habituellement sur une machine UNIX ou Windows NT.

Un serveur RADIUS permet d'authentifier un utilisateur grâce à son nom d'utilisateur et son mot de passe interne ou il peut jouer le rôle de client (via un proxy RADIUS) pour l'authentification des utilisateurs basée sur un système d'authentification différent (comme Unix, NT, Netware, etc). Un serveur RADIUS peut jouer le rôle de client pour un autre serveur RADIUS. Ce mécanisme est particulièrement utile lorsqu'une entreprise veut externaliser la gestion de l'accès distant tout en gardant le contrôle sur sa sécurité. Le protocole RADIUS offre beaucoup de possibilités, le succès ou l'échec d'une tentative d'authentification peut dépendre du serveur d'accès depuis lequel la requête a été envoyée, l'heure, le jour ou l'adresse IP de l'utilisateur. Il est aussi possible de définir des restrictions pour les transactions qu'un utilisateur peu effectuer. Des implémentations peuvent ajouter des fonctionnalités supplémentaires à celle de base (RADIUS est un protocole ouvert).

Un utilisateur qui souhaite établir une connexion contacte le serveur d'accès distant (remote access server – RAS ou network access server - NAS) qui est en fait un client RADIUS. L'utilisateur envoie son nom d'utilisateur et son mot de passe au serveur d'accès (requête de type access-request), qui transmet les informations au serveur RADIUS pour l'authentification. Le serveur RADIUS vérifie les informations d'authentification et renvoie le paquet adéquat :
- un access-accept : l'autorisation est acceptée, des informations supplémentaires comme l'adresse IP ou le masque de réseau sont envoyées.
- access-reject : le nom d'utilisateur et le mot de passe sont erronés.
- access-challenge : dans le cas de l'utilisation d'un mécanisme de mot de passe à usage unique (One Time Passsword – OTP) avec challenge.
Dans le cas de l'utilisation d'un mécanisme d'authentification à mot de passe dynamique (mot de passe à usage unique), le serveur envoi un challenge (numéro) à l'utilisateur. L'utilisateur génère un nouveau mot de passe en utilisant son authentifieur. L'utilisateur envoie ensuite un access-request contenant le mot de passe généré. Le serveur vérifie les informations reçues et renvoi un paquet adéquat (access-accept ou access-reject).
Les clients autorisés à émettre une requête vers le serveur sont identifiés par leur adresse IP et une clef partagée (secret). Le mot de passe est chiffré en utilisant l'algorithme suivant : MD5(secret) XOR password (où MD5 est un algorithme de hachage).
Un certain nombre de fonctions de suivi d'activité sont définies dans la norme (accounting-request / accounting-response).

5.4.2.2.3 METHODES D'AUTHENTIFICATION ET AUTHENTIFIEURS

Après avoir sélectionné le protocole d'authentification, il faut déterminer la manière dont on va s'authentifier.
Plusieurs méthodes d'authentification sont possibles, certaines nécessitent le déploiement, pour chaque utilisateur, d'un objet appelé authentifieur fournissant des informations nécessaires à la procédure d'authentification. Les méthodes présentées sont les plus courantes, elles ne sont pas supportées par toutes les solutions du marché.

5.4.2.2.3.1 MOT DE PASSE STATIQUE

L'authentification par mot de passe statique est très répandue. C'est la solution la plus souvent utilisée pour accéder à un système. La procédure d'authentification débute par une procédure de login durant laquelle on fournit son login et son mot de passe (chaîne de caractères secrètes). Le système récupère ces informations et regarde dans sa base de comptes des utilisateurs si la personne est bien enregistrée et si le mot de passe qui a été tapé est correct. Si le couple login/mot de passe est correct, l'authentification est réussie et l'accès au système est permis.
Pour un hacker expérimenté ou un utilisateur « initié » il est techniquement facile de découvrir le mot de passe d'un utilisateur. En effet, en utilisant des outils disponibles sur l'Internet il est assez aisé de découvrir les mots de passe d'ouverture d'une session Windows NT ou Unix. De tels outils sont basés sur l'utilisation d'un dictionnaire répertoriant les mots de passe les plus utilisés. Plus le mot de passe est simple, plus il sera facile et rapide de le découvrir. Pour les mots de passe plus complexes, il faudra un peu plus de temps mais sa découverte reste toujours possible pour des durées inférieures à une journée dans des configurations classiques c'est à dire sans mécanisme de sécurité spécifique. De plus, la principale faiblesse de cette méthode est qu'en sniffant le réseau on peut rejouer la séquence d'authentification. Il faut donc chiffrer les échanges et le fichier dans lequel sont stockés les mots de passe sur le serveur.

5.4.2.2.3.2 MOT DE PASSE A USAGE UNIQUE (OU ONE TIME PASSWORD – OTP)

A chaque demande de connexion l'utilisateur fournit un mot de passe différent générer soit par une petite calculette affichant un nouveau mot de passe périodiquement ou à chaque fois que l'on a à se connecter en pressant une touche. Ce mécanisme est souvent associé à l'utilisation d'un code PIN que seul l'utilisateur connaît.
Le principe est simple : un même algorithme tourne de manière indépendante sur le serveur et sur la calculette. Lorsque la calculette fournie un nouveau mot de passe à usage unique le serveur, de son côté, connaît le mot de passe sans pour autant qu'il y ait une communication entre les deux entités. Il n'est pas utile de chiffrer ce mot de passe puisqu'il n'est pas rejouable.

5.4.2.2.3.3 CARTE A PUCE

Le plus souvent, la carte à puce est utilisée dans le cadre d'une infrastructure à clé publique. Mais elle peut aussi servir d'authentifieur en fournissant le mot de passe à usage unique. La puce générant un mot de passe périodiquement.

5.4.2.2.3.4 CLE USB

Le principe est le même que celui d'une carte à puce. On peut à la fois l'utiliser dans le cadre d'une infrastructure à clé publique mais aussi comme authentifieur fournissant un mot de passe dynamique (OTP).
Pour utiliser une clé USB, il suffit de posséder un port USB disponible sur tous les postes datant de moins de trois ans. L'inventeur de la clé d'authentification USB est Rainbow Technologies avec ses produits iKey1000 et iKey2000 (version PKI).

5.4.2.2.3.5 LA BIOMETRIE

La biométrie est basée sur l'utilisation des caractéristiques physiques des personnes.
Un éditeur français : ZalixBiométrie (www.zalix.fr) propose des solutions s'intégrant dans les environnements Windows et notamment à Active Directory.
Le marché de la biométrie est en pleine expansion et les prix deviennent abordables.

5.4.2.2.4 CHOIX D'UNE METHODE D'AUTHENTIFICATION

La technologie Citrix permet d'utiliser des terminaux Windows appelés terminaux client-léger sur lesquels il n'est pas possible d'installer un logiciel spécifique pour gérer l'utilisation de l'authentifieur. Un lecteur de cartes à puce, une clé USB ou les systèmes basés sur la biométrie nécessitent l'installation d'un logiciel spécifique pour la gestion de ces périphériques. Leur utilisation n'est possible que si l'on n'utilise pas de terminaux client-léger ou ci ces derniers prennent en considération, dans le futur, ces solutions.
Pour toutes les raisons qui viennent d'être énoncés, la méthode d'authentification forte préconisée est celle du mot de passe à usage unique (OTP) s'appuyant sur un authentificateur souvent sous forme de calculette.

5.4.2.3 SOLUTIONS

Dans le cas d'une utilisation de Citrix au sein d'un domaine Windows 2000, Kerberos peut être mise en place au travers d'Active Directory. Kerberos fournit un bon niveau de sécurité pour l'authentification (Kerberos authentifie à la fois les utilisateurs et les services en utilisant un algorithme de chiffrement asymétrique). Dans le cas où les applications sont rendues accessibles par Citrix en utilisant un accès distant, RADIUS est à privilégier comme protocole d'authentification.
Il existe de nombreuses solutions implémentant le protocole RADIUS dont certaines sont libres. RADIUS nécessite l'installation d'un client auquel s'adresse le serveur MetaFrame pour authentifier l'utilisateur. Ce client est installé sur le serveur MetaFrame pour en permettre l'accès authentifié en utilisant RADIUS. Toutefois, le produit Citrix MetaFrame est en majorité présent dans l'environnement Windows bien qu'il existe un produit Citrix MetaFrame pour l'environnement Unix. Les solutions libres ne sont pas adaptées à l'environnement Citrix sous Windows, elles sont plutôt destinées aux environnements Unix. Les solutions commerciales sont donc à envisager.

Voici les quatre principales solutions d'authentification du marché, toutes compatibles RADIUS:

- RSA SecurID de RSA Security (leader mondial)
- SafeWord de SecureComputing (très présent aux Etats-Unis)
- ActivCard
- SafeData de SafeData Systems (racheté récemment par ActivCard)

Les solutions RSA SecurID et SafeWord s'avèrent bien adaptées à l'environnement Citrix. La solution SafeWord propose même un agent spécifique à l'environnement Citrix. L'intégration de RSA SecurID en environnement Citrix est documentée dans l'aide du produit MetaFrame.

