

# Algorithmes de chiffrement

## *Mesures de performances réseaux*

Documentation version 1.0 créé le 22 juin 2005

Dernière mise à jour le 24 juin 2005

Licence : GNU FDL

Copyright © : CRI74

Auteur :

Emonet jean-Bruno

[jbemonet@ext.cri74.org](mailto:jbemonet@ext.cri74.org)



Bâtiment le Salève I  
Site d'Archamps  
F-74160 ARCHAMPS

Tél. : +33 (0)4 50 31 56 30  
Fax : +33 (0)4 50 95 38 17

E-mail : [info@cri74.fr](mailto:info@cri74.fr)  
Web : [www.cri74.fr](http://www.cri74.fr)

SIRET : 400 210 646 000 14  
APE : 913 E

# Table des matières

<b>1 – <a href="#">Introduction</a></b> .....	<b>3</b>
<b>2 – <a href="#">Chiffrement à clé privée</a></b> .....	<b>4</b>
2.1 – <a href="#">Chiffrements par blocs (Block Cyphers)</a> .....	4
2.2 – <a href="#">Chiffrements de flux</a> .....	4
<b>3 – <a href="#">Les algorithmes de chiffrement</a></b> .....	<b>5</b>
3.1 – <a href="#">3Des</a> .....	5
3.2 – <a href="#">Blowfish</a> .....	5
3.3 – <a href="#">Des</a> .....	5
3.4 – <a href="#">AES</a> .....	5
3.4.1 – <a href="#">Recommandations de la NSA</a> .....	6
3.4.2 – <a href="#">Twofish</a> .....	6
3.4.3 – <a href="#">Serpent</a> .....	6
3.4.4 – <a href="#">Rijndael</a> .....	7
<b>4 – <a href="#">Les fonctions de hachage</a></b> .....	<b>8</b>
<b>5 – <a href="#">Comparatif</a></b> .....	<b>9</b>
5.1 – <a href="#">Tableau</a> .....	9
5.2 – <a href="#">Performances</a> .....	9
<b>6 – <a href="#">Conclusion</a></b> .....	<b>10</b>
<b>7 – <a href="#">Webliographie</a></b> .....	<b>11</b>
<b>8 – <a href="#">Lexique</a></b> .....	<b>12</b>

# 1 – Introduction

Cette documentation a pour objectif de comparer les performance des algorithmes de chiffrements les plus importants tels que 3des, Blowfish, Twofish, Serpent, Rijndael. Le comparatif est précédé de notions et d'explications sur les systèmes de chiffrement à clé privée ainsi que sur les fonctions de hachage(MD5, SHA-1, etc..).

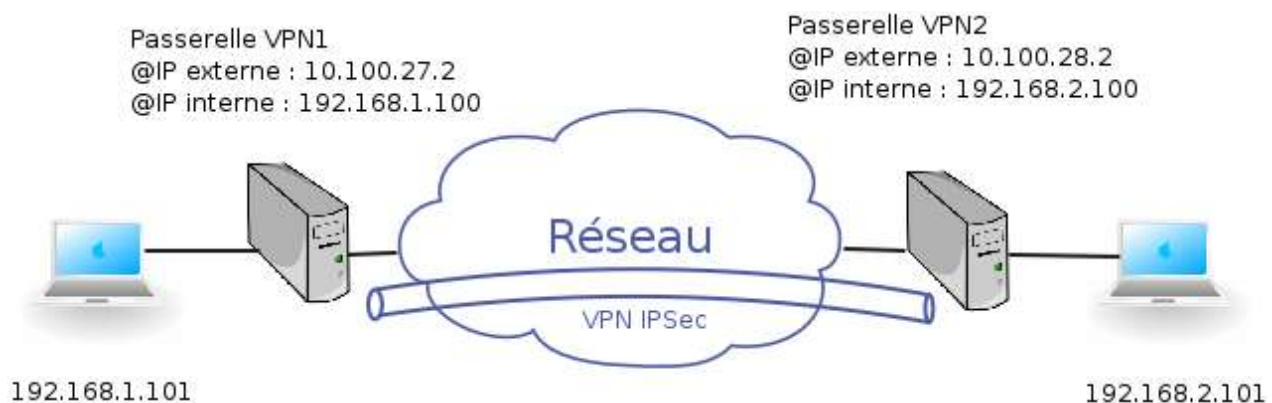
Les tests de performances ont été réalisés sous Linux avec l'outil IPERF. Cet outil permet par exemple de mesurer le bande passante maximale d'un réseau.

