

Accès distant

Management des serveurs et clients
& Outils de client léger

Les usa



- Agir à distance
 - Gérer les serveurs
 - Dépanner les utilisateurs et les postes
- Interaction entre bureaux
 - (travail d'équipe)
- Terminal server & clients légers

Les protocoles & Les outils

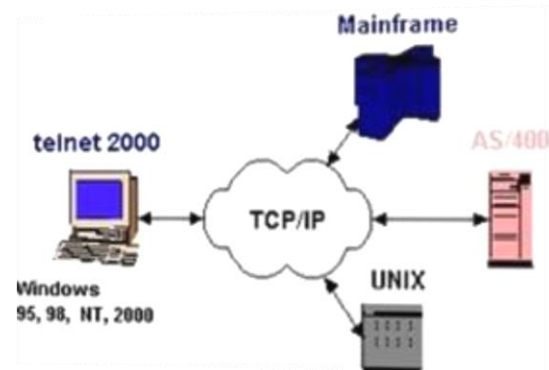
- Telnet
- SSH
- RDP
- RFB (VNC)
- Open SSH / Putty
- TeamViewer
- DameWare
- Connexion bureau a distance

Terminal Server & Clients légers

Telnet

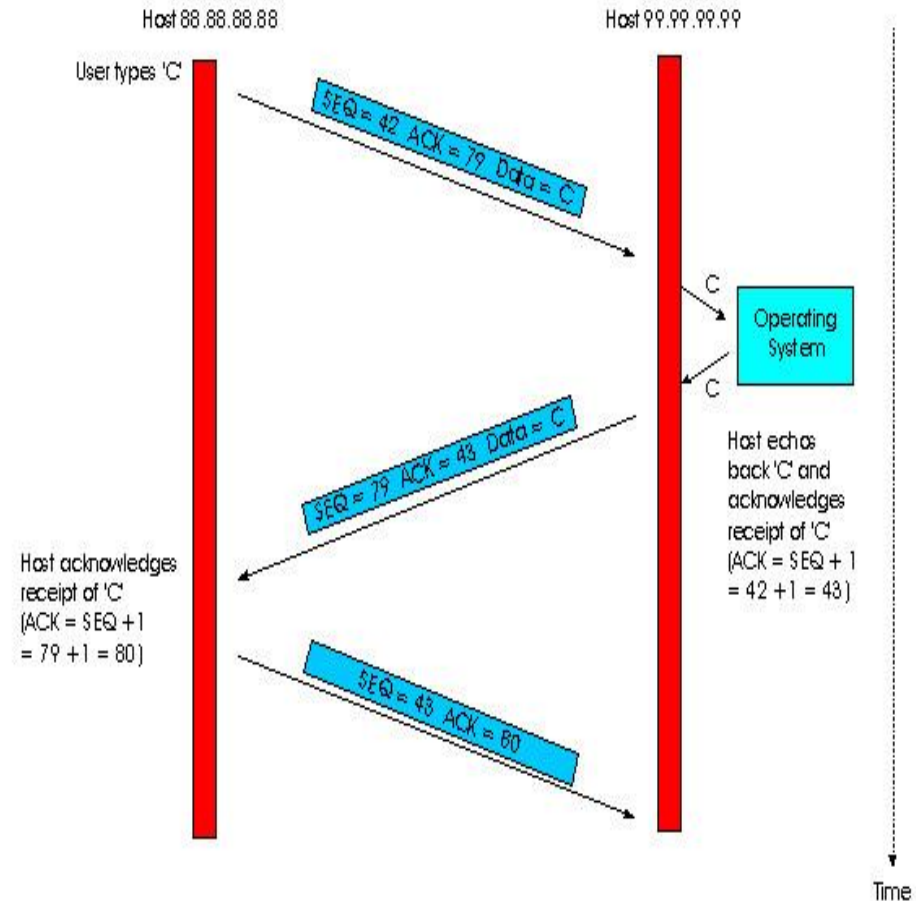
- Protocole standard d'Internet qui permet l'interfaçage de terminaux et d'applications à travers Internet.
- Aux débuts d'Internet, le réseau (ARPANET) était composé de machines dont les configurations étaient très peu homogènes (claviers, jeux de caractères, résolutions, longueur des lignes d'affichage).
- Au lieu de créer des adaptateurs pour chaque type de terminaux, il a été décidé de mettre au point une interface standard, appelée **NVT** (*Network Virtual Terminal* : *Terminal réseau virtuel*,

- *crée une abstraction du terminal, permettant à n'importe quel hôte (client ou serveur) de communiquer avec un autre sans connaître ses caractéristiques*



Telnet et TCP

- Telnet s'appuie sur une connexion [TCP](#)
- Pour envoyer des données au format [ASCII](#) codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet.
- En tant que serveur, ce protocole est assigné au [port 23](#).
- FTP, SMTP, POP3, ...s'appuient sur Telnet



- système orienté communication, bi-directionnel (half-duplex), codé sur 8 bits
- facile à mettre en oeuvre.

- Les spécifications de Telnet ne mentionnent pas d'authentification
 - Telnet est totalement séparé des applications qui l'utilisent (le protocole FTP définit une séquence d'authentification au-dessus de Telnet).
- Protocole de transfert de données non sûr, les données circulent en clair sur le réseau (de manière non chiffrée).