Voici une étude détaillée de ces deux solutions :

5.4.2.3.1 RSA SECUREID

RSA SecurID, solution d'authentification forte de RSA Security, repose sur le principe de mot de passe à usage unique. Afin d'être autorisés à se connecter, les utilisateurs doivent s'authentifier en utilisant conjointement deux facteurs d'authentification totalement distincts :
Quelque chose que seul l'utilisateur connaît : le code secret (PIN).
Quelque chose d'unique que seul l'utilisateur possède : l'authentifieur RSA SecurID.
L'authentifieur génère un code unique toutes les 30 à 60 secondes, non usurpable, non rejouable.
L'authentification est réalisée en une seule étape : l'utilisateur saisit son login et recopie la suite de chiffres affichée sur son authentifieur suivie de son code secret dans la partie « password ».
La solution d'authentification forte RSA SecurID est composée d'un ou plusieurs serveurs d'authentification RSA ACE/Server et d'agents RSA ACE/Agent qui envoient les requêtes au(x) serveur(s) d'authentification.
Les serveurs d'authentification RSA ACE/Server contiennent les informations d'authentification pour chaque utilisateur. C'est une base de données à partir de laquelle on donne ou non l'autorisation de connexion à un utilisateur. Le code secret associé au code d'authentification forme un « passcode » transmis au serveur d'authentification.
Le serveur ACE/Server peut être installé sur une plate-forme Windows NT ou Unix (Sun, HP ou IBM). Un unique ACE/Server peut gérer 100 000 utilisateurs.
Un mécanisme de Master/Backup (Principal/Secours) permet d'assurer une haute disponibilité. Lorsque le serveur principal est hors d'usage, le serveur de secours prend le relais automatiquement.

Quand le serveur principal est réparé, il reprend alors la main. La communication entre le serveur principal et celui de secours s'appuie sur le protocole TCP, les échanges entre ces deux entités sont chiffrés et la clé est modifiée toutes les 10 minutes. Un mécanisme de répartition de charge peut être mis en place entre les serveurs par réplication des serveurs ACE/Server.
L'ACE/Server permet d'authentifier à la fois les utilisateurs locaux et les utilisateurs distants. L'authentification des utilisateurs qui souhaitent accéder aux ressources du réseau est réalisée par l'intermédiaire d'agents installés sur les ressources du réseau. Les paquets sont chiffrés, lors de la première connexion entre l'agent et le serveur, un secret est échangé.
Les agents d'authentification RSA ACE/Agent sont chargés de la transmission du passcode entre la plate-forme de l'utilisateur et le serveur d'authentification. Cet agent déclenche la demande d'authentification dès qu'un utilisateur demande l'accès à une ressource protégée. Un agent permet de sécuriser les accès aux ressources : RAS/NAS (accès distant), firewall, serveurs web (Microsoft IIS, Lotus Domino, IPlanet), systèmes d'exploitation (Windows NT, Solaris, IBM AIX, HP-UX, RedHat Linux),et messagerie.
RSA SecurID se décline selon une vaste gamme de formes possibles répondant à des besoins différents. Un authentifieur fourni un nouveau code toutes les 30 à 60 secondes. Voici les différentes formes d'authentifieurs :

- Porte-clés : fourni un nouveau code périodiquement.
- Calculette : avec ou sans pin pour obtenir un nouveau code d'authentification..
- Carte à puce.
- Logiciel : pour PC ou pour PalmPilot.

Les serveurs d'authentification sont synchronisés de manière temporelle avec les authentifieurs qui fournissent un nouveau code périodiquement. Il arrive qu'un authentifieur soit désynchronisé avec le serveur, il faut alors le resynchroniser à la main (voir www.rsasecurity.com pour plus de détails).

5.4.2.3.2 SAFEWORD

Le principe de fonctionnement de la solution d'authentification SafeWord de SecureComputing est proche de celui de RSA SecurID.
Les principales caractéristiques de ce produit sont :

- serveur AAA : authentification, contrôle d'accès et suivi d'activités,
- mot de passe dynamique à usage unique (OTP),
- support de nombreux périphériques d'authentification,
- performances élevées – jusqu'à 150 authentifications par seconde,
- réplication et répartition de charge entre serveurs d'authentification (jusqu'à 4 serveurs),
- administration centralisée à partir d'une seule console d'administration.
- gestion des déplacements au sein d'un réseau (un utilisateur qui est habituellement authentifié sur un lieu A par un service d'authentification, se déplace sur un lieu B ou un autre service d'authentification est présent, le service d'authentification B interroge le service A pour authentifier l'utilisateur mobile et met à jour sa table pour gérer l'utilisateur en B).

Les authentifieurs disponibles sont :

- Calculette : avec ou sans code PIN pour obtenir un nouveau code d'authentification.
- Logiciel pour PC, PalmPilot.
- Cartes à puce et clé USB uniquement pour le produit SafeWord Plus (permet d'utiliser une infrastructure à clé publique).
- Biométrie.
- Mot de passe classique.

La génération des mots de passe dynamique n'est pas basée sur le temps mais sur un numéro d'ordre. Par rapport au numéro d'ordre, un mot de passe dynamique est possible. Lors d'une désynchronisation entre le serveur et l'authentifieur, la première connexion est refusée toutefois le serveur essaye de retrouver le numéro d'ordre par rapport à mot de passe dynamique qu'il a reçu. Lors de la seconde authentification, si le mot de passe correspond bien au numéro d'ordre alors l'authentification réussie. Il n'est donc pas nécessaire de resynchroniser le serveur avec l'authentifieur en passant par l'administrateur.
Un agent spécifique à Citrix MetaFrame permet d'intégrer cette solution d'authentification dans cet environnement. Pour cela, les serveurs d'applications doivent faire partie d'un domaine Windows. Sur chaque serveur Citrix, on doit installer cet agent.
SafeWord est une solution d'authentification bien adaptée à l'environnement Citrix car elle est simple à installer, à administrer et à utiliser. De plus, elle ne nécessite aucune modification sur le poste de travail de l'utilisateur répondant bien à la problématique du poste client-léger.
Pour plus de détails, il est possible de se référer au site web de l'éditeur : www.securecomputing.com.

5.4.2.3.3 CHOIX D'UNE SOLUTION

Les principales différences entre SafeWord et RSA SecurID sont :

- la notion de serveur principal/secours pour les serveurs d'authentification qui est présente dans la solution de RSA Security alors que celle de SecureComputing n'établie pas cette hiérarchie.
- la génération des mots de passe à usage unique est basée sur le temps pour RSA SecurID (un toutes les 60 secondes) tandis qu'elle est basée sur un numéro d'ordre pour SafeWord (à chaque nouvelle authentification on récupère le mot de passe à usage unique en appuyant sur une touche).

La solution SafeWord possède un agent spécifique à l'environnement Citrix contrairement à RSA SecurID qui utilise un agent classique.

Globalement, RSA SecurID est un produit plus complexe à mettre en œuvre et à utiliser que SafeWord. Ce dernier est plus convivial. RSA Security est mieux implantée en France et son produit est distribué en plus grand nombre alors que SecureComputing, qui a monté une antenne française il y a un an, a son réseau de distributeur encore peu développé en France.

5.4.2.4 SELECTION D'UNE SOLUTION COMPLETE D'AUTHENTIFICATION

Pour les raisons qui viennent d'être énoncés, la solution complète d'authentification que nous préconisée est le produit SafeWord de SecureComputing en utilisant RADIUS comme protocole d'authentificaton et la méthode d'authentification de mot passe à usage unique utilisant une calculette distribuée à chaque utilisateur du système.
L'utilisation d'une infrastructure est rare de nos jours, peu d'entreprises en déploient une car de telles solutions sont lourdes et complexes à déployer et à gérer, et en plus elles sont très chères. Elles ne sont utilisées que dans des environnements nécessitant un niveau de sécurité très élevé avec un nombre de postes important.

5.4.3 FILTRAGE

Un des principes de base de la sécurité des réseaux est le cloisonnement des réseaux. Il permet de limiter les échanges entre deux réseaux au strict nécessaire en n'autorisant que certains flux. Le cloisonnement des réseaux est basé sur le découpage du réseau en zones de sécurité. Les mécanismes de filtrage sont mis en place sur des équipements dédiés, des routeurs ou des serveurs.

5.4.3.1 FIREWALL

Le terme firewall (pare-feu en français) est souvent utilisé pour définir un équipement qui implémente un mécanisme de filtrage réseau.
Un firewall peut être défini comme un ensemble de composants mis en œuvre entre deux réseaux, et contribuant à fournir les propriétés suivantes :

- Tout trafic de l'intérieur vers l'extérieur ou de l'extérieur vers l'intérieur doit impérativement passer par le firewall.
- Seuls les flux autorisés conformément à la politique de sécurité peuvent franchir le firewall.
- Le firewall doit être lui-même inaccessible afin d'être insensible aux attaques.

A ces trois propriétés s'ajoute une fonctionnalité importante, qui contribue notamment à différencier les firewalls de simples routeurs sur lesquels on met en place des filtres : la génération de traces relatives à toute tentative de violation de la politique de sécurité, mais aussi aux communications autorisées.

5.4.3.2 DEFINITIONS

5.4.3.2.1 BASTION

On appelle bastion une machine exposée aux attaques en provenance de l'Internet ; elle bénéficie en général d'une configuration renforcée sur le plan de la sécurité (limitation des comptes et des services disponibles) lui permettant d'être immunisée contre les attaques qui peuvent être lancées contre lui.

5.4.3.2.2 ZONE DEMILITARISEE (DMZ)

Une DMZ est un réseau isolé du réseau protégé par le firewall. Il supporte les machines vers lesquelles les utilisateurs d'Internet ont le droit d'établir des connexions (serveurs SMTP, HTTP, FTP, etc.). L'accès à une DMZ depuis l'extérieur est contrôlé par le firewall, mais avec un politique de sécurité moins stricte que pour le réseau interne.