Pour plus d'informations sur IPERF : <http://dast.nlanr.net/Projects/lperf/>.

Les tests ont été réalisés à l'aide de 2 machines avec la configuration suivante:

Processeur :	Pentium II
Fréquence CPU :	450 MHz
Mémoire Cache :	512 KB
O.S :	Debian Sarge
Noyau Linux:	2.6

Les algorithmes de chiffrement sont utilisés pour chiffrer les données passant par un VPN (Virtual Private Network).



Pour permettre l'établissement d'un VPN, j'ai utilisé Strongswan. Il permet l'utilisation de nombreux algorithmes de chiffrement tels que : 3des, Blowfish, Twofish, Serpent, AES128, AES256.

## 2 – Chiffrement à clé privée

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clé pour le chiffrement que pour le déchiffrement.

Le chiffrement consiste alors à effectuer une opération entre la clé privée et les données à chiffrer afin de rendre ces dernières inintelligibles. Ainsi, le moindre algorithme (tel qu'un OU exclusif) peut rendre le système quasiment inviolable (la sécurité absolue n'existant pas).

Il y a deux catégories de systèmes à clé privée : les chiffrements par blocs et les chiffrements de flux.

### 2.1 – Chiffrements par blocs (Block Cyphers)

Dans ce type de chiffrement, il y a une séparation du texte clair en blocs d'une longueur fixe selon un alphabet, et un algorithme chiffre un bloc à la fois.

Une bonne sécurité est définie par une clé assez longue. Les clés très longues sont plus coûteuses en travail à cause notamment de leur génération, de leur transmission, de leur espace mémoire et de la difficulté de s'en rappeler (mots de passe).

La taille des blocs a un impact sur la sécurité et sur la complexité : les blocs de grandes dimensions sont plus sécuritaires mais sont plus lourds à implémenter.

### 2.2 – Chiffrements de flux

Les algorithmes de chiffrement de flux (stream ciphers) peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension unitaire (1 bit, 1 octet, etc.) ou relativement petite. Leurs avantages principaux viennent du fait que la transformation (méthode de chiffrement) peut être changée à chaque symbole du texte clair et du fait qu'ils soient extrêmement rapides. De plus, ils sont utiles dans un environnement où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs (diffusion). Ils sont aussi utilisés lorsque l'information ne peut être traitée qu'avec de petites quantités de symboles à la fois, comme par exemple si l'équipement n'a pas de mémoire physique ou une mémoire tampon très limitée.

# 3 – Les algorithmes de chiffrement

## 3.1 – 3Des

Le tripleDES (3DES) est en fait l'algorithme DES appliqué trois fois sur les données. Il a été conçu par Whitfield Diffie, Martin Hellman et Walt Tuchmann en 1978. L'algorithme utilise une taille de clé comprise entre 128 bits et 192 bits. La taille des blocs est de 8 octets (64 bits).

Le tripleDES a été approuvé FIPS (Federal Information Processing Standards) par le NIST et donc peut être utilisé par les organisations gouvernementales.

## 3.2 – Blowfish

Blowfish a été conçu par Bruce Schneier en 1993 comme étant une alternative aux algorithmes existants, en étant rapide et gratuit. Blowfish est sensiblement plus rapide que le DES. Il est un chiffrement Feistel, utilisant itérativement une fonction de chiffrement 16 fois. La grandeur des blocs est de 64 bits.