1 Propriétés de Telnet (Ordinateur local)

Nom du service : TlnSvr
 Nom affiché : Telnet
 Description : Permet à un utilisateur système et d'exécuter
 Chemin d'accès des fichiers exécutables : C:\WINDOWS\system32\tlntsvr.exe
 Type de démarrage : Manuel
 Statut du service : Démarré

2 Réseaux - Serveurs (13)
 Analyse réseau (1)
 Yale
 Bande passante (1)
 NetWorx
 Client Telnet-SSH
 KiTTY (PuTTY)

3 KITT Configuration

Category:
 Session
 Logging
 Terminal
 Keyboard
 Bell
 Features
 Window
 Appearance
 Background
 Behaviour
 Translation
 Selection
 Colours
 Hyperlinks
 Connection

Basic options for your KITT session

Specify the destination you want to connect to

Host Name (or IP address) Port
 192.168.0.8 23

Connection type:
 Raw Telnet Plugin SSH Serial

Load, save or delete a session

Saved Sessions

Default Settings SSH

4 192.168.0.8 - KITT

Welcome to Microsoft Telnet Service

Login: administrateur
 password:

Bienvenue
 Microsoft Telnet Server.
 C:\Documents and Settings\Administrateur>

5 Broadcom NetXtreme Gigabit Ethernet Driver - Wireshark

Filter: tcp.stream eq 83

No.	Time	Source	Destination	Protocol	Info
523	80.471738	192.168.0.7	192.168.0.8	TCP	53887 > telnet [SYN] Seq=0 win=8192 Len=0 MSS=1460 wS=2
524	80.477162	192.168.0.8	192.168.0.7	TCP	telnet > 53887 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MS
525	80.477408	192.168.0.7	192.168.0.8	TCP	53887 > telnet [ACK] Seq=1 Ack=1 win=65700 Len=0
526	80.503181	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
529	80.617825	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
530	80.619017	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
531	80.619110	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
532	80.619166	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
533	80.619222	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
534	80.620397	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
535	80.620759	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
536	80.620998	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
537	80.621066	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
538	80.621835	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
539	80.621901	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
548	80.827934	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...
576	82.628389	192.168.0.8	192.168.0.7	TELNET	Telnet Data ...
577	82.828292	192.168.0.7	192.168.0.8	TELNET	Telnet Data ...

Follow TCP Stream

Stream Content

```

.....SFUTLNTVER.SFUTLNTMODE.....welcome to Microsoft
Telnet Service

Login: aaddmiinniisstrraatteeurr

password: admin
.....XTERM.....XTERM..

*****
Bienvenue . Microsoft Telnet Server.
*****
C:\Documents and Settings\Administrateur>

```

End Save As Print Entire conversation (459 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Plus d'info sur : <http://www.commentcamarche.net/contents/internet/telnet.php3>

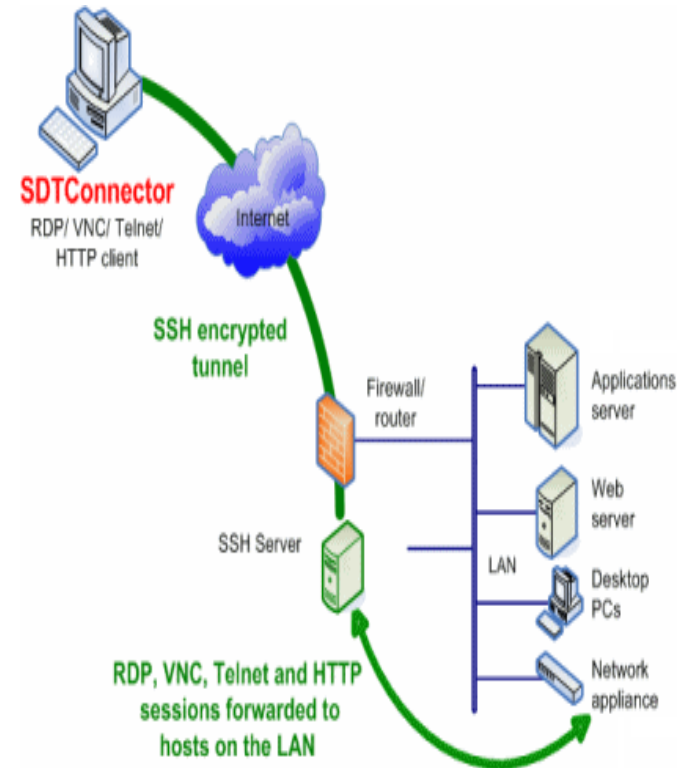
SSH

- **Secure Shell (SSH)** défini en janvier 2006 est à la fois un [programme informatique](#) et un [protocole de communication](#) sécurisé.
- Il est particulièrement utilisé pour ouvrir un [shell](#) sur un ordinateur distant.
 - *Principalement pour les stations [Linux](#) et [Unix](#).*
 - *Mais aussi très utilisé sur le matériel actif – switches et routeurs*
- Habituellement le protocole SSH utilise le [port TCP](#) 22 mais on peut utiliser le port 443 ou autre .

SSH - Tunnel

- Le protocole de connexion impose un échange de clés de chiffrement en début de connexion.
- SSH peut également être utilisé pour transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel.
 - Par la suite toutes les trames sont chiffrées, impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
- *Cette méthode est couramment utilisée afin de sécuriser une connexion qui ne l'est pas (par exemple le protocole email POP3) en la faisant transférer par le biais du tunnel chiffré SSH.*

❖ *Note : rien n'empêche de faire plusieurs sauts entre consoles SSH, c'est-à-dire ouvrir une console sur un serveur, puis, de là, en ouvrir une autre sur un autre serveur.*



Open SSH

- OpenSSH est une version **LIBRE** du protocole SSH de connexion réseau utilisée par les utilisateurs techniques de l'Internet.
- Les utilisateurs de telnet et ftp ne réalisent pas que leur mot de passe est transmis non chiffré à travers l'Internet.
- OpenSSH chiffre tout le trafic (mots de passe inclus) de façon à déjouer les écoutes réseau, les prises de contrôle de connexion, et autres attaques réseaux.
- OpenSSH fournit des possibilités de création de tunnels sécurisés, plusieurs méthodes d'authentification et supporte toutes les versions SSH.
- La suite logicielle OpenSSH remplace rlogin et telnet avec le programme [ssh](#), rcp avec le programme [scp](#) et ftp avec le programme [sftp](#).
- D'autres utilitaires tels que [ssh-add](#), [ssh-agent](#), [ssh-keysign](#), [ssh-keyscan](#), [ssh-keygen](#), et [sftp-server](#) sont inclus
- L'installation d'OpenSSH est extrêmement simple : `sudo apt-get install openssh-server & sudo apt-get install openssh-client`

Fichier Édition Affichage Aller à Signets Aide

Précédent Suivant

Arborescence

- Système de fichiers
- sftp sur 192.168.0.10
 - bin
 - boot
 - cdrom
 - dev
 - etc
 - home
 - initrd.img
 - ssl

ssh_config 1,6 Kio

sshd_config 2,3 Kio

ssh_host_dsa_key 668 octets

ssh_host_dsa_key.pub 609 octets

ssh_host_rsa_key 1,6 Kio

ssh_host_rsa_key.pub 401 octets

sshd_config

Package generated configuration file
See the sshd_config(5) manpage for details

What ports, IPs and protocols we listen for

Port 443

port 22

#ListenAddress

#ListenAddress 0.0.0.0

Protocol 2

HostKeys for protocol

HostKey /etc/ssh/ssh_host_dsa_key

HostKey /etc/ssh/ssh_host_rsa_key

#Privilege Separation is

Connexion au serveur

Type de service : SSH

Serveur : 192.168.0.8

Informations personnelles :

Port : 443

Dossier : /

Nom d'utilisateur : sophie

Ajouter un signal

Nom du signal :

Aide Annuler Se connecter

```
ig@ig-VirtualBox: ~
Fichier Édition Affichage Rechercher Terminal Aide
ig@ig-VirtualBox:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a3:59:bc
          inet addr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fea3:59bc/64 Scope:Lien
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

85	8.871937	192.168.0.10	192.168.0.7	SSL	Continuation Data
86	8.888146	192.168.0.7	192.168.0.10	TCP	[TCP segment of a reassembled PDU]
87	8.889356	192.168.0.10	192.168.0.7	SSL	Continuation Data
88	9.084839	192.168.0.7	192.168.0.10	TCP	56065 > https [ACK] Seq=1073 Ack=1425 win=16425 Len=0
105	10.830925	192.168.0.7	192.168.0.10	TCP	[TCP segment of a reassembled PDU]
106	10.834197	192.168.0.10	192.168.0.7	SSL	Continuation Data
107	10.834299	192.168.0.7	192.168.0.10	TCP	[TCP segment of a reassembled PDU]
108	10.836434	192.168.0.10	192.168.0.7	SSL	Continuation Data
109	10.836518	192.168.0.7	192.168.0.10	TCP	[TCP segment of a reassembled PDU]
110	10.838076	192.168.0.10	192.168.0.7	SSL	Continuation Data
111	10.842664	192.168.0.7	192.168.0.10	TCP	[TCP segment of a reassembled PDU]
112	10.850001	192.168.0.10	192.168.0.7	SSL	Continuation Data

Frame 105 (102 bytes on wire, 102 bytes captured)

Ethernet II, Src: QuantaCo_94:ef:c6 (00:1b:24:94:ef:c6), Dst: AsustekC_1a:93:a5 (00:0c:6e:1a:93:a5)

Internet Protocol, Src: 192.168.0.7 (192.168.0.7), Dst: 192.168.0.10 (192.168.0.10)

Transmission Control Protocol, Src Port: 56065 (56065), Dst Port: https (443), Seq: 1073, Ack: 1425, Len: 48

Follow TCP Stream

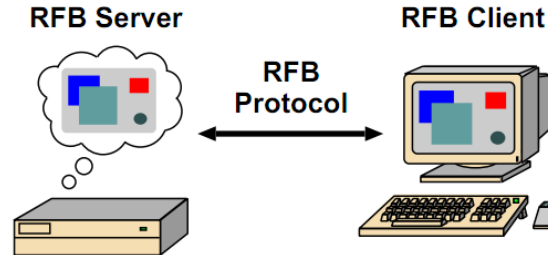
Stream Content

```
-N.0.a.....6..k7.....}.....9w....Py.....
Uwh.1.
F8x=\.2.0.q.....\..p.>.^.(.....o&...xk....j.l&.=s.T-.rNo.aL.#)..G.....
{I.3.....e.....S.r8..p-n..ew&. |.p.....J..Tp.^
{.y.....).3.a.^.....r.E....._F.....=..qC..UO.4.s.h.z?.....K.....>...t.D.m.S&
.V.....d.....ZV.....X...2.....V.....\.....$.X...
..\......7r.R..[.A..C..
..7.....JrXZ:..:;<.....[.%..vP..j.....'.....]...X/".....^.[.....9;..Tlx.FJ2].
```

Modif du fichier de config sur le serveur pour écouter sur le port 443

RFB Remote Frame Buffer

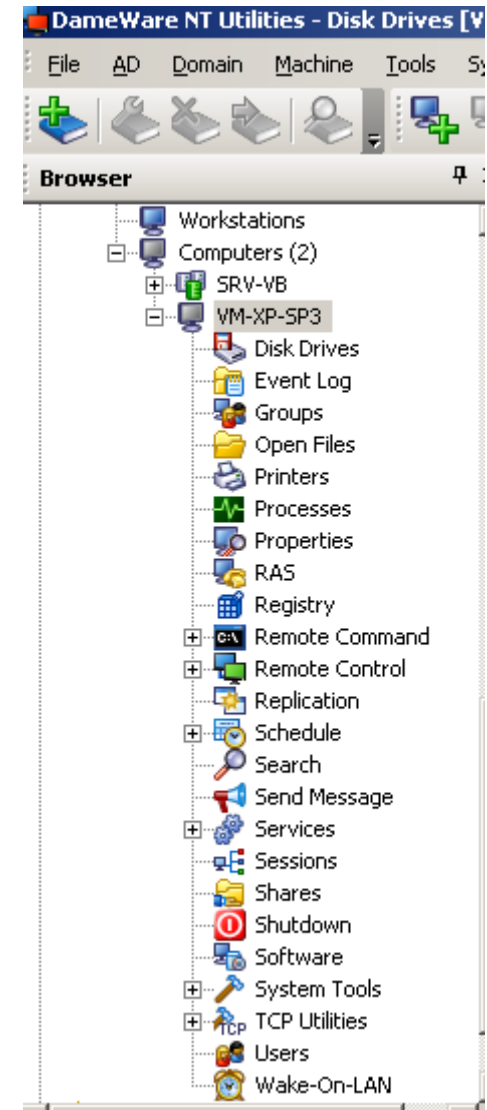
- RFB est un protocole simple pour l'accès à distance aux interfaces graphiques des utilisateurs, utilisé dans le système d'affichage distant VNC (Virtual Network Computing).
 - Le point de terminaison distant où se trouve le poste qui prend la main (c.-à l'écran plus clavier et / ou pointeur) est appelé le client RFB ou spectateur.
 - Inversement l'utilisateur associé est le serveur



- Le logiciel [iTALC](#) de gestion de salle de classe utilise ce protocole pour capturer les écrans des postes "élèves" par le poste "maître".
- RFB utilise le port [5900](#) UDP/TCP (VNC server)

DameWare

- **Avantages :**
 - gestion des serveurs, des clients et des utilisateurs au sein d'un programme
 - Gestion de l'AD à distance
 - Exchange 2000/5.5
 - Terminal Services/Citrix support
 - Pour les ordinateurs à distance tout est intégré (déploiement à distance)
- **Collaborateurs du Help Desk**
 - Réinitialisation des mots de passe oubliés
 - Contrôle à distance utilisateurs et clients
 - Inventaire des logiciels et du hardware des clients et des serveurs
 - Fichiers ouverts : couper la connexion aux données dont l'accès est bloqué, même si les données ont été mises à disposition
 - Processus – fermer les applications qui ne réagissent plus
- **Administrateurs du back office**
 - Liste des événements peut être lue et vidée à distance
 - Des services peuvent être entamés et terminés, qu'il s'agisse de client ou de serveurs...depuis votre bureau
 - Administration complète d'utilisateurs, de groupes (locale et globale), GPO's, OU's
 - Redémarrer les postes clients et serveurs à distance
 - « Wake-on-Lan », exécution des applications à distance, redémarrage et arrêt seront soutenus... à distance



Démo

TeamViewer

.....
Constatez vous-même pourquoi 100 millions d'utilisateurs dans le monde misent sur TeamViewer et sa flexibilité.
.....

- ✓ Assistance spontanée
- ✓ Maintenance à distance des ordinateurs sans surveillance (serveurs)
- ✓ Présentations en ligne, négociations commerciales par exemple
- ✓ Formations en ligne
- ✓ Travail en équipe
- ✓ Bureau à domicile
- ✓ Transfert de fichiers via Internet
- ✓ VPN



La solution "Tout en un" pour toute application

Contrairement aux tendances du marché, TeamViewer intègre en une seule application extrêmement abordable assistance spontanée, maintenance à distance, présentations, formations en ligne, travail en équipe, VPN ...etc.



Fonctionnement optimal, même à travers les pare-feu

Les problèmes majeurs qui surviennent lors de l'utilisation de logiciels de commande à distance sont généralement causés par des pare-feu, des ports verrouillés ou des routeurs NAT pour des adresses IP locales. Avec TeamViewer, c'est du passé ! TeamViewer trouve votre partenaire, même à travers les pare-feu.



Standards de sécurité maximaux

Avec TeamViewer, la maintenance à distance est parfaitement sécurisée. Vos connexions transitent par des canaux de données sécurisés avec échange de clé RSA 1024-bit et codage de session AES 256-bit.



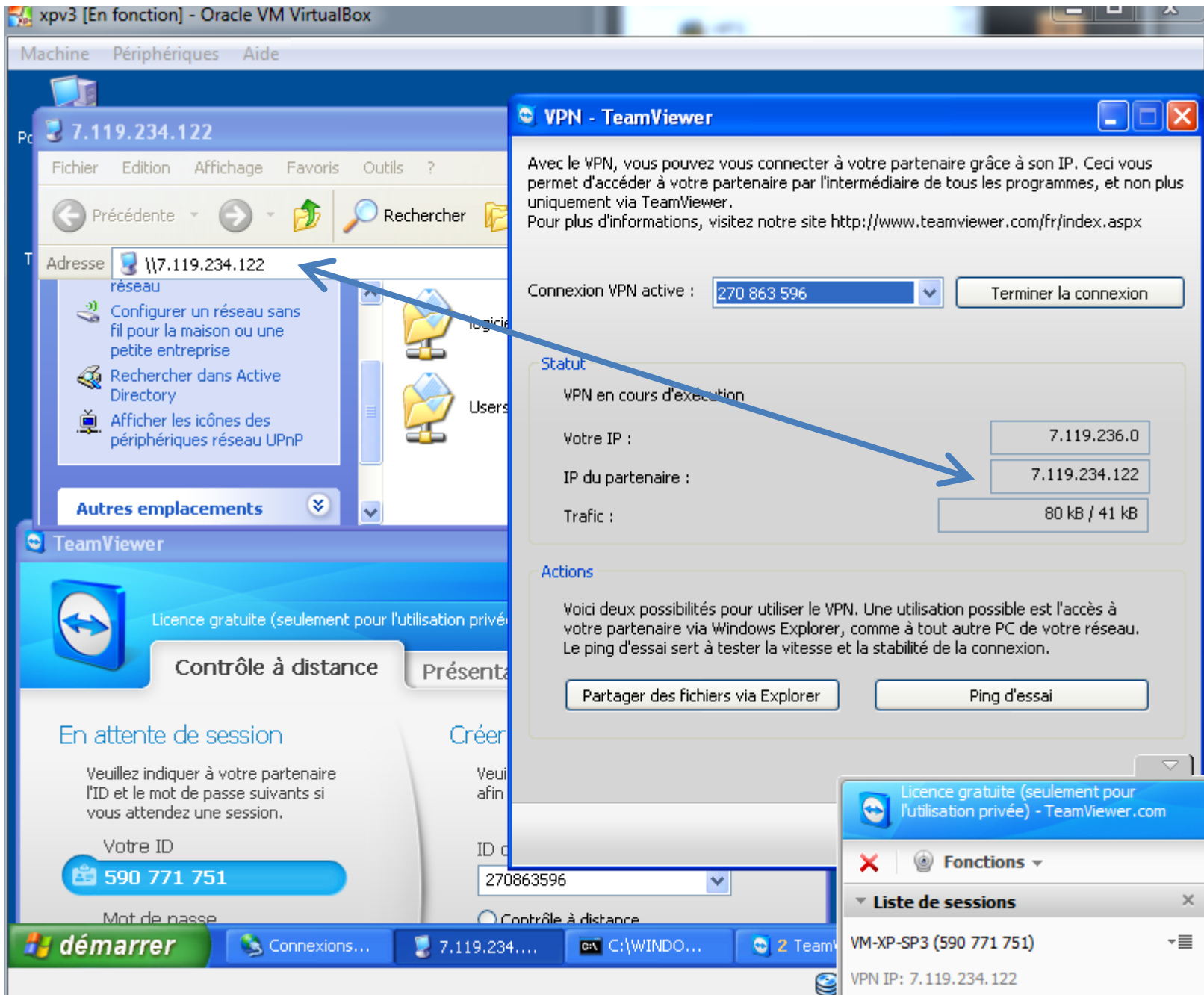
Un prix plus que compétitif

Le prix de TeamViewer défie toute concurrence. TeamViewer est vendu comme ensemble logiciel complet autonome. Il ne donne lieu à aucun frais mensuel ou charges masquées comme des contrats de maintenance.



Installation et utilisation ultra-simples !

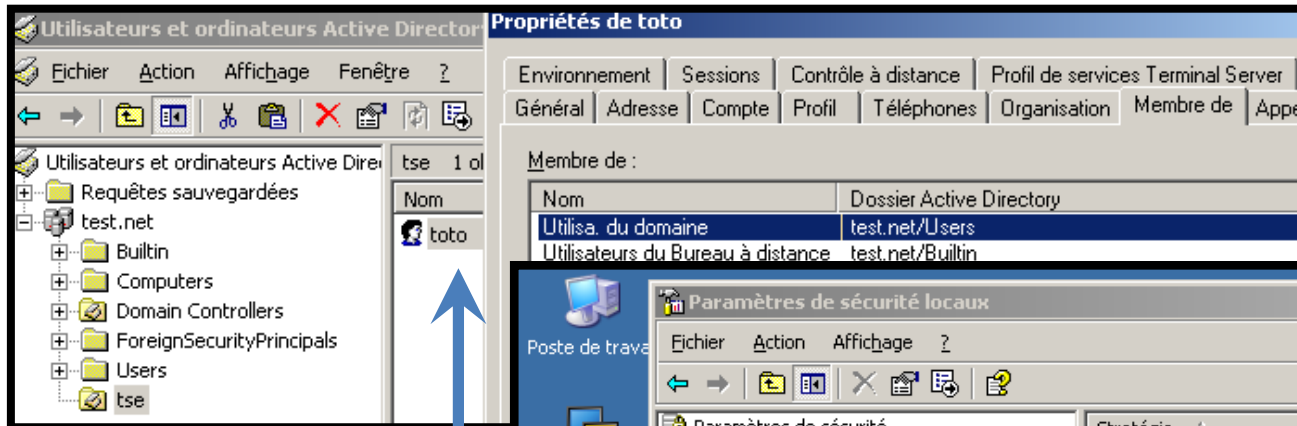
Du côté client, aucune installation ni aucun droit d'administrateur ne sont nécessaires ; votre client exécute simplement un petit programme, et c'est parti !



RDP Remote Desktop

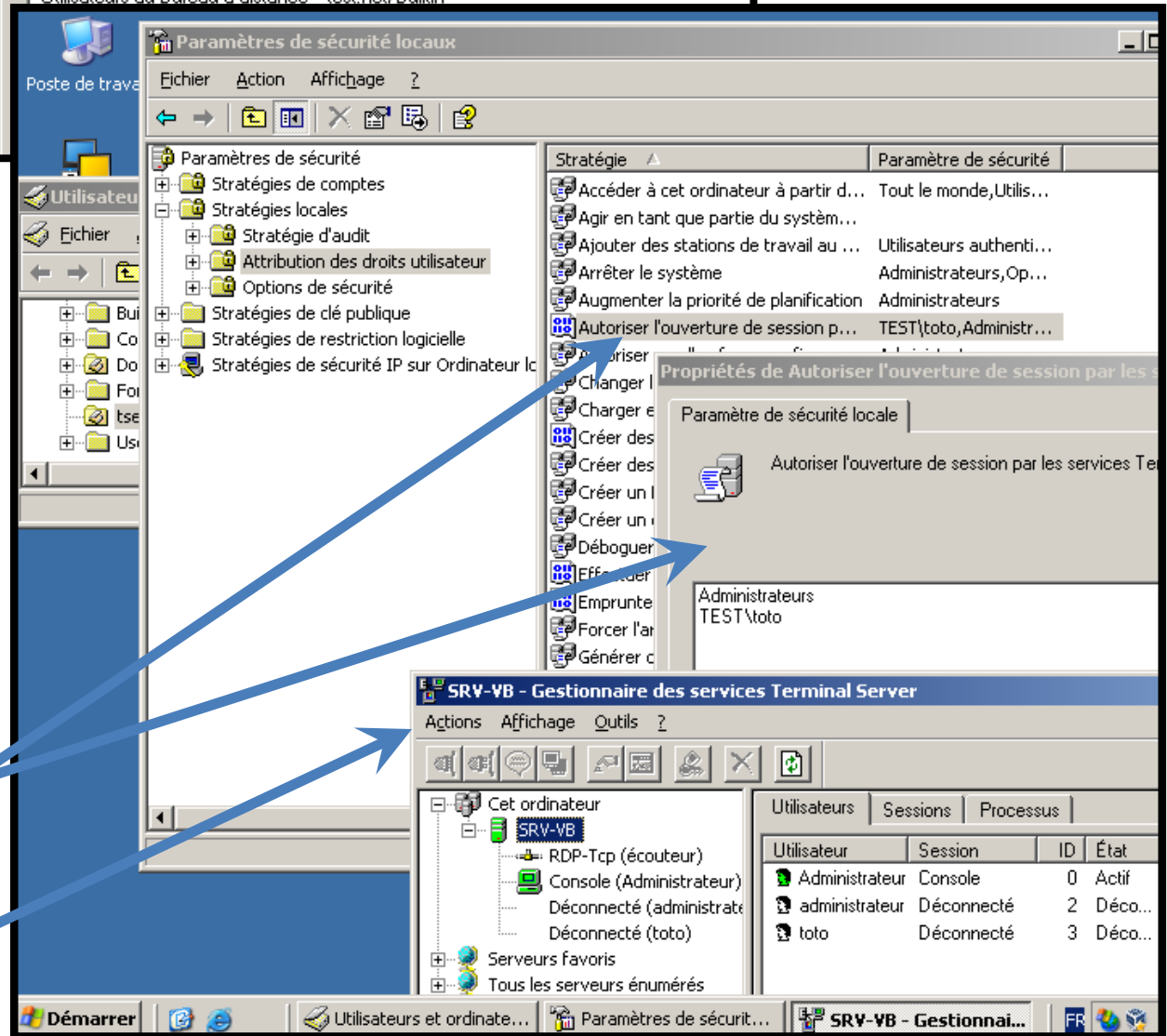
Protocol

- **RDP** est un protocole qui permet à un utilisateur de se connecter sur un serveur faisant tourner [Microsoft Terminal Services](#).
- Des clients existent pour la quasi-totalité des versions de Windows, et pour d'autres systèmes d'exploitation, comme [Linux](#).
- Le serveur écoute par défaut sur le port TCP 3389.
 - Basé sur le protocole [ITU T.share](#), la première version de RDP a été introduite avec Terminal Services dans [Windows NT 4.0 Server](#),
 - La version 5.0, introduite avec [Windows 2000 Server](#), ajoute le support de nombreuses fonctionnalités, support de l'impression sur les imprimantes locales, une amélioration de l'utilisation de la bande passante réseau.
 - La version 5.1, introduite avec [Windows XP Professionnel](#), inclut le support du son ainsi que des couleurs 24-bits.
 - La version 5.2, introduite avec [Windows Server 2003](#), inclut le support pour le mappage de ressources locales.
 - [Windows Server 2008](#) voit apparaître de nouvelles fonctions de RDP qui passe en version 6.1 :
 - passerelle TS,
 - applications distantes,
 - authentification unique,
 - driver universel d'impression.
 - Ces nouvelles fonctions nécessitent également que le poste client dispose du protocole 6.1 (Vista SP1, XP SP3).

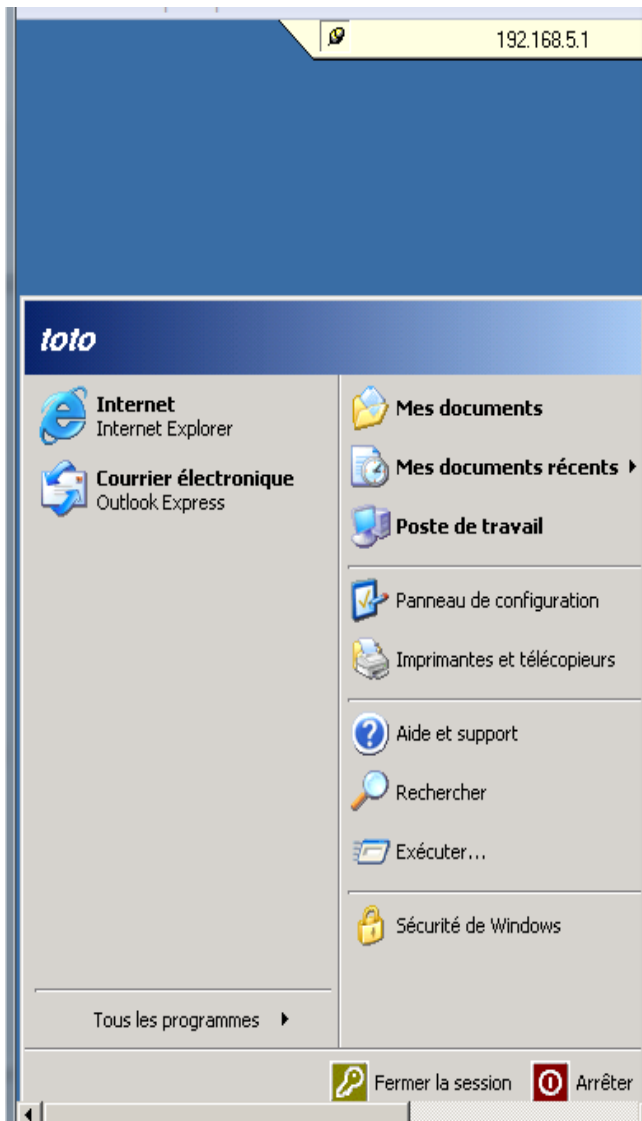


L'installation de TSE nécessite quelques réglages

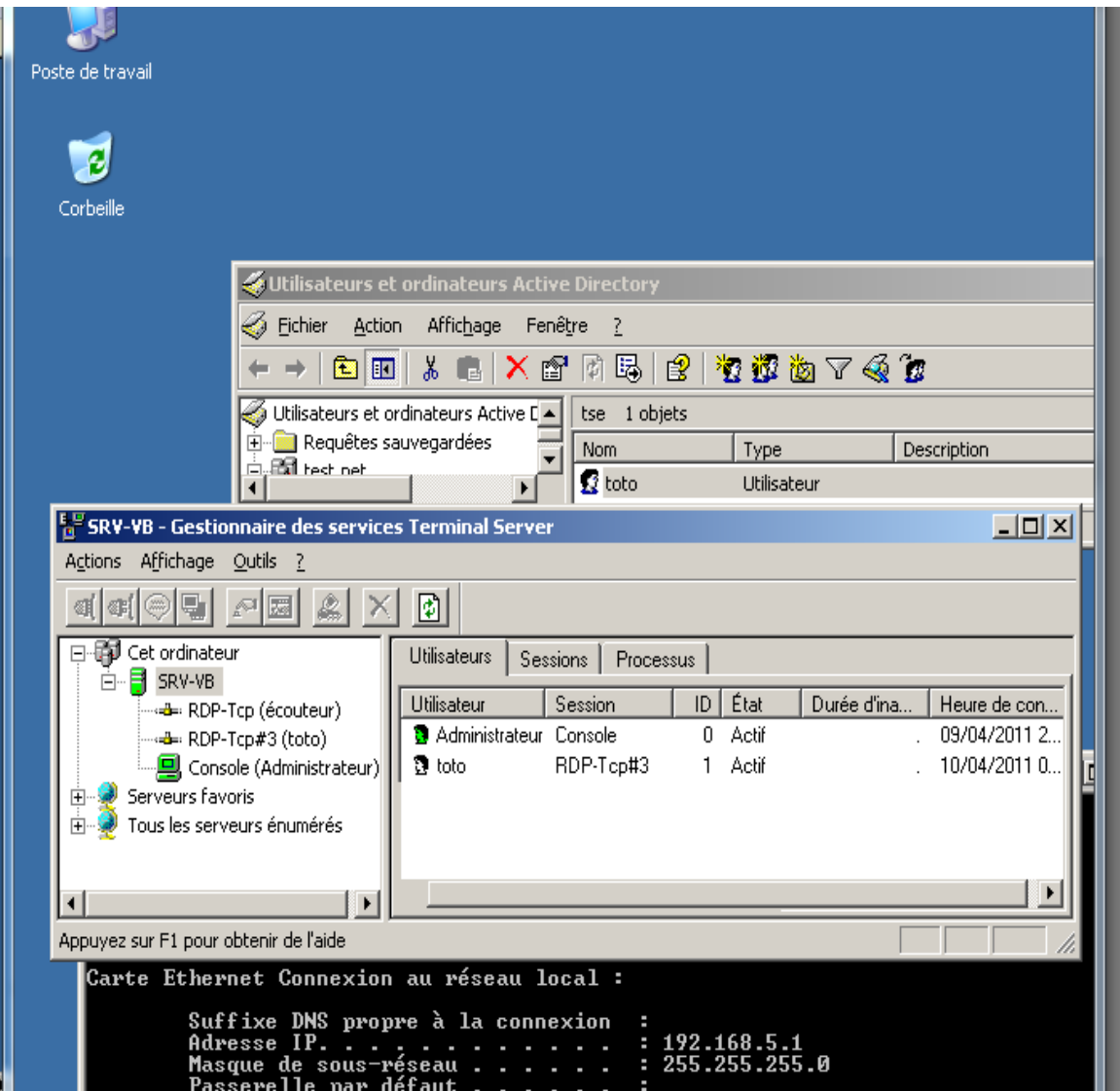
- Ajouter d'abord le rôle Terminal Server
- Puis créer vos utilisateurs, et UO
- Aller dans les stratégies locales (secpol.msc)
- Utiliser le gestionnaire des services TS



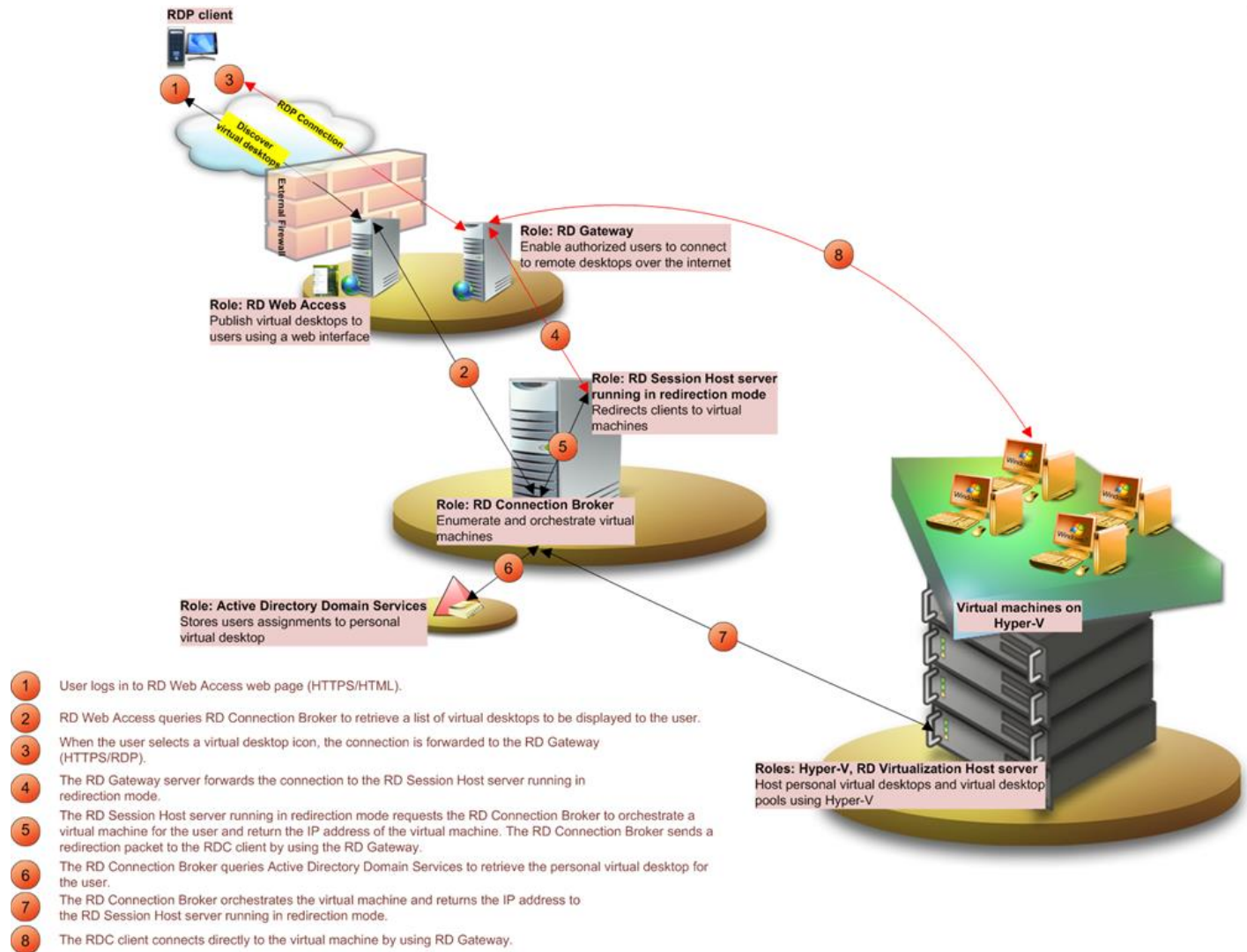
Le client



Le serveur



RDS Remote desktop services



RDS Remote desktop services

- **Remote Desktop Session Host:** Le serveur hôte, qui va stocker les applications (RemoteApp) et bureaux virtuels (Desktop Connection).
- **Remote Desktop Virtualization Host:** Permet aux utilisateurs d'utiliser des RemoteApp et des bureaux virtuels stockés sur des VM. Ce rôle nécessite l'installation d'Hyper-V sur le serveur.
- **Remote Desktop Licensing:** Comme sous Citrix, un serveur de licence pour gérer l'accès au serveur.
- **Remote Desktop Connection Broker:** Permet de faire du Load-balancing entre deux serveurs Session Host.
- **Remote Desktop Gateway:** Permet d'accéder à votre environnement Remote Desktop depuis internet (serveur à placer en DMZ).
- **Remote Desktop Web Access:** Permet aux utilisateurs d'accéder aux RemoteApp et Desktop Connection depuis le menu "Démarrer" de leur Windows 7, ou depuis une interface web.