5.4.3.3 TERMINOLOGIE DES MECANISMES DE FILTRAGE

En général, chaque produit du marché utilise une dénomination propre pour définir son mode de fonctionnement. Toutefois, on distingue plusieurs classes. Un produit peut implémenter plusieurs de ces méthodes. Pour un flux donné, une seule méthode sera appliquée.

5.4.3.3.1 CONTROLE AU NIVEAU DES COUCHES RESEAU ET TRANSPORT

5.4.3.3.1.1 FILTRAGE DE PAQUETS (PACKET FILTERING)

Chaque trame subit une comparaison de certains de ses champs (adresses source et destination, numéros de ports source et destination, options protocolaires) avec les paramètres des filtres qui sont définis. Ce mécanisme est très performant et généralement matériel (sur les routeurs).
La notion de session n'est pas gérée.
Le filtrage d'éléments de niveau applicatif ne peut être réalisé que par comparaison de séquences de bits à des emplacements fixes dans les trames.

Ce filtrage de bas niveau ne permet pas d'avoir beaucoup de recul sur les flux notamment en ce qui concerne la fragmentation IP. De plus ce type de firewall ne dispose pas de mécanisme d'authentification.
Un exemple d'utilisation de ce mécanisme est les ACL (Access Control List) dans les routeurs Cisco.

5.4.3.3.1.2 RELAYAGE DE CIRCUIT (CIRCUIT LEVEL GATEWAY)

Ce mécanisme gère la notion de session. Lorsqu'une connexion peut être établie conformément à la politique de sécurité, un contexte est créé en mémoire. Il sera détruit à la fin de la connexion. Tous les paquets d'un même flux sont rattachés au contexte correspondant et sont transmis directement au lieu d'appliquer les règles de filtrage à chaque paquet comme précédemment.
La notion de contexte permet une plus grande précision dans la gestion des flux, par exemple, il est possible de conditionner l'établissement d'une connexion FTP à l'existence d'un contexte pour la connexion de contrôle associée.
Pour les services basés sur UDP, qui fonctionnent en mode non connecté, la notion de session est gérée au moyen d'un compteur de temps.

5.4.3.3.2 CONTROLE AU NIVEAU APPLICATIF

5.4.3.3.2.1 RELAYAGE APPLICATIF (APPLICATION LEVEL GATEWAY)

Chaque service réseau est géré par un programme spécifique (proxy). Ce programme sait en analyser le flux applicatif et permet donc une plus grande finesse dans le contrôle offert, tant sur le plan du filtrage que de la traçabilité. Ce mécanisme est uniquement logiciel et ses performances sont médiocre. Le niveau de sécurité offert, pour une application donne, est élevé
La mise en œuvre du relayage applicatif conduit à masquer les adresses des machines clientes aux serveurs et inversement. En effet, il y a deux connexions, la première initiée par le client vers le proxy et la seconde initiée par le proxy vers la machine destinataire (serveur). Lorsque l'on se connecte à un service on se connecte sur le proxy qui relaye la connexion au serveur cible. La machine cible est masquée.
Un programme de relayage générique (exemple : proxy SOCKS décrit plus loin) peut être utilisé pour les services ne disposant pas d'un programme spécifique (on ne bénéficie alors d'aucune fonction d'analyse du contenu du flux).

5.4.3.3.2.2 FILTRAGE ADAPTATIF (STATEFUL INSPECTION)

Ce mécanisme est le plus récent. Bien qu'agissant au niveau des trames, un contrôle des informations de niveau applicatif est réalisé. La finesse de contrôle est en général moindre que celle qui peut être obtenue grâce à un relais applicatif. Le niveau de performance est potentiellement plus élevé du fait que le traitement est effectué sans que les données aient eu à remonter jusqu'au niveau des couches applicatives contrairement aux proxy.
Ce mécanisme est un bon compromis entre le filtrage de paquet et le relais applicatif en terme de niveau de sécurité offert et de performances. Des solutions matérielles commencent à apparaître sur le marché et offrent des logiciels qui implémentent ce mécanisme.

5.4.3.3.2.3 CONTROLE DE CONTENU

Un degré très avancé de contrôle de l'utilisation des applications est atteint par certains produits mettant en œuvre les deux modes de contrôle précédents.
Certains sont capables :

- De filtrer les commandes GET ou PUT du protocole FTP ou HTTP
- De remplacer les informations relatives aux machines du réseau privé dans l'en-tête des messages électroniques
- D'inhiber sélectivement les scripts ActiveX et javascript, ou les applets Java dans les flux HTTP.

On peut contrôler les objets transmis au travers du mécanisme de filtrage comme :
Un contrôle antivirus appliqué aux messages et aux fichiers entrants et sortants.
Une vérification de la nature du contenu des informations entrante et sortante (sujet, mots-clés, images à caractère pornographique, ...).

5.4.3.4 STATEFUL INSPECTION PAR L'EXEMPLE DE FIREWALL-1 DE CHECKPOINT

FireWall-1 (FW-1) de CheckPoint est un des acteurs principaux de la sécurité réseaux pour les équipements filtrages.
Le produit est composé de trois fonctionnalités :

- le filtrage par table d'états : technologie Stateful Inspection
- la translation d'adresses (dynamique et statique)
- la mise en place de VPN

Dans la suite de cette description, nous nous intéresserons aux mécanismes mis en place dans la version 4.1 de FW-1.

5.4.3.4.1 LA BASE DE REGLES

La base de règles de FW-1 permet de filtrer les paquets en fonctions des éléments suivant : l'adresse IP source, l'adresse IP destination et les services source et destination (numéro de port). Pour chaque règle on associe une action dont les principales sont :
Accept : le paquet est accepté.
Drop : le paquet est jeté.
Reject : la connexion est rejetée
Log : une information concernant l'application de la règle correspondante est écrite dans un fichier.
Alert : une alerte est envoyée.

5.4.3.4.2 FONCTIONNEMENT

Lorsque le firewall reçoit un paquet SYN initiant une connexion TCP, ce paquet SYN est confronté à la base de règles du firewall. Ce paquet SYN est comparé aux règles de façon séquentielle, si le paquet passe toutes les règles sans être accepté , le paquet est refusé. La connexion est alors droppée ou rejetée (un RST est envoyée à la machine distante). Toutefois, si le paquet est accepté, la session est enregistrée dans la table de connexion du firewall. Chaque paquet suivant, s'il n'a pas le bit SYN positionné, est comparé à la table d'état (stateful inspection). Si la session est dans la table, et que le paquet appartient à cette session, alors le paquet est accepté. Si le paquet n'appartient pas à la session, alors il est jeté. Ce principe permet d'améliorer les performances car tous les paquets ne sont pas comparés à la base de règle, seuls les paquets SYN initiant une connexion sont comparés à la base de règles. Tous les autres paquets sont comparés à la table d'état située en mémoire noyau et donc très rapide.
Lorsqu'une session est initiée par un paquet SYN, un timeout est positionné à 60 secondes. Le firewall attend alors un paquet retour pour établir la connexion. Lorsqu'il reçoit ce paquet, le timeout est positionné à 3600 secondes. Le firewall attend n'importe quel paquet alors qu'il devrait attendre un paquet SYN/ACK et pas de contrôle sur les numéros de séquence,
Si on initie une session avec un paquet ACK, le firewall n'accepte pas le paquet (ceci n'est vrai qu'à partir de la version 4.1 SP2) car seul un paquet SYN peut initier une connexion et donc insérer une session dans la table d'état. Ce mécanisme est désactivable permettant d'éviter de perdre les connexions établies alors que l'on est entrain de modifier la base de règles ou que l'on souhaite arrêter puis redémarrer le firewall sans que les sessions en cours soit perdues. Toutefois, en désactivant ce mécanisme on accroît le risque d'intrusion étant donné qu'un paquet autre que SYN peut initier une session et donc cette session peut être insérée dans la table d'état. Ainsi, un paquet ACK d'une session antérieur au redémarrage du firewall peut permettre d'accepter de nouveau cette connexion en rajoutant les éléments correspondants dans la table d'états.

5.4.3.4.3 FERMETURE D'UNE CONNEXION TCP

FW-1 ferme les connexions en les laissant tomber en timeout. En effet, lorsqu'un paquet FIN ou RST est reçu pour une session, le timeout passe de 3600 secondes à 50 secondes. Si aucun paquet n'est échangé durant cette période, la connexion est enlevée de la table d'états. Si des paquets sont envoyés pendant cette période, le timeout est remis à 50 secondes. Ce mécanisme permet de réduire les possibilités de dénis de service si quelqu'un envoie des paquets RST ou FIN spoofés. Ce comportement est similaire à l'état TIME_WAIT dans lequel passe une connexion TCP après avoir acquitté le second paquet FIN lors de la fermeture d'une session.

5.4.3.4.4 UDP

Les paquets UDP sont plus simples à gérer au niveau du firewall car par définition du protocole UDP, il n'y a pas de notion d'état. Lorsque la base de règles autorise un paquet UDP à traverser le firewall, une entrée est ajoutée à la table. Si un paquet se représente pendant la durée du timeout (40 secondes) avec les adresses IP source et destination et les ports source et destination correspondant, le paquet est accepté.