Il peut prendre une longueur de clé variant entre 32 bits et 448 bits. Depuis sa conception il a été grandement analysé et est aujourd'hui considéré comme étant un algorithme de chiffrement robuste. Il n'est pas breveté et ainsi son utilisation est libre et gratuite.

## 3.3 – Des

L'algorithme DES, Data Encryption Standard, a été créé dans les laboratoires de la firme IBM Corp. Il est devenu le standard du NIST en 1976 et a été adopté par le gouvernement en 1977. C'est un chiffrement qui transforme des blocs de 64 bits avec une clé secrète de 56 bits au moyen de permutations et de substitutions. Le DES est considéré comme étant raisonnablement sécuritaire.

Le DES est officiellement défini dans la publication FIPS 46-3 et il est public.

La clé est en fait constituée de 64 bits, dont 56 bits sont générés aléatoirement et utilisés dans l'algorithme. Les huit autres bits peuvent être utilisés pour la détection d'erreurs (dans une transmission par exemple). Chacun des huit bits est utilisé comme bit de parité des sept groupes de 8 bits.

Comme blowfish, le DES est un chiffrement Feistel. Il utilise les transformations de substitution et de transposition (chiffrement par produit). Il est aussi appelé Data Encryption Algorithm (DEA).

## 3.4 – AES

AES est le sigle d'Advanced Encryption Standard, en français « standard de chiffrement avancé ». Il s'agit d'un algorithme de chiffrement symétrique, choisi en octobre 2000 par le NIST pour être le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis.

Il est issu d'un appel d'offre international lancé en janvier 1997 et ayant reçu 15 propositions. Parmi ces 15 algorithmes, 5 furent choisis pour une évaluation plus poussée en avril 1999, MARS, RC6, Rijndael, Serpent, et Twofish. Au bout de cette évaluation, ce fut finalement le candidat Rijndael, du nom de ses deux concepteurs Joan Daemen et Vincent Rijmen (tous les deux de nationalité belge) qui a été choisi. Ces deux experts en cryptographie étaient déjà les

auteurs d'un autre algorithme : Square. Le terme d'AES remplace désormais celui de Rijndael mais l'algorithme n'a pas été modifié. Ceci n'est pas tout à fait vrai, AES est un sous-ensemble de Rijndael puisque il ne travaille qu'avec des blocs de 128 bits alors que Rijndael offre des tailles de blocs et de clefs qui sont des multiples de 32 (compris entre 128 et 256 bits).

Ce faisant, l'AES remplace le DES (choisi comme standard dans les années 1970) qui de nos jours devenait obsolète, car il utilisait des clefs de 56 bits seulement. L'AES a été adopté par le NIST (National Institute of Standards and Technology) en 2001. De plus, son utilisation est très pratique car il consomme peu de mémoire et n'étant pas basé sur des schémas de Feistel, sa complexité est moindre et il est plus facile à implémenter.

### 3.4.1 – Recommandations de la NSA

La NSA a annoncé que tous les finalistes qui avaient participé au concours AES pouvaient être considérés comme sûrs et qu'ils étaient suffisamment robustes pour chiffrer les données non-classifiées du gouvernement américain. En juin 2003, le gouvernement américain a annoncé que (traduction de la dépêche originale) :

"L'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128,192 et 256) étaient suffisantes pour protéger des documents classifiés jusqu'au niveau SECRET. Le niveau TOP-SECRET nécessite des clés de 192 ou 256 bits. L'implémentation de l'AES dans des produits destinés à la protection des systèmes de sécurité nationaux (ainsi que les documents) doit faire l'objet d'une analyse et d'une certification par la NSA avant leur acquisition et leur utilisation" .

### 3.4.2 – Twofish

Twofish est un algorithme de chiffrement symétrique par bloc inventé et analysé par Bruce Schneier, Niels Ferguson, John Kelsey, Doug Whiting, David Wagner et Chris Hall.

Il chiffre des blocs de 128 bits avec une clé de 128, 192 ou 256 bits. Twofish était l'un des cinq finalistes du concours AES mais il n'a pas été sélectionné pour le standard. Il reprend en partie des concepts présents dans le populaire Blowfish, du même auteur.