5.4.3.4.5 ICMP

Le trafic ICMP n'est pas inspecté de façon « stateful ». Il n'est jamais entré dans la table de connexions. Ainsi, il est difficile de faire différencier les différents trafics ICMP.

5.4.3.4.6 FRAGMENTATION

La fragmentation IP est souvent un problème pour les équipements de filtrages comme FW-1. FW-1 réalise un réassemblage des fragments, inspecte le paquet réassemblé et applique la règle correspondante.

5.4.3.5 PROXY SOCKS

Il n'existe pas de proxy pour la gestion du protocole ICA. Pour se rapprocher de la sécurité et du service offert par un relais applicatif on peut utiliser les SOCKS. On peut configurer un client ICA pour se connecter à un serveur Citrix via un proxy SOCKS. Toutefois, un proxy SOCKS ne fournit pas un niveau de sécurité suffisant mais nous la présentons car c'est la solution proposée par Citrix.
L'utilisation d'un serveur proxy SOCKS permet entre autres :
- de camoufler des informations : les noms système à l'intérieur du pare-feu ne sont pas connus des systèmes extérieurs au pare-feu via le DNS;
- d'effectuer l'authentification entre le client ICA et les serveurs proxy SOCKS ;
- d'effectuer l'authentification entre deux serveurs proxy SOCKS ;
- d'effectuer le relais entre deux serveurs proxy SOCKS ;
- de canaliser plusieurs connexions TCP dans une connexion ;
- d'assurer une fonction proxy sur les diffusions UDP.

Emplacement d'un serveur proxy SOCKS
On peut placer le serveur proxy d'un côté ou de l'autre du pare-feu. Dans certains cas, on peut choisir d'en placer un de chaque côté du pare-feu.
Les configurations typiques d'un serveur proxy SOCKS sont :
- Configuration d'un serveur proxy entre systèmes clients et pare-feu (pour des connexions vers l'extérieur) :

Pour interdire aux clients de se connecter directement à des serveurs situés à l'extérieur du pare-feu, installer un serveur proxy entre les systèmes clients et le pare-feu, comme indiqué ci-dessous. Le serveur proxy utilise ses fonctionnalités d'authentification pour déterminer si les clients ICA peuvent accéder aux réseaux extérieurs au pare-feu. Configurer le pare-feu pour qu'il laisse passer uniquement le trafic réseau provenant du serveur proxy SOCKS.
- Configuration d'un serveur proxy entre serveurs Citrix et pare-feu (pour des connexions vers l'intérieur) :

Pour protéger les serveurs Citrix, installer un serveur proxy entre les serveurs et le pare-feu. Le pare-feu peut être configuré de deux manières décrites ci-dessous.
- Maximalisation de l'approbation : le pare-feu ne laisse passer que le trafic réseau dirigé vers le serveur proxy SOCKS. Le serveur proxy procède à l'authentification du client ICA.
- Minimalisation du risque : non seulement le pare-feu ne laisse passer que le trafic réseau dirigé vers le serveur proxy SOCKS, mais il n'autorise de plus que les connexions à partir d'ordinateurs spécifiques.

- Configuration d'un réseau privé virtuel avec deux serveurs proxy :

On peut créer un réseau privé virtuel entre deux sites en configurant un serveur proxy à l'intérieur du pare-feu de chacun des sites client et serveur. Configurer les pare-feu pour qu'ils n'autorisent que le trafic UDP dirigé entre les deux serveurs proxy SOCKS et le protocole TCP sur le port SOCKS. Pour plus de sécurité, configurer le serveur proxy SOCKS du site client ICA pour qu'il effectue l'authentification avec le serveur proxy SOCKS du site serveur Citrix. Il faut connaître l'adresse du serveur proxy SOCKS situé à l'intérieur du pare-feu externe.
Le trafic UDP et le trafic TCP sont relayés par le proxy.

5.4.3.6 SELECTION DES PRODUITS

Parmi tous les équipements de filtrage disponible sur le marché il est difficile d'en choisir un plutôt qu'un autre si on ne connaît pas les mécanismes utilisés qui viennent d'être énoncés ci-dessus. Il faut souvent faire très attention en choisissant un tel équipement car s'il n'est pas adapté aux besoins ou s'il est mal configuré, il ne sert à rien.
Comme nous avons vu précédemment, la technologie Citrix s'appuie sur l'utilisation du protocole ICA utilisant le port 1494 et sur un service d'exploration utilisant le port UDP 1604. Il n'existe pas de relais applicatif (proxy) pour le protocole ICA, cette solution doit donc être écartée à moins qu'on utilise un proxy générique (SOCKS). Toutefois, cette solution ne fournie pas un niveau de sécurité suffisant.
Le filtrage de paquets (Packet Filtering) n'est pas non plus adapté aux flux ICA car il ne prend pas en compte la notion de session. Le filtrage adaptatif (Stateful Inspection) est bien adapté au flux ICA nécessaire au fonctionnement de la technologie Citrix. Nous choisirons donc les produits parmi cette catégorie.
En ce qui concerne les solutions tournant sur un serveur Windows NT ou Unix, elles vont être amenées à disparaître. On assiste à une évolution de ces fonctionnalités vers des boîtiers dédiés et les routeurs.
Voici quand même deux solutions tournant sur un serveur :

- CheckPoint Firewall-1 : facile d'utilisation, il est à l'origine du développement de la technologie Stateful Inspection.
- NetWall d'Evidian qui est un pare-feu hybride à la fois proxy et aussi Stateful Inspection, ce produit est complexe et coûte assez cher.

Voici une liste non exhaustive des équipements de filtrages sur des boîtiers , ils mettent tous en œuvre un mécanisme similaire au Stateful Inspection :

- Le PIX de Cisco : châssis firewall gigabit par inspection de paquets avec gestion de RPV compatible IPSec (chiffrement Triple DES, 168 bits) ; boîtier 3U pour armoire 19 pouces.
- Cisco IOS Firewall : système d'exploitation permettant de faire du filtrage, il est mis en place directement sur les routeurs Cisco.
- Nokia IPXXX de Nokia Internet Communication : réunit un routeur IP et le coupe-feu logiciel de Check Point FireWall-1, VPN-1. Il cumule des fonctions de routage avancées (RIP1 et 2, OSPF, BGP4, etc.) et offre un large choix d'interfaces WAN.
- NetScreen : châssis firewall gigabit matériel doté d'une passerelle de VPN ; utilise la technologie Stateful Inspection ; VPN compatible IPSec ; client LDAP ; gestion des sous-réseaux virtuels (VLAN) ; fonctions de gestion du trafic (diffserv, gestion de priorités au niveau 4) ; alimentation et ventilation redondantes.
- WatchGuard : boîtier firewall qui met nettement l'accent sur les dispositifs de surveillance de l'activité et d'alerte en cas d'attaque. Un abonnement permet l'accès à des mises à jour automatiques.
- NetASQ : un éditeur français proposant des boîtiers firewall (inspection de paquets) et VPN. Cette solution est compatible OPSEC et est un acteur en pleine croissance.

L'interopérabilité entre les solutions peut se faire à l'aide du protocole CVP qui est implémenté sur de nombreux équipements de filtrage qui utilisent la plate-forme de compatibilité OPSEC de CheckPoint.

5.4.3.7 UNE AUTRE SOLUTION : ICA PASS THROUGH

Cette fonctionnalité fait office de relais applicatif ICA (proxy). Cette solution n'offre pas de service de sécurité en analysant les flux. C'est un service permettant de relayer une connexion ICA (port TCP 1494) et uniquement ce type de connexion. Ce service doit être installé sur un serveur dédié que l'on place sur une DMZ publique. Il communique avec une ferme de serveur placée sur une DMZ privée.

L'ICA Pass Through s'implémente sous la forme d'un serveur Citrix MetaFrame configuré de manière à exécuter le logiciel client ICA pour le compte des postes clients ICA. C'est donc ce serveur qui établit une connexion au serveur d'applications Metaframe.

Cette fonctionnalité permet de n'autoriser le service explorateur ICA (trafic UDP) uniquement entre la ferme de serveurs et le serveur ICA pass through. Cette fonctionnalité est largement mise en œuvre chez les entreprises autorisant l'usage du client ICA via Internet (ex : Yahoo).

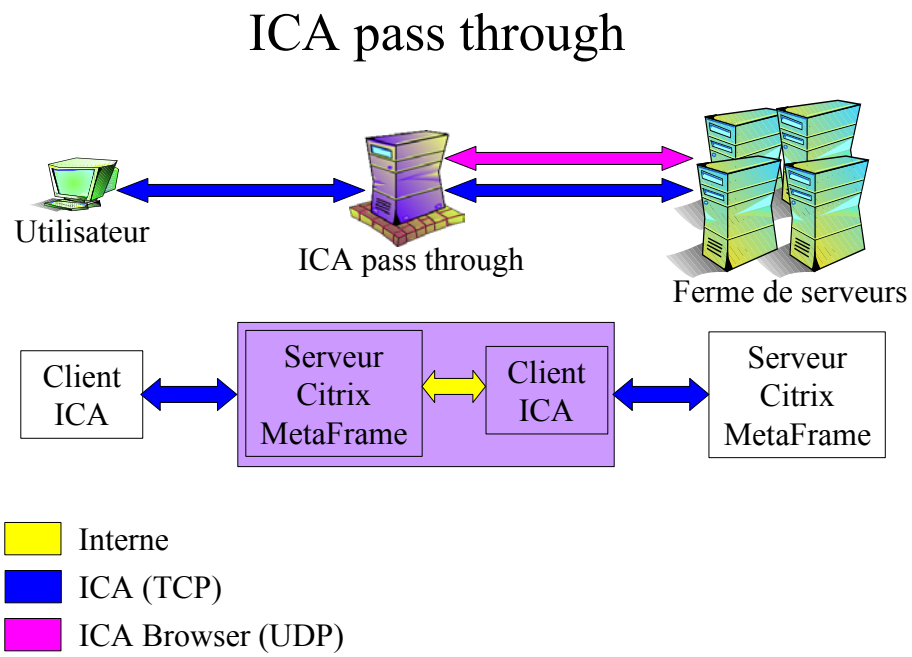


FIGURE 13 : PRINCIPE DE FONCTIONNEMENT D'ICA PASS THROUGH

Le serveur ICA pass through n'entraîne pas l'acquisition de licenses supplémentaires pour les utilisateurs. Celles-ci sont décomptées sur le serveur d'applications Citrix réel.

5.4.4 SECURISATION DES ECHANGES

5.4.4.1 SERVICE DE CHIFFREMENT INTEGRE AUX PRODUITS DE CITRIX

Citrix MetaFrame propose un service de chiffrement du flux ICA. Le produit NFuse (associé à un service web) fournit un service de chiffrement des flux HTTP et Citrix XML.

5.4.4.1.1 ARCHITECTURE SIMPLE

Dans une architecture simple, on peut sécuriser les flux d'informations échangées en chiffrant le flux ICA. Cette fonctionnalité fait partie du produit Citrix MetaFrame. Plusieurs niveaux de chiffrement sont disponibles.
L'algorithme de chiffrement utilisé est RC5 de RSA Security. RC5 est un algorithme de chiffrement symétrique (encore appelé à clé secrète), la clé de chiffrement et de déchiffrement est identique, les deux entités communicantes doivent posséder la même clé. Cette clé est générée séparément sur chaque entité par l'algorithme de Diffie-Hellman avec des clés de 1024 bits. Cet algorithme permet de générer une nouvelle clé sur chaque entité de la communication sans échanger d'information. Les paramètres de cet algorithme sont périodiquement modifiés pour renouveler la clé partagée. En limitant dans le temps l'utilisation d'une clé on réduit les risques de décryptage des informations échangées.
Les possibilités offertes sont les suivantes :
- Cryptage des données d'authentification avec une clé RC5 de 128 bits.
- Cryptage du flux ICA avec une clé RC5 de 40, 56 ou 128 bits.

Le niveau de chiffrement avec une clé de 128 bits est considéré comme impossible à décrypter (en théorie). Le chiffrement avec des clés d'une longueur de 40 bits et 56 bits nécessitent un investissement relativement important pour décrypter les informations chiffrées.
On peut utiliser un niveau de chiffrement par type de connexion.
L'administrateur peut forcer les utilisateurs à chiffrer leur connexion avec le serveur Citrix. Si le niveau minimum de chiffrement n'est pas appliqué du côté du client ICA la connexion n'est pas permise.

5.4.4.1.2 ARCHITECTURE PORTAIL

La sécurisation des échanges entre les différentes entités de l'architecture portail est possible comme suit :
- Entre le navigateur web et le serveur web : mettre en place SSL au niveau du serveur Web et utiliser un navigateur web compatible SSL. Pour protéger les informations d'authentification contenues dans le fichier ICA on peut utiliser un mécanisme appelé ticketing qui fournit un jeton de durée limitée et valide pour une seule session ICA. La correspondance entre les informations d'authentification et ce jeton est effectué sur le serveur web.
- Entre le serveur Web et le serveur MetaFrame : sécurisation du trafic XML en utilisant un relais Citrix SSL comme intermédiaire entre le serveur web et la ferme de serveurs MetaFrame. Dans le cas où l'on ne peut pas utiliser cette configuration, on doit installer le serveur web sur le serveur Citrix MetaFrame si l'on souhaite sécuriser cet échange.
- Entre le client ICA et le serveur MetaFrame : chiffrement de la séquence d'initialisation et du flux ICA par RC5, utilisation du ticketing pour sécuriser l'authentification.

5.4.4.2 IPSEC

Les applications publiées peuvent être accessibles non seulement par l'intermédiaire du réseau informatique interne à l'entreprise mais aussi par des utilisateurs externes comme leurs partenaires, leurs clients, les utilisateurs nomades ou des agences dispersées dans le monde accessible via l'Internet. Pour transporter les informations en toute sécurité on peut chiffrer les communications.

IPSec est le standard de sécurisation des échanges sur réseau IP définis par l'IETF. Nous étudierons cette solution car IPSec est amené à remplacer les autres solutions de sécurisation des échanges (L2TP, PPTP, L2F). IPSec s'ajoute comme extension à IPv4 et est intégrée nativement dans IPv6.

Dans la suite, nous nous intéresserons uniquement au cas d'IPv4, IPv6 n'étant pas encore utilisé à grande échelle.

5.4.4.2.1 DESCRIPTION SUCCINCTE D'IPSEC

IPSec est un protocole de sécurisation des échanges au niveau IP qui repose sur deux mécanismes : AH (Authentification Header) et ESP (Encapsulating Security Payload) fournissant plusieurs mode de sécurisation. Les paramètres nécessaires à l'utilisation de ces mécanismes sont gérés à l'aide d'associations de sécurité (Security Association – SA). Une association de sécurité regroupe les paramètres servant à protéger le trafic en fonction du mode de sécurisation utilisé. Les SA sont stockées dans une base de données des associations de sécurité (Security Association Database – SAD) et gérées à l'aide du protocole IKE (Internet Key Exchange) d'échange de clés. Les protections offertes par IPSec sont basées sur des choix définis dans la base de données de politique de sécurité (Security Policy Database, SPD). Cette liste de règles permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou sera rejeté.

IPSec peut être utilisé au niveau d'un hôte (station de travail ou serveur) ou au niveau de passerelles de sécurité (routeur, firewall, proxy, ...) permettant ainsi des approches de sécurisation lien par lien comme de bout en bout. IPSec peut être utilisé, notamment, pour la création de réseaux privés virtuels ou la sécurisation des accès distants.

Le document de base pour comprendre le fonctionnement d'IPSec est la RFC 2401.

5.4.4.2.2 LES DIFFERENTES APPROCHES DE SECURISATION

Entre deux machines (host-to-host) :

Figure 14 : architecture IPSec Host-to-Host

Entre deux réseaux (subnet-to-subnet) :

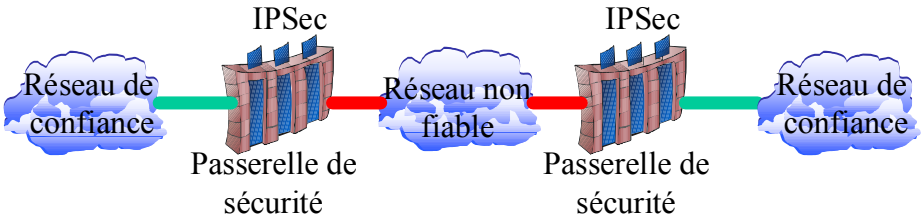


Figure 15 : architecture IPSec Subnet-to-Subnet

Entre une machine et un réseau (host-to-subnet) :

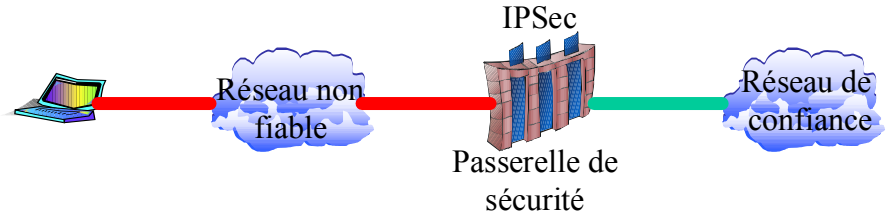


Figure 16 : architecture IPSec Host-to-Subnet

IPSec fournit plusieurs services de sécurisation des échanges basée sur des en-têtes différentes : AH et ESP.
AH (Authentication Header) assure l'intégrité des données en mode non connecté, l'authentification de l'origine des données et, de façon optionnelle, la protection contre le rejeu. Les services d'intégrité et d'authentification sont réalisés ensembles, à l'aide d'un bloc de données supplémentaire adjoint au message à protéger. L'expéditeur calcule les données d'authentification à partir de l'ensemble des champs invariants du datagramme IP final.
Ce mécanisme est décrit dans la RFC 2402.
ESP (Ensapsulating Security Payload) peut assurer, au choix, un ou plusieurs des services suivants :

- confidentialité
- intégrité des données en mode non connecté et authentification de l'origine des données, protection contre le rejeu. ESP fonctionne sur le principe de l'encapsulation : les données originales sont chiffrées puis encapsulées entre un en-tête et un trailer (pour indiquer la fin).

Si elle a été sélectionnée, l'authentification est toujours appliquée après que les données ne soient chiffrées. Cela permet, à la réception, de vérifier la validité du datagramme avant de se lancer dans la coûteuse tâche de déchiffrement.
Ce mécanisme est décrit dans la RFC 2406.
Les algorithmes d'authentification (pour AH et ESP), et de chiffrement (pour ESP) utilisables sont listés dans la RFC 2407.
Pour les mécanismes AH et ESP, deux modes sont possibles pour la sécurisation des échanges :

- le mode transport qui protège juste les données transportées.
- le mode tunnel qui protège le paquet IP complet (en-tête et données).

Voici les configurations possibles en fonction du service désiré (le champ « données » correspond au protocole de niveau supérieur à IP) :

Figure 17 : datagramme IP d'origine

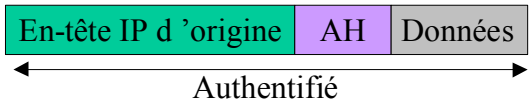


Figure 18 : position de AH en mode transport

Figure 19 : position de AH en mode tunnel

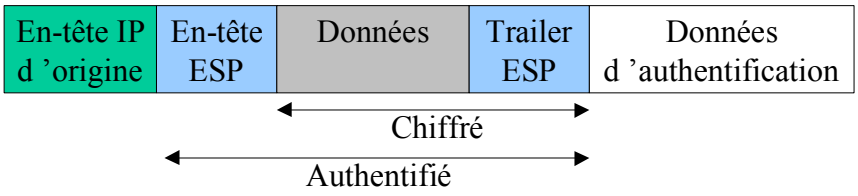


Figure 20 : position de ESP en mode transport

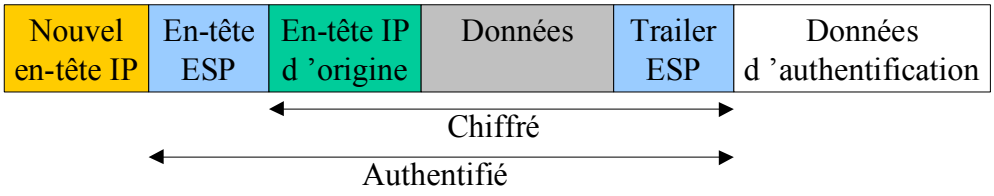


Figure 21 : position de ESP en mode tunnel

5.4.4.2.3 SYSTEME DE NEGOCIATION ET D'ECHANGE DE CLES

Le cœur du fonctionnement d'IPSec repose sur des mécanismes de négociation et d'échange de paramètres (clés, algorithmes) pour l'authentification, l'intégrité et la confidentialité. IPSec s'appuie sur IKE (Internet Key Exchange) qui est une combinaison d'ISAKMP, Oakley et SKEME(décrits ci-dessous).
ISAKMP (Internet Security Association for Key Management Protocol) pose les bases permettant de construire des associations de sécurité. ISAKMP est décrit dans la RFC 2408.
SKEME est un protocole orienté connexion qui propose plusieurs modes d'échanges de clefs distincts et se compose de trois phases : partage, échange et authentification.
Oakley ressemble beaucoup à SKEME, et permet en plus la négociation de paramètres. Oakley est décrit dans la RFC 2412.
IKE comporte différents modes et options de négociation des clés. Une première phase consiste en la négociation d'une association de sécurité ISAKMP. Trois clés sont générées à l'issue de cette première phase : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs (par Diffie-Helman). L'authentification des tiers peut se faire par secret partagé préalable, chiffrement à clé publique ou signature.
Une seconde phase a pour objet la négociation d'associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser. Les messages échangés durant cette phase sont protégés en authentification, intégrité et confidentialité grâce aux éléments négociés durant la première phase.
IKE est décrit dans la RFC 2409.

5.4.4.3 CHOIX D'UNE SOLUTION DE SECURISATION DES ECHANGES

Les fonctions de réseau privé virtuel peuvent être purement logicielles, à installer sur les plates-formes de serveurs généralistes du marché, ou préconfigurées dans des boîtiers dédiés, des coupe-feu (firewall) ou des routeurs multifonctions.
Nous ne considérons que les principaux éditeurs de solutions de sécurité qui vont nous permettent de sécuriser les échanges en environnement Citrix.
Les critères de choix essentiels sont la facilité de déploiement et d'administration, l'étendue des fonctions de sécurité comme la possibilité de se référer à une politique globale de sécurité.

5.4.4.3.1 SECURISATION DES ECHANGES ENTRE UN CLIENT ISOLE ET UN SERVICE CITRIX METAFRAME

Pour des connexions entre une plate-forme utilisateur et un réseau hébergeant le service Citrix MetaFrame d'accès aux applications (cf. Figure 16 : architecture IPSec Host-to-Subnet) ou serveur isolé (cf. Figure 14 : architecture IPSec Host-to-Host), il suffit d'installer un logiciel client (client VPN) spécifique sur la plate-forme utilisateur pour la gestion du VPN. Cette configuration prend en compte le cas des nomades.
Pour utiliser la technologie Citrix tout en garantissant la sécurisation des échanges, il faut ouvrir une session VPN à l'aide d'un client VPN avant d'établir la connexion au serveur Citrix à l'aide d'un client ICA. Ceci complique grandement l'utilisation du service Citrix, l'idéal est que le client VPN soit intégré au client ICA ce qui est proposée par Citrix au travers de son produit Citrix Extranet décrit plus loin.
Dans le cas de l'utilisation de terminaux, il n'est pas possible d'installer de logiciel supplémentaire pour la gestion du VPN. Le client VPN comme le client ICA doit être préinstallé.
Dans cette architecture Host-to, les solutions les plus intéressantes sont le logiciel CheckPoint 2000, Windows 2000 Server et bien sûr Citrix Extranet.
Couplé à un pare feu individuel, qui s'installe en même temps sur le poste de l'utilisateur, le logiciel SecureClient de CheckPoint hérite directement et automatiquement des règles de sécurité fixées par l'administrateur. La seule configuration sur le poste de l'utilisateur se résume à la déclaration d'une adresse IP du serveur de VPN à contacter. CheckPoint propose trois modes de chiffrement DES ou 3-DES (de 40 à 168 bits).
Microsoft se limite en standard à l'algorithme 56 bits toutefois l'algorithme 3-DES 168 bits peut être utilisé nécessitant une mise à niveau. Dans tous les cas la configuration nécessite l'obtention d'un certificat numérique, soit auprès d'un organisme certificateur, soit par un serveur de certificats existant dans le réseau de l'entreprise ou installé à l'occasion. L'installation du client nomade est plus simple que pour CheckPoint mais cette dernière solution est plus riche pour la configuration en accès distant et le déploiement des clients mobiles.
Citrix, avec son produit Citrix Extranet, propose un produit complet sous la forme d'un serveur gérant les connexions VPN entre les clients ICA VPN et le(s) serveur(s) Metaframe.
Les fonctionnalités offertes par le produit Citrix Extranet sont les suivantes :

- Contrôle d'accès.
- Identification et authentification des utilisateurs (possibilité de mécanisme d'authentification tierce avec RSA SecurID)
- Chiffrement.
- Suivie d'activité.
- Inscription en ligne d'un utilisateur pour l'accès aux applications ce qui facilite le déploiement de l'accès aux applications. Pour accéder aux applications, l'utilisateur installe le client Citrix Extranet puis s'enregistre via une interface web.
- Administration centralisée (gestion des serveurs et des utilisateurs, des droits d'accès sur les applications, gestion de groupes, administration à distance).

Le port utilisé par ce service est le port TCP 443 qui est couramment alloué pour l'utilisation de communications sécurisées par SSL. Il faudra veiller à autoriser ce service sur les équipements de filtrages.
Dans cette architecture Host-to, la solution préconisée est le produit Citrix Extranet qui ajoute une fonctionnalité de client VPN au client ICA.

5.4.4.3.2 SECURISATION DES ECHANGES DE SITE A SITE

Un ensemble d'utilisateurs présents sur un même réseau d'un site d'une entreprise peut avoir besoin d'utiliser un service Citrix présent sur un autre site de l'entreprise ou site un extérieur à l'entreprise (on peut utiliser l'Internet). Il faut donc sécuriser les échanges entre ces deux réseaux.
Dans cette architecture dite « Subnet-to-Subnet », il n'y a pas de contraintes liées à l'utilisation de Citrix puisque les flux ICA sont chiffrés à la sortie du réseau et déchiffrés à l'entrée dans le second réseau au niveau des passerelles de sécurité (routeur, firewall).
Les solutions qui s'avèrent les plus intéressantes sont les fonctionnalités de sécurité des routeurs Cisco et le produit CheckPoint 2000 de CheckPoint (FW-1/VPN-1).
L'utilisation d'un routeur Cisco (par exemple le 1720) est le plus simple à mettre en œuvre. Le logiciel Cisco Secure Policy Manager, livré avec le routeur, permet d'associer par simple glisser-déposer les éléments constitutifs d'un tunnel (équipements de réseau, conditions de filtrage de trafic, autorisations d'accès, ...). Les options pour la configuration des tunnels sont assez complètes. Les règles de chiffrement peuvent être créées hors connexion. Une fois validées et traduites en langage IOS (langage des routeurs Cisco), elles sont, au choix de l'utilisateur, transférées immédiatement ou ultérieurement aux routeurs.
CheckPoint 2000, comme le routeur Cisco, oblige de décrire au préalable, et très précisément, la topologie du réseau, ce qui procure ensuite une vision bien plus claire de l'infrastructure. CheckPoint 2000 relie étroitement VPN et firewall. Les stratégies de sécurité définies sont dans la pratique traduites en règles du firewall.
Le routeur Cisco est plus simple d'utilisation et plus riche en fonctions de sécurité, de plus, le mode de licences de CheckPoint 2000 est très contraignant. Enfin, Cisco prend en compte les protocoles de chiffrement VPN antérieurs à IPSec comme L2TP, PPTP, L2F permettant ainsi une interopérabilité théorique avec des solutions VPN existantes utilisant ces protocoles.
Cisco avec le Cisco Secure Policy Manager est la solution préconisée pour une architecture VPN site à site (Subnet-to-Subnet).