Twofish est légèrement plus lent que Rijndael mais plus rapide que les autres finalistes de AES. Twofish a été conçu pour être implémenté dans des smartcards et d'autres systèmes embarqués. Sur un Pentium, une implémentation optimisée en assembleur permet de chiffrer un bloc de 128 bits en 18 coups d'horloge (16.1 coups d'horloge sur un Pentium Pro).

En 2005, aucune attaque n'a pu être appliquée sur la version complète de Twofish. La recherche exhaustive reste le seul moyen pour le casser. Il semble en tout cas plus résistant que ce qui avait été initialement annoncé durant le concours AES. De part sa complexité, la cryptanalyse de cet algorithme reste délicate. Ses concepteurs ont eux-mêmes publiés des attaques sur des versions à 6 et 7 rondes. Une attaque sur 5 rondes a une complexité de  $2^{51}$ . Malgré ses atouts, il reste relativement peu utilisé et a été supplanté par le gagnant de AES, Rijndael. Il n'en demeure pas moins une alternative séduisante à l'actuel AES si celui-ci devenait vulnérable.

### 3.4.3 – Serpent

Serpent est un algorithme de chiffrement symétrique par bloc inventé par Ross Anderson, Eli Biham and Lars Knudsen. Il chiffre des blocs de 128 bits. Il a été finaliste au concours AES.

Voici le résultat des votes :

- Rijndael : 86 votes
- Serpent : 59 votes

- Twofish : 31 votes
- RC6 : 23 votes
- MARS : 13 votes

Le choix du NIST pour AES s'est donc porté sur Rijndael. Serpent et Rijndael sont similaires. La principale différence est que Rijndael est plus rapide mais Serpent est plus sûr.

### 3.4.4 – Rijndael

Rijndael a été conçu par Joan Daemen et Vincent Rijmen, deux chercheurs de la Belgique, dans le but de devenir un candidat à l'Advanced Encryption Standard (AES) du NIST. Après avoir réussi à se classer dans les six premiers, Rijndael a été choisi le standard en 2000, prenant la place du premier véritable standard de la cryptographie : le DES.

Le chiffrement a une longueur de bloc variable, une longueur de clé variable et un nombre de rounds variables. Par contre, Rijndael version "AES" est restreint à des longueurs de clé de 128, 192 et 256 bits avec une longueur de bloc fixée à 128 bits (en fait, Rijndael supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard).

Trois critères principaux ont été respectés dans sa conception :

- Résistance face à toutes les attaques connues.
- Rapidité du code sur la plus grande variété de plates-formes possible.
- Simplicité dans la conception.

Rijndael (1998) a été fortement influencé par son prédécesseur, l'algorithme Square (1997). Les algorithmes Crypton et Twofish utilisent aussi des opérations de Square. Rijndael se prononce "Raindal"

## 4 – Les fonctions de hachage

Une fonction de hachage est aussi appelée fonction de hachage à sens unique ou "one-way hash function" en anglais. Ce type de fonction est très utilisé en cryptographie, principalement dans le but de réduire la taille des données à traiter par l'algorithme de chiffrement. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée .

Fonctions de hachage usuelles :

- MD4 et MD5 (Message Digest) furent développées par Ron Rivest. MD5 produit des hachés de 128 bits en travaillant les données originales par blocs de 512 bits.
- SHA-1 (Secure Hash Algorithm 1), comme MD5, est basé sur MD4. Il fonctionne également à partir de blocs de 512 bits de données et produit par contre des condensés de 160 bits en sortie. Il nécessite donc plus de ressources que MD5.
- SHA-2 (Secure Hash Algorithm 2) a été publié récemment et est destiné à remplacer SHA-1. Les différences principales résident dans les tailles de hachés possibles : 256, 384 ou 512 bits. Il sera bientôt la nouvelle référence en termes de fonction de hachage.
- RIPEMD-160 (Ripe Message Digest) est la dernière version de l'algorithme RIPEMD. La version précédente produisait des condensés de 128 bits mais présentait des failles de sécurité importantes. La version actuelle reste pour l'instant sûre; elle produit comme son nom l'indique des condensés de 160 bits. Un dernier point la concernant est sa relative gourmandise en termes de ressources et en comparaison avec SHA-1 qui est son principal concurrent.
- Tiger : Tiger est une fonction de hachage cryptographique conçue par Ross Anderson et Eli Biham en 1996. Tiger fournit une empreinte sur 192 bits mais des versions sur 128 et 160 bits existent aussi. Ces versions raccourcies prennent simplement les premiers bits de la signature de 192 bits.