6. CONCURENTS

6.1 MICROSOFT

Microsoft propose son propre composant Terminal Server, intégré en standard à Windows 2000 Server, ainsi que son propre protocole RDP (Remote Display Protocol), pour la mise en place d'une architecture client-léger. Mais la plupart des entreprises qui adoptent cette architecture préfèrent bénéficier en plus des services à valeur ajoutée de la couche Metaframe de Citrix.
Sur 100 serveurs Windows NT4 ou 2000 installés en environnement Terminal Server, on estime que 70 à 80 disposent de la couche Metaframe (Citrix).
Comparaison entre les protocoles RDP (Microsoft) et ICA (Citrix) :

	RDP	ICA
Clients Windows 3.11, 9x,NT, CE	OUI	OUI
Clients DOS, Windows 3.1x, 9x, NT, CE, Unix, Mac, JAVA, NC, Navigateur WEB	NON	OUI
Optimisation bande passante	OUI	OUI
Caching des bitmaps sur le disque du poste client	OUI	OUI
Répartition de charge / Load balancing	OUI[1]	OUI[2]
Prise de main / Contrôle à distance	OUI	OUI
Gestion des imprimantes locales	OUI	OUI
Gestion des disques locaux	NON	OUI
Gestion du copier / coller	OUI	OUI
Support Audio	OUI[3]	OUI
Support Vidéo	OUI	OUI[4]
Kits de développements	OUI	OUI
Support DCOM	OUI	OUI
API publiques	OUI	OUI
Cryptage	OUI	OUI[5]

(1) NLBS disponible sur W 2000 Advanced Server(2) Disponible avec Citrix Load Balancing (option)(3) Disponible avec le kit de développement SDK
(4) Disponible avec Citrix Vidéoframe
(3) Disponible avec Citrix Secure ICA Services (Option) - Support de clés 40 et 56 bits
L'architecture ICA apporte une vraie valeur ajoutée en terme d'administration des fermes de serveurs, de gestion de la répartition des charges et de possibilité de prise de contrôle à distance pour faire du shadowing.

De plus, le client ICA est disponible pour d'autres clients que Windows et il permet la visibilité des disques locaux lorsque l'utilisateur est en session sur le serveur.

6.2 NEW MOON

New Moon System Inc. est un éditeur qui a mis au point des plates-formes logicielles permettant aux entreprises et ASP de gérer efficacement et facilement leurs applications Windows distribuées. La solution Canaveral iQ de New Moon améliore les performances du système informatique et donc la rentabilité de l'entreprise.

New Moon Canaveral iQ est associé à Microsoft WTS, et représente une solution alternative à Citrix.

New Moon Canaveral iQ est une plate-forme de gestion d'applications pour les environnements client léger. Elle permet aux administrateurs système de gérer simplement et efficacement les relations complexes entre les utilisateurs, les serveurs applicatifs et les applications Windows hébergées sur serveur.

Canaveral iQ permet de :

- Compléter et sublimer les fonctionnalités de **Microsoft RDP**,
- Administrer, installer et configurer simplement,
- Contrôler son activité afin de gérer au mieux ses achats logiciels,
- Apporter une solution client léger serveur à un prix abordable,
- Fournir une alternative intelligente aux solutions existant sur le marché.

CONCLUSION

Bien plus qu'un simple éditeur de logiciel, Citrix est aujourd'hui devenu une technologie, un savoir-faire. Le marché du Client Léger est en pleine expansion ces derniers temps.

Les budgets de fonctionnement des Systèmes d'Information des entreprises sont revus fortement à la baisse depuis 2001. Ainsi, les décideurs et architectes s'orientent de plus en plus vers des architectures de type portail afin de maîtriser les coûts lors de l'ouverture du système à leur partenaire.

Glossaire

Administrateur Citrix : administrateur système chargé de l'installation, de la configuration et de la maintenance de serveurs Citrix.

Application anonyme : application publiée exclusivement pour les utilisateurs anonymes.

Application publiée : application installée sur un serveur Citrix ou dans une batterie de serveurs Citrix et configurés pour un accès multi-utilisateurs à partir de clients ICA.
Load Manager permet de gérer la charge des applications publiées sur les différents serveurs d'une batterie.
Program Neighborhood et NFuse permettent d'ajouter une application publiée sur le bureau client des utilisateurs.

Assistant de publication d'application : assistant utilisé pour publier des applications dans une batterie de serveurs Citrix.

Bande passante : Quantité maximale d'informations que peut véhiculer un canal de communication.

Barre des tâches d'observation : barre des tâches affichée sur le bureau d'un serveur Citrix, qui peut être utilisée pour observer plusieurs utilisateurs et pour basculer entre les différentes sessions observées.

Base de données des mises à jour des clients : base de donnée utilisée par les serveurs Citrix pour mettre à jour automatiquement les clients ICA. Elle contient les copies des clients et des informations de configuration permettant d'effectuer les mises à jour.

Batterie de serveurs : groupe de serveurs Citrix gérés comme une entité unique, avec des connexions physiques entre les serveurs et un magasin de données IMA.

Choix d'un explorateur : processus suivi par les explorateurs ICA pour choisir un explorateur principal parmi les serveurs Citrix d'un réseau donné. Ce processus est déclenché lorsqu'un nouveau serveur Citrix est démarré, lorsque l'explorateur principal courant ne répond pas ou lorsqu'un serveur ou un client ICA détecte deux explorateurs principaux.

Client de liaison : client ICA installé sur un serveur MétaFrame et qui permet à un utilisateur d'un client ICA quelconque d'accéder à des applications publiées en s'y connectant à partir du logiciel Citrix Program Neighborhood utilisé alors en tant qu'application publiée.

Client ICA : logiciel Citrix qui permet à un serveur Citrix à partir de différents types de machine cliente.

Client léger ou Client Fin (Thin Client) : Une architecture de ce type est une architecture client-serveur particulière, permettant à plusieurs utilisateurs de se connecter en même temps et d'exécuter des applications sur le serveur dans des sessions indépendantes et protégées. Le client est dit « fin » ou « léger » parce seuls les frappes clavier, les clics souris et les différentiels d'affichage écran transitent sur le réseau : la machine cliente ne prend en charge aucun traitement de l'application en cours d'exécution, c'est le serveur qui s'occupe de tout. Par opposition au client léger, un client dit "lourd" assume une part du traitement applicatif dans une architecture client-serveur.

Collecteur de données : serveur MétaFrame utilisé pour le stockage des données dynamiques d'une zone définie dans une batterie de serveurs MétaFrame XP.
Connexion ICA : 1.port logique utilisé par un client ICA pour se connecter à un serveur Citrix et y ouvrir une session. Une connexion ICA est associée à une connexion réseau (TCP/IP, IPX, SPX ou Net BIOS, par exemple) ou à une connexion série (par modem ou par câble). 2. Liaison active établie entre un client ICA et un serveur Citrix.

Connexion ICA personnalisée : raccourci défini par l'utilisateur, vers une application publiée ou un serveur Citrix.

Connexions ICA asynchrones : les connexions de type asynchrone permettent un accès direct par modem à un serveur Citrix sans recourir à RAS ni à TCP/IP.

Citrix Management Console : cet outil évolutif et indépendant de toute plateforme, développé par Citrix, permet l'administration des serveurs Citrix et des produits de gestion.

Dimensionnement : détermination des ressources nécessaires.

Echo local du texte : fonctionnalité qui accélère l'affichage du texte ainsi saisi sur la machine cliente pour évitera à l'utilisateur des temps d'attente trop importants sur le réseau.

Explorateur ICA membre : en mode mixte, explorateur ICA sur un serveur Citrix d'un réseau, qui fournit à l'explorateur principal des informations relatives aux licences, aux applications publiées, aux performances et à la charge des serveurs.

Explorateur ICA principal : en mode mixte, explorateur ICA sur un serveur Citrix d'un réseau, qui collecte et met à jour les informations relatives aux licences, aux applications publiées, aux performances et à la charge des serveurs, qu'il obtient des autres explorateurs membres du réseau.

Fenêtre transparente : si une application publiée est exécutée dans une fenêtre transparente, l'utilisateur peut se servir de toutes les fonctions de gestion de fenêtre de la plate-forme cliente (redimensionnement, réduction ...).

Fichier ICA : fichier texte (avec l'extension .ICA) contenant des informations sur une application publiée. Un fichier .ICA a le même format qu'un fichier Windows .INI. Les informations y sont structurées et peuvent être interprétées par les clients ICA. Lorsqu'un client ICA reçoit un fichier ICA, il initialise une session pour l'exécution de l'application spécifiée, sur le serveur Citrix indiqué dans le fichier.

Flux : Données informatiques transitant sur un réseau d'un point à un autre.

Gestion de la charge : fonctionnalité de Citrix Load Manager, qui permet de gérer la charge des applications. Lorsqu'un utilisateur lance une application publiée qui est configurée pour la gestion de la charge, la session ICA de cet utilisateur est lancée sur le moins chargé de la batterie, selon des critères qui peuvent être définis.

ICA (Independant Computing Architecture) : architecture utilisée par Citrix pour séparer la logique d'une application de son interface utilisateur.

ID de session : identificateur propre à une session ICA sur un serveur Citrix donné.

IMA (Independant Management Architecture) : infrastructure serveur-serveur, développée par Citrix, qui fournit des outils fiables, sécurisés et évolutifs pour la gestion d'une batterie de serveurs de toute taille.

Installation des clients citrix ICA par le Web : méthode utilisant le Web pour déployer les logiciels clients ICA vers les utilisateurs. Elle consiste à construire un site Web auquel les utilisateurs peuvent accéder pour télécharger les clients Citrix ICA correspondant à leurs machines clientes.

Interopérabilité : fonctionnalité de MétaFrame XP, qui permet à celui-ci de fonctionner en mode mixte avec des serveurs MétaFrame 1.8 au sein de la même batterie de serveurs. Les fonctions de MétaFrame XP ne sont pas toutes disponibles en mode mixte.

Lancement et incorporation d'application (ALE) : fonctionnalité des serveurs Citrix et des clients ICA qui permet de lancer des applications Windows à partir d'une page HTML ou de les incorporer dans une page HTML sans réécrire le code de ces applications.

Licence de connexion : licence qui permet l'établissement de connexions ICA entre une machine cliente et une batterie de serveurs Citrix. Un certain nombre d'unité de licence de connexion peut être attribué à un serveur donné, ou regroupé pour tous les serveurs d'une batterie.

Licence de produit : licence de logiciel qui autorise l'utilisation d'un produit Citrix.

Machine cliente : système informatique capable d'exécuter l'un des clients ICA.

Magasin de données : base de données ODBC utilisée par une batterie de serveurs MétaFrame XP. Le magasin de données centralise les données de configuration relatives aux applications publiées, aux utilisateurs, aux imprimantes et aux serveurs. Un seul magasin de données est associé à chacune des batteries de serveurs Citrix IMA.

Mappage des imprimantes clientes : fonctionnalité qui permet aux applications exécutées sur un serveur Citrix d'envoyer des travaux d'impression aux imprimantes configurées sur la machine cliente.

Mappage des lecteurs clients : fonctionnalité qui permet aux applications exécutées sur un serveur Citrix d'accéder aux unités physiques et logiques configurées sur la machine cliente.

Mappage des périphériques clients : fonctionnalité qui permet aux applications distantes exécutées sur un serveur Citrix d'accéder aux périphériques et aux unités de stockage reliées à la machine locale. Elle consiste en plusieurs fonctionnalités distinctes : mappage des lecteurs clients, mappage des imprimantes clientes et mappage des ports COM clients.

Mappage des ports COM clients : fonctionnalité qui permet aux applications exécutées sur un serveur Citrix d'accéder aux périphériques reliés aux ports COM de la machine cliente.

Mise à jour automatique des clients : fonctionnalité des serveurs Citrix, permettant d'installer les versions les plus récentes des clients ICA et de planifier le téléchargement et l'installation de ces logiciels sur les machines clientes des utilisateurs.

Mode mixte : mode de fonctionnement des serveurs MétaFrame XP lorsqu'une batterie de serveurs contient à la fois des serveurs MétaFrame XP et des serveurs MétaFrame 1.8.

Mode natif : mode de fonctionnement des serveurs MétaFrame XP lorsqu'un réseau comporte uniquement des serveurs Citrix IMA et que l'option permettant de fonctionner avec des serveurs MétaFrame 1.8 n'est pas sélectionnée.

Noeud distant : machine cliente qui peut se connecter à un réseau local ou étendu à l'aide d'un modem et d'un logiciel de communication. Une fois connectée, la machine a accès aux mêmes ressources réseau que n'importe quel autre noeud du réseau, mais elle est limitée par la bande passante et les performances du modem.
Nom affiché : nom attribué à l'application lors de sa publication. Ce nom apparaît dans le nouveau client Program Neignborhood et dans les dossiers Applications de la console Citrix Management Console. Il est également utilisable par les portails Web produits par la technologie NFuse de Citrix.

Nom de l'application : chaîne de caractère permettant d'identifier de manière unique une application publiée dans une batterie de serveurs. Les serveurs Citrix et les clients ICA utilisent ce nom pour différencier plusieurs applications qui pourraient porter le m^me nom affiché.

Observation : fonctionnalité des serveurs Citrix, qui permet à un utilisateur disposant des droits appropriés de se connecter à distance à la session ICA d'un autre utilisateur ou d'en prendre le contrôle, à des fins de diagnostic, de formation ou de support technique.

Panoramique et mise à l'échelle : fonctionnalité du client ICA permettant aux utilisateurs de visualiser une session distante dont la taille est supérieure à celle du bureau de la machine cliente. Par exemple, si les dimensions du bureau de la machine cliente sont 1024 x 768 pixels et si les dimensions de la session ICA sont 1600 x 1200 pixels, l'image de la session est trop grande pour être affichée dans la fenêtre d'affichage de la session. Le panoramique permet d'utiliser des barres de défilement. La mise à l'échelle fournit des contrôles dans le menu système, pour réduire la fenêtre de la session.

Program Neighborhood : interface utilisateur des clients ICA Win32 et ICA Java, qui permet à l'utilisateur de visualiser les applications publiées qu'il peut utiliser dans la batterie de serveurs. Le logiciel Citrix Program Neighborhood contient des séries d'applications et des connexions ICA personnalisées.

Protocole ICA : protocole utilisé par les clients ICA pour formater les données entrées par l'utilisateur (frappes clavier, clics de souris ...) et pour les envoyer aux serveurs Citrix où elles doivent être traitées. Les serveurs Citrix utilisent également ce protocole pour formater les données restituées par les applications (affichage, son, ...) et les envoyer à la machine cliente.

Réduction de latence Speedscreen : ensemble de technologies mises en oeuvre dans ICA et permettant de réduire la consommation en bande passante et le nombre total de paquets transmis, et donc de réduire les temps d'attente et d'harmoniser les performances, quelle que soit la connexion réseau utilisée.

Réseau étendu ou WAN (Wide Area Network) : Réseau de communication de données qui déssert des utilisateurs séparés par une grande zone géographique et qui utilise souvent des équipements de transmission fournis par un opérateur.

Réseau local ou LAN (Local Area Network) : Réseau de données à haute vitesse et à faible taux d'erreurs couvrant une zone géographique relativement petite (jusqu'à quelques milliers de mètres). Les réseaux locaux interconnectent des stations de travail, des périphériques, des terminaux et d'autres équipements dans un seul immeuble ou autre zone géographique limitée.

Restauration des connexions : fonction de client ICA qui permet aux utilisateurs ou aux administrateurs de définir plusieurs adresses de serveurs (serveurs principaux et serveurs de secours) pour une même application publiée. Cette fonction garantit aux utilisateurs la connexion aux applications publiées, même en cas d'incident sur un serveur.

Retour des clics souris : fonctionnalité qui fournit une confirmation visuelle des clics souris. Lorsque l'utilisateur clique avec la souris, le logiciel client ICA transforme immédiatement le pointeur en sablier et confirme ainsi la prise en compte de cette action.

Série d'applications :ensemble des applications publiées sur une batterie de serveurs et accessibles à un utilisateur.

Serveur Citrix : serveur MétaFrame, WinFrame ou VidéoFrame sur lequel des applications ou des vidéos sont publiées.

Service XML Citrix : service Windows NT qui fournit une interface HTTP à l'explorateur ICA. Comme ce service utilise des paquets TCP et non UDP, les connexions peuvent être établies au travers de la plupart des pare-feu. Le service XML Citrix utilise le port 80 comme port par défaut.

Session anonyme : Session ICA ouverte par un utilisateur anonyme.

Session déconnectée : session ICA sur le serveur Citrix, à laquelle le client ICA n'est plus connecté mais dans laquelle les applications de l'utilisateur sont toujours en cours d'exécution. L'utilisateur peut se reconnecter à une session déconnectée. S'il ne se reconnecte pas sous un certain délai, le serveur Citrix met automatiquement fin à la session.

Session ICA : connexion durable entre un client ICA et un serveur Citrix, définie par un ID utilisateur et une connexion ICA spécifiques. Une session ICA est caractérisée par un état de connexion, des ressources serveur attribuées à l'utilisateur pour la durée de la session et toutes les applications exécutées pendant la session. Une session ICA se termine normalement lorsque l'utilisateur du client ICA ferme sa session sur le serveur Citrix.

SOCKS : protocole pour les communications TCP sécurisées au travers d'un pare-feu.

Solution serveur centralisée : modèle informatique développé par Citrix, dans lequel les applications sont publiées sur des serveurs centralisés ou dans des batteries de serveurs. Les utilisateurs accèdent à ces applications à partir de machines clientes distantes. Ce modèle diffère du modèle client-serveur traditionnel dans ce sens que toute la logique d'une application est exécutée sur le serveur hôte, ce qui réduit la consommation en bande passante et les besoins en ressources des machines clientes.

Terminal Windows (WBT) : Machine de type client fin à fonctionnement limité, qui peut exécuter des applications uniquement en se connectant à un serveur d'application Citrix. Un terminal Windows ne peut pas exécuter des applications localement.

Utilisateur anonyme : utilisateur non identifié disposant de droits d'accès minimaux à un serveur ou à une batterie de serveurs Citrix et aux applications qui y sont publiées.

Zone : Ensemble de serveurs MétaFrame XP regroupés logiquement, généralement en fonction de leur sous-réseaux. Tous les serveurs MétaFrame XP d'une zone communiquent avec le serveur MétaFrame XP désigné collecteur de données pour cette zone.