# 5 – Comparatif

## 5.1 – Tableau

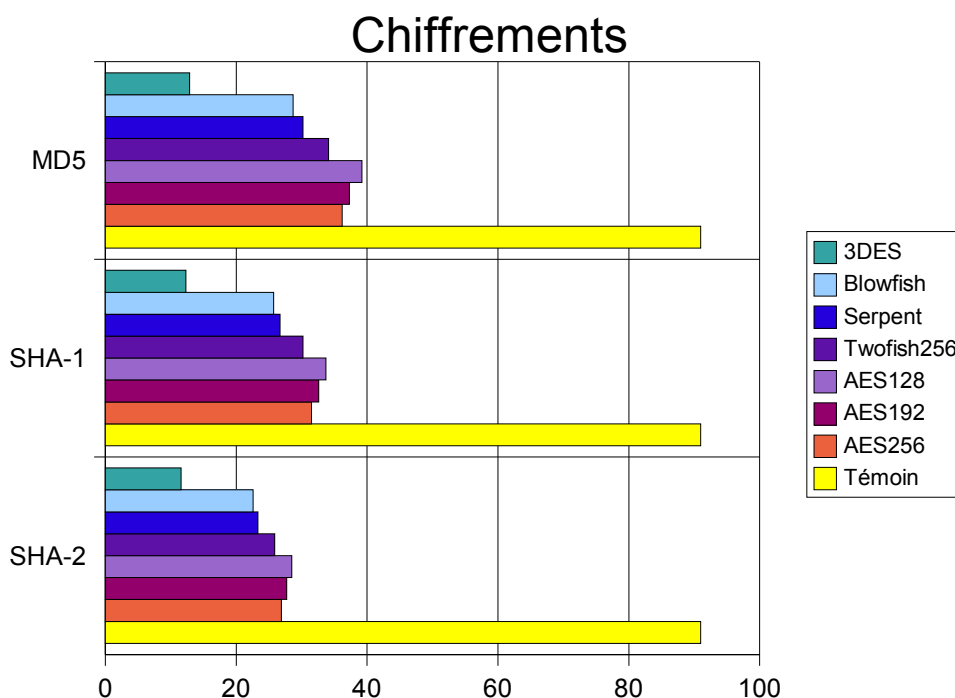
	<i>DES</i>	<i>3DES</i>	<i>BlowFish</i>	<i>TwoFish</i>	<i>Serpent</i>	<i>Rijndael</i>
Date	1976	1978	1993	1996	1997	1998
Type de chiffrement	chiffrement par blocs	chiffrement par blocs	chiffrement par blocs	chiffrement par blocs	chiffrement par blocs	chiffrement par blocs
Taille de blocs	64 bits	64 bits(56+8)	64 bits	128 bits	128 bits	variable
Taille de clés	64 bits	128 à 192 bits	32 à 448 bits	128, 192, 256 bits	128, 192, or 256 bits	128, 192, 256 bits
Sécurité	Faible	Moyenne	Haute	Haute	Haute	Haute

## 5.2 – Performances

Ce comparatif fait l'étude des algorithmes de chiffrement suivants : Blowfish, Des, 3Des, Twofish, Serpent, Rijndael(AES). Chacun de ces algorithmes est associé à trois fonctions de hachage : MD5, SHA-1, SHA-2.

Le témoin indique le débit maximal quand il n' y a aucun chiffrement.

	3DES	Blowfish	Serpent	Twofish256	AES128	AES192	AES256	Témoin
MD5	12,9	28,7	30,2	34,1	39,2	37,3	36,2	91
SHA-1	12,3	25,7	26,7	30,2	33,7	32,6	31,5	91
SHA-2	11,6	22,6	23,3	25,9	28,5	27,7	26,9	91



## 6 – Conclusion

L'algorithme de chiffrement joue un rôle important aussi bien au niveau de la sécurité que des performances. Dans le cas de configurations réseaux importantes, le choix d'un algorithme devient judicieux.

Pour conclure, les algorithmes TwoFish, Serpent et Rijndael conviennent parfaitement, ils sont sûrs et offrent de bonnes performances.

# 7 – Webliographie

<http://www.uqtr.ca/~delisle/Crypto/prives/>

<http://fr.wikipedia.org/>

<http://www.commentcamarche.net>

<http://www.securiteinfo.com>

## 8 – Lexique

**Chiffrement Feistel** : Le chiffrement Feistel est une classe particulière des chiffrements par blocs où le texte est chiffré à partir de la même transformation sur le texte clair dans chaque round. L'avantage est que la fonction de chiffrement et la fonction de déchiffrement sont identiques. Ainsi la fonction n'a pas à être inversible.

**Cryptanalyse** : La cryptanalyse s'oppose, en quelque sorte, à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de s'en passer. Même si on décrit les cryptanalystes comme des « briseurs de codes », il convient de remarquer qu'un algorithme est considéré comme cassé lorsqu'une attaque permet de retrouver la clé en effectuant moins d'opérations que via une attaque par force brute. L'algorithme ainsi cassé ne devient pas inutile pour autant, mais son degré de sécurité, c'est-à-dire le nombre moyen d'opérations nécessaires pour le déchiffrer, s'affaiblit.

**Cryptographie** : La cryptographie est une des disciplines de la cryptologie, s'attachant à protéger des messages (assurant confidentialité et/ou authenticité), en s'aidant souvent de *secrets* ou clés. Elle est utilisée depuis l'antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, n'ont que quelques dizaines d'années d'existence.

**Cryptologie** : La cryptologie, étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie — l'écriture secrète — et la cryptanalyse — l'analyse de cette dernière.

**MARS** : MARS est un bloc de chiffre de clé partage (symétrique) créé par IBM comme algorithme pour le standard Advanced Encryption Standard (AES). MARS prend en charge les blocs de 128-bit et les clés de dimensions variables. MARS est unique car il associe toutes les techniques de chiffrement connues dans un seul produit. Il utilise deux algorithmes séparés, de façon que si une partie de MARS est cassée, le reste des chiffres restera sécurisées et les données seront sauvegardées.

**NIST** : Le National Institute of Standards and Technology (Institut national des standards et de la technologie), aussi connu sous le sigle NIST, est une agence du département américain du commerce. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie.

**NSA** : La NSA (National Security Agency, ou Agence de sécurité nationale, en français) est un organisme gouvernemental des États-Unis, responsable de la collecte et de l'analyse de toutes formes de communications, aussi bien militaires et gouvernementales que commerciales ou même personnelles, par radiodiffusion, par Internet ou par tout autre mode de transmission.

**Serpent** : Serpent a été créée par Ross Anderson, Eli Biham et Lars Knudsen pour être un Advanced Encryption Standard. Serpent a été sélectionné comme l'un des cinq finalistes dans le concours AES où Rijndael a été sélectionné comme standard AES. Serpent est plus rapide que DES et utilise un algorithme plus simple et plus sécurisé. Il n'existe aucune attaque connue qui a réussi à casser cet algorithme.

**VPN** : (Virtual Private Network ou Réseau Privé Virtuel), un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

Le terme de « tunnel » est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer les données à l'entrée et serveur VPN (ou plus généralement serveur d'accès distant) l'élément

déchiffrant les données en sortie. De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au système pare-feu de son réseau local qui va transmettre la réponse de façon chiffrée. À la réception sur le proxy de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur