



جامعة عبد المالك السعدي
Université Abdelmalek Essaadi

Université Abdelmalek Essaadi
Faculté des Sciences et Techniques de
Tanger



FST
Tanger

Administration Réseaux

(services sous Linux)

Pr. Abdelhamid ZOUHAIR


Intitulé du module	Administration Réseaux
Etablissement dont relève le module	Faculté des Sciences et Techniques de Tanger
Filière	Cycle Ingénieur LSI
Semestre d'appartenance du module	S 4

A. U: 2024/2025

Objectif du Module

L'objectif de ce cours est de préparer les étudiants à l'administration d'un réseau d'ordinateurs. L'accent sera mis sur les aspects pratiques et concrets de l'administration d'un réseau d'entreprise pour les systèmes UNIX et Windows /Présenter les différentes services :

- ✂ Serveur FTP, Telnet et SSH
- ✂ Serveur DHCP, Serveur HTTP Apache
- ✂ VPN & OpenVPN
- ✂ Configuration VLAN, VTP et STP
- ✂ Configuration des ACLs
- ✂ Configuration SNMP
- ✂ Serveur NFS et Serveur de fichiers Samba
- ✂ Serveur d'impression
- ✂ ...



Plan

- Serveur FTP, Telnet et SSH
- Serveur HTTP Apache
- VPN & OpenVPN
- Configuration VLAN, VTP et STP
- Configuration des ACLs
- Configuration SNMP
- Serveur NFS et Serveur de fichiers Samba
- Serveur DNS (BIND9)
- Serveur OpenLDAP (Annuaire, authentification et Centralisation des services)
- Serveur d'impression

3

Plan

Serveur FTP

1. Présentation de protocole FTP
2. Description des ports et modes multiples de FTP
3. Installation et manipulation de serveur vsftpd
4. Options de configurations
5. Démarrage de multiples instances de vsftpd
6. Sécurité FTP

4

Modèle OSI: Protocoles

La couche **Application** fournit à ces utilisateurs quelques applications et services généraux que nous allons voir (FTP, Telnet, SSH, ...)

7	Application	FTP, Telnet, HTTP, HTTPS, SMTP, DNS, SSH, POP, IMAP, ...
6	Présentation	SSL, WEP, WPA, Kerberos, TLS
5	Session	Ports, NetBIOS
4	Transport	TCP, UDP
3	Réseau	IPv4, IP v6, IPX, ARP, ICMP
2	Liaison de données	802.11, Wi-Fi, MAC, HDLC, PPP
1	Physique	UTP, Fibre optique, Radio, ...

5

Serveur FTP

01 - Présentation de protocole FTP : Introduction et définition

File Transfer Protocol (protocole de transfert de fichier, ou FTP), est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP.

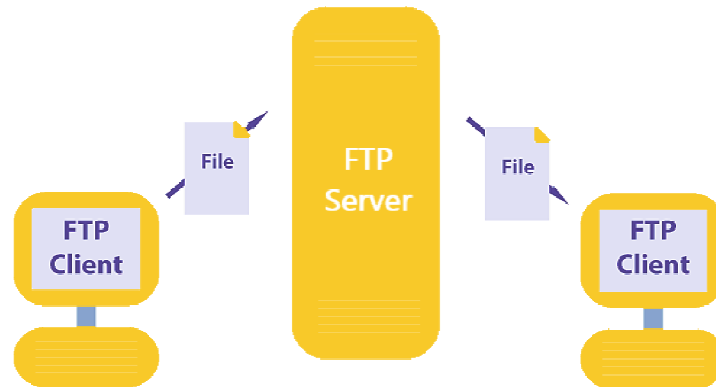
- ✎ Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.
- ✎ La mise en place du protocole FTP date de 1971, date à laquelle un mécanisme de transfert de fichiers (décrit dans le RFC 114) entre les machines du MIT (Massachusetts Institute of Technology) avait été mis au point.
- ✎ Plusieurs RFC viennent compléter cette spécification, comme la RFC 2228 de juin 1997 pour l'ajout d'extensions de sécurité ou la RFC 2428 de septembre 1998 qui ajoute la prise en charge du protocole IPv6 et définit un nouveau type de mode passif.

6

Serveur FTP

01 - Présentation de protocole FTP : Introduction et définition

- En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel, maniable aussi en ligne de commande, lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX.

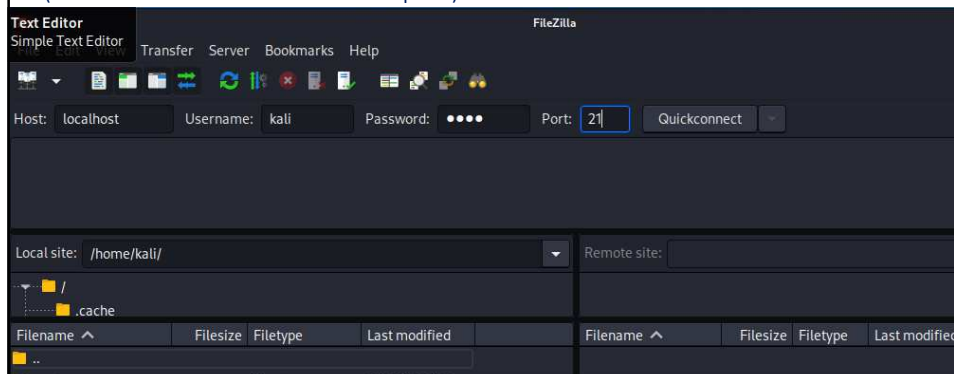


7

Serveur FTP

01 - Présentation de protocole FTP : Introduction et définition

- Ce qui rend FTP non sécurisé, c'est que tout ce qui est envoyé entre le client et le serveur FTP se fait en texte clair. Le protocole FTP a été créé à une époque où la plupart des communications informatiques se faisaient sur des réseaux privés, lignes téléphoniques ou par ligne commutée, où le cryptage n'était pas considéré comme critique.
- Si vous utilisez FTP sur un réseau public, quelqu'un reniflant la ligne n'importe où entre le client et le serveur pourra voir non seulement les données transférées mais aussi le processus d'authentification (informations de connexion et de mot de passe).



Serveur FTP

01 - Présentation de protocole FTP : Introduction et définition

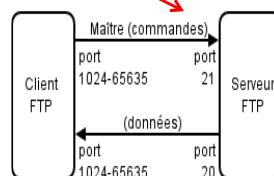
- ✎ FTP n'est pas bon pour partager des fichiers en privé (utilisez des commandes SSH telles que sftp, scp ou rsync si vous avez besoin de transferts de fichiers privés et cryptés). Cependant, si vous partagez des documents publics, des référentiels de logiciels open source ou d'autres données librement disponibles, FTP est un bon choix.
- ✎ Quel que soit le système d'exploitation que les utilisateurs utilisent, ils disposent sûrement d'une application de transfert de fichiers FTP pour obtenir les fichiers que vous proposez à partir de votre serveur FTP.
- ✎ Lorsque les utilisateurs s'authentifient auprès d'un serveur FTP sous Linux, leurs noms d'utilisateur et mots de passe sont authentifiés par rapport aux comptes d'utilisateur et mots de passe Linux standard. Il existe également un compte spécial non authentifié utilisé par le serveur FTP appelé **anonymous**. Le compte anonymous est accessible à tous car il ne nécessite pas de mot de passe valide.
- ✎ En fait, le terme serveur FTP **anonyme** est souvent utilisé pour décrire un serveur FTP public qui ne nécessite pas (ni même n'autorise) l'authentification d'un compte utilisateur légitime.



Serveur FTP

02 - Description des ports et modes multiples de FTP

- ✎ Après la phase d'authentification (sur le port de contrôle, port TCP 21), une deuxième connexion est établie entre le client et le serveur. FTP prend en charge les types de connexion actifs et passifs.

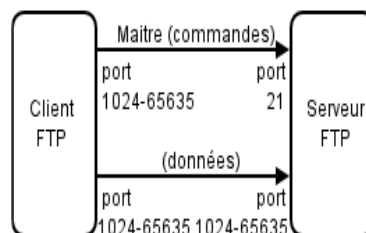


- ✎ En mode actif, c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données. Ainsi, pour que l'échange des données puisse se faire, le serveur FTP initialisera la connexion de son port de données (port 20) vers le port spécifié par le client.
- ✎ Le client devra alors configurer son pare-feu pour autoriser les nouvelles connexions entrantes afin que l'échange des données se fasse.

Serveur FTP

02 - Description des ports et modes multiples de FTP

- En mode passif, le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client. En cas de présence d'un pare-feu devant le serveur, celui-ci devra être configuré pour autoriser la connexion de données.
- L'avantage de ce mode est que le serveur FTP n'initialise aucune connexion. Ce mode fonctionne sans problème avec des clients derrière une passerelle NAT. Dans les nouvelles implémentations, le client initialise et communique directement par le port 21 du serveur ; cela permet de simplifier les configurations des pare-feu serveur.

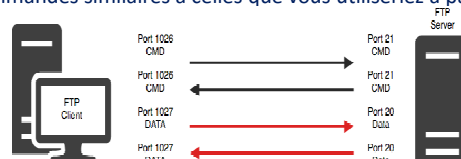


11

Serveur FTP

02 - Description des ports et modes multiples de FTP

- De nombreux navigateurs prennent en charge le mode FTP passif afin que si le client dispose d'un pare-feu, il ne bloque pas le port de données que le serveur FTP pourrait utiliser en mode actif.
- La prise en charge du mode passif nécessite un travail supplémentaire sur le pare-feu du serveur pour permettre des connexions aléatoires aux ports supérieurs à 1023 sur le serveur.
- Une fois la connexion établie entre le client et le serveur, le répertoire actuel du client est établi. Pour l'utilisateur anonyme, le répertoire /srv/ftp est le répertoire personnel pour Ubuntu et la plupart des distributions basées sur Debian. L'utilisateur anonyme ne peut pas sortir de la structure du répertoire /var/ftp.
- Si un utilisateur régulier, disons Sami, se connecte au serveur FTP, /home/Sami est le répertoire actuel de Sami, mais ce dernier peut passer à n'importe quelle partie du système de fichiers pour lequel il a l'autorisation.
- Les clients FTP orientés commandes (tels que les commandes lftp et ftp) passent en mode interactif une fois connectés au serveur. À partir de l'invite de commande qui s'affiche, vous pouvez exécuter de nombreuses commandes similaires à celles que vous utiliseriez à partir du shell.

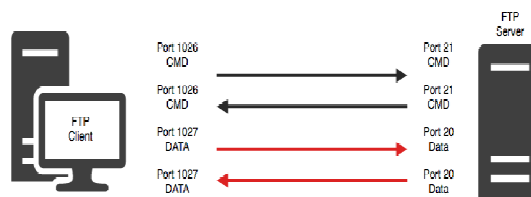


12

Serveur FTP

02 - Description des ports et modes multiples de FTP

- Vous pouvez utiliser `pwd` pour voir votre répertoire actuel, `ls` pour lister le contenu du répertoire et `cd` pour changer de répertoire. Lorsque vous voyez un fichier que vous voulez, vous utilisez les commandes `GET` et `PUT` pour télécharger des fichiers ou les charger sur le serveur, respectivement.
- Avec des outils graphiques pour accéder aux serveurs FTP (comme un navigateur Web), vous tapez l'URL du site que vous souhaitez visiter (comme `ftp://docs.example.com`) dans la zone d'emplacement du navigateur. Si vous n'ajoutez pas de nom d'utilisateur ou de mot de passe, une connexion anonyme est établie et le contenu du répertoire d'accueil du site est affiché. Cliquez sur les liens vers les répertoires pour accéder à ces répertoires. Cliquez sur les liens vers les fichiers pour afficher ou télécharger ces fichiers sur votre système local.



13

Serveur FTP

03 - Installation et manipulation de serveur vsftpd

Installation : FTP Server on Kali Linux

- `vsftpd` étant le serveur FTP choisi par défaut dans les distributions Linux:

- Installation du FTP Server on Kali Linux**

- `sudo apt-get install vsftpd`

```
(kali@kali)-[~]
$ sudo apt-get install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13+b3).
0 upgraded, 0 newly installed, 0 to remove and 1946 not upgraded.
```

- `sudo service vsftpd start`

```
(kali@kali)-[~]
$ sudo service vsftpd start
```

- Edit du fichier de configuration vsftpd

```
(kali@kali)-[~]
$ sudo nano /etc/vsftpd.conf
```



03 - Installation et manipulation de serveur vsftpd

Installation : FTP Server on Kali Linux

- **Anonymous access**

- `sudo nano /etc/vsftpd.conf`
- `=> anonymous_enable=YES`

```
GNU nano 6.2 /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
[ Read 155 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Renlace    ^U Paste      ^I Justify
```



03 - Installation et manipulation de serveur vsftpd

Installation : FTP Server on Kali Linux

- 🔍 check FTP service running or not

```
$ systemctl enable vsftpd.service
Synchronizing state of vsftpd.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
update-rc.d: error: Permission denied

(kali@kali)-[~]
$ sudo systemctl enable vsftpd.service
[sudo] password for kali:
Synchronizing state of vsftpd.service with SysV service script with /lib/syst
emd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service →
/lib/systemd/system/vsftpd.service.

(kali@kali)-[~]
$ ftp localhost
Trying [::1]:21 ...
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:kali): kali
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



03 - Installation et manipulation de serveur vsftpd

Installation : FTP Server on Kali Linux

Une fois l'installation effectuée, pour que le serveur se lance automatiquement au démarrage:

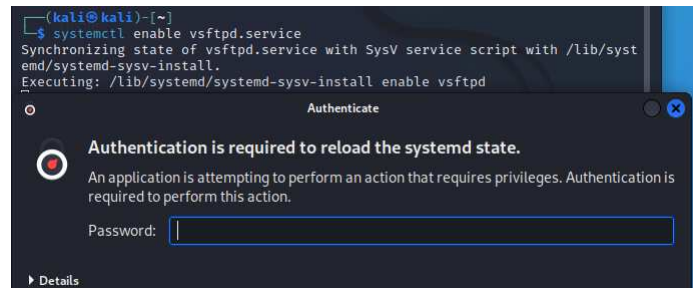
```
# systemctl enable vsftpd.service
```

Pour démarrer et stopper le service, les commandes respectives sont :

```
# systemctl start vsftpd.service
```

```
# systemctl stop vsftpd.service
```

Normalement votre système doit déjà avoir un utilisateur ftp et un groupe ftp (**Anonymous access**):



```
(kali@kali)~$ systemctl enable vsftpd.service
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
```

Authenticate

Authentication is required to reload the systemd state.

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:

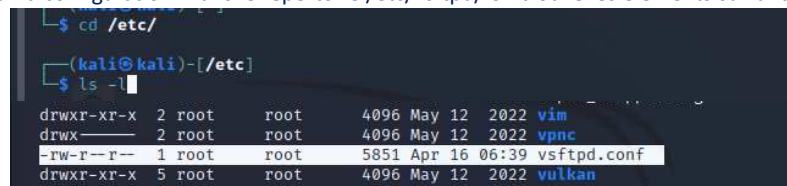
► Details



03 - Installation et manipulation de serveur vsftpd

Configuration : FTP Server on Kali Linux

Pour la configuration. Dans le répertoire /etc/vsftpd/ on trouve les éléments suivants:



```
(kali@kali)~$ cd /etc/
(kali@kali)~/etc$ ls -l
```

drwxr-xr-x	2	root	root	4096	May 12 2022	vim
drwx	2	root	root	4096	May 12 2022	vpnc
-rw-r--r--	1	root	root	5851	Apr 16 06:39	vsftpd.conf
drwxr-xr-x	5	root	root	4096	May 12 2022	vulkan

Le fichier **vsftpd.conf** est le fichier de configuration principale

ftusers et user_list. Ces deux fichiers ont la même vocation : interdire des utilisateurs. En effet, ils contiennent tous les deux une liste d'utilisateurs pour lesquels le serveur FTP refusera toute connexion.

Ftusers est utilisé via PAM dans la configuration par défaut. A la connexion d'un utilisateur, PAM vient lire ce fichier et si l'identifiant de connexion utilisé est dans ce fichier, la connexion est refusée.

```
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
```

Serveur FTP

03 - Installation et manipulation de serveur vsftpd

Configuration : FTP Server on Kali Linux

✎ Ftpusers est utilisé directement par vsftpd. Il peut avoir deux usages : soit les seuls utilisateurs contenus dans ce fichier ont le droit de se connecter, soit l'accès leurs est systématiquement refusé.

➤ Anonymous access

```
root@kali:~# nano /etc/ftpusers
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
```

19

Serveur FTP

03 - Installation et manipulation de serveur vsftpd

Configuration : FTP Server on Kali Linux

✎ ftpusers et user_list. Ces deux fichiers ont la même vocation : interdire des utilisateurs. En effet, ils contiennent tous les deux une liste d'utilisateurs pour lesquels le serveur FTP refusera toute connexion.

```
(kali@kali)~$ sudo nano /etc/vsftpd/user_list/
[sudo] password for kali:
```

```
root@kali:~# nano /etc/vsftpd/user_list/

# This file contains a list of users who cannot use the FTP server
# (violation of the ftpd chrooting, or 'chroot jailing', without this
# file).  The list should not include the root user.
#
# This file has been generated by the vsftpd package.
#
# The following users are listed:
#
# root
# daemon
# bin
# sys
# sync
# games
# man
# lp
# mail
# news
# uucp
# nobody
```

20

Serveur FTP

03 - Installation et manipulation de serveur vsftpd

Configuration : FTP Server on Kali Linux

Après on passe à la configuration du fichier principal vsftpd.conf :

- On écoute sur le port 21/tcp ;
- On **accepte** / **refuse** les utilisateurs anonymes ;
- On accepte les utilisateurs système et les utilisateurs virtuels ;
- Les utilisateurs virtuels sont mappés sur l'utilisateur système "ftp" ;
- /etc/vsftpd/user_list contiendra la liste des utilisateurs refusés (pour lesquels on ne demandera même pas le mot de passe).
- ...
- listen_ipv6=YES
- anonymous_enable=YES
- local_enable=YES
- connect_from_port_20=YES
- connect_from_port_20=YES
- **connect_from_port_20=YES**

```
GNU nano 6.2 /etc/ftpusers
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

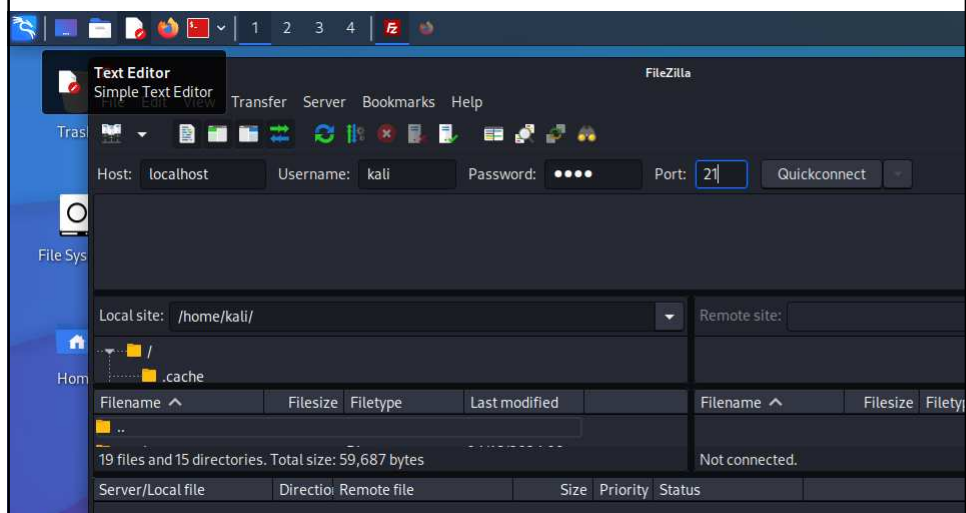
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
```

Client FTP File Zilla

03 - Installation et manipulation de serveur vsftpd

Tests : FTP Server on Kali Linux

Pour accéder au serveur on utilise un outil comme **file zilla** ou via l'invite de commande:



04 - Options de configurations : le démon

✎ Toute configuration de vsftpd est traitée par son fichier de configuration, /etc/vsftpd/vsftpd.conf. Chaque directive apparaît sur sa propre ligne au sein du fichier et suit le format suivant :

✎ <directive>=<value>

✎ La liste ci-dessous représente les directives les plus importantes dans /etc/vsftpd/vsftpd.conf :

- Les directives contrôlant le comportement général du démon vsftpd.
- **listen** - Lorsque cette option est activée, vsftpd est exécuté en mode autonome.
- **listen_ipv6** - Lorsque cette option est activée, vsftpd est exécuté en mode autonome, mais n'écoute que l'interface de connexion (ou socket) IPv6. Cette directive ne peut pas être utilisée de concert avec la directive listen.
- **session_support** - Lorsque cette option est activée, vsftpd tente de maintenir les sessions de connexion pour chaque utilisateur par le biais de modules d'authentification enfichables (ou PAM). Si l'ouverture de sessions n'est pas nécessaire, la désactivation de cette option permet à vsftpd de tourner avec moins de processus et avec des privilèges moindres.

23

04 - Options de configurations : connexion et contrôles d'accès

Les directives qui contrôlent le comportement de connexion et les mécanismes de contrôle d'accès.

- **anonymous_enable** — Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à se connecter. Les noms d'utilisateurs anonymes (dits anonymous) et ftp sont acceptés.
- **banner_file** — Spécifie le fichier contenant le texte affiché lorsqu'une connexion est établie avec le serveur. Cette option écrase tout texte spécifié dans la directive ftpd_banner.
- **ftpd_banner** — Lorsque cette option est activée, la chaîne spécifiée dans cette directive est affichée lorsque qu'une connexion au serveur est établie. Cette option peut être annulée par la directive banner_file.
- **local_enable** — Lorsque cette option est activée, les utilisateurs locaux sont autorisés à se connecter au système.
- **userlist_enable** — Lorsque cette option est activée, les utilisateurs mentionnés dans le fichier spécifiés par la directive userlist_file se voient refuser l'accès. Étant donné que l'accès est refusé avant même que le client ne puisse saisir son mot de passe, les utilisateurs n'ont pas la possibilité de soumettre des mots de passe non-cryptés sur le réseau.
- **userlist_file** — Spécifie le fichier référencé par vsftpd lorsque la directive userlist_enable est activée. La valeur par défaut est /etc/vsftpd.user_list ; cette dernière est créée durant l'installation.
- ...

24

04 - Options de configurations : les utilisateurs anonymes

Les directives qui contrôlent l'accès des utilisateurs anonymes au serveur. Pour utiliser ces options, la valeur de la directive `anonymous_enable` doit être YES.

- **`anon_mkdir_write_enable`** — Lorsque cette option est activée de concert avec la directive `write_enable`, des utilisateurs anonymes sont autorisés à créer de nouveaux répertoires au sein du répertoire parent qui a des permissions en écriture.
- **`anon_root`** — Spécifie le répertoire que vsftpd utilise après la connexion d'un utilisateur anonyme.
- **`anon_upload_enable`** — Lorsque cette option est activée de concert avec la directive `write_enable`, des utilisateurs anonymes sont autorisés à télécharger vers le serveur des fichiers dans un répertoire parent doté de permissions en écriture.
- **`anon_world_readable_only`** — Lorsque cette option est activée, des utilisateurs anonymes sont autorisés à télécharger des fichiers lisibles par tout un chacun.
- **`ftp_username`** — Spécifie le compte de l'utilisateur local (énoncé dans `/etc/passwd`) employé pour l'utilisateur FTP anonyme. Le répertoire personnel spécifié dans `/etc/passwd` pour l'utilisateur est le répertoire `root` de l'utilisateur FTP anonyme.
- **`no_anon_password`** — Lorsque cette option est activée, l'utilisateur anonyme ne doit pas saisir de mot de passe.

25

04 - Options de configurations : les utilisateurs locaux

Les directives caractérisant la manière selon laquelle les utilisateurs locaux ont accès au serveur. Pour utiliser ces options, la directive `local_enable` doit avoir la valeur YES.

- **`chroot_list_enable`** — Lorsque cette option est activée, les utilisateurs locaux énumérés dans le fichier qui est spécifié dans la directive `chroot_list_file`, sont placés dans une prison `chroot` dès qu'ils se connectent. Si cette option est activée de concert avec la directive `chroot_local_user`, les utilisateurs locaux énumérés dans le fichier qui est spécifié dans la directive `chroot_list_file` ne sont pas placés dans une prison `chroot` lors de la connexion.
- **`chroot_list_file`** — Spécifie le fichier contenant une liste des utilisateurs locaux référencés lorsque la valeur de la directive `chroot_list_enable` est YES. La valeur par défaut est `/etc/vsftpd.chroot_list`.
- **`chroot_local_user`** — Lorsque cette option est activée, les utilisateurs locaux opèrent dans l'environnement `chrooté` de leur répertoire personnel après leur connexion.
- **`local_root`** — Spécifie le répertoire que vsftpd utilise après la connexion d'un utilisateur local.
- **`local_umask`** — Spécifie la valeur donnée à `umask` pour la création de fichiers. Notez que la valeur par défaut se présente sous la forme octale (un système numérique en base huit), qui inclut un préfixe "0". Sinon la valeur est traitée comme un entier à base 10.

26

04 - Options de configurations : les répertoires

Les directives ayant un impact sur les répertoires.

- **dirlist_enable** — Lorsque cette option est activée, les utilisateurs sont autorisés à visionner les listes de répertoires.
- **dirmessage_enable** — Lorsque cette option est activée, un message apparaît chaque fois qu'un utilisateur ouvre un répertoire avec un fichier message. Ce message se trouve dans le répertoire qui est ouvert. Le nom de ce fichier est spécifié dans la directive `message_file` et par défaut prend la valeur `.message`.
- **force_dot_files** — Lorsque cette option est activée, les fichiers commençant par un point (.) sont inclus dans les listes de répertoires, à l'exception des fichiers `.` et `...`
- **hide_ids** — Lorsque cette option est activée, toutes les listes de répertoires font apparaître ftp comme l'utilisateur et le groupe de chaque fichier.
- **message_file** — Spécifie le nom du fichier message lorsque la directive `dirmessage_enable` est utilisée. La valeur par défaut est `.message`.
- **text_userdb_names** — Lorsque cette option est activée, des noms d'utilisateurs et noms de groupes test sont utilisés au lieu des entrées UID et GID. L'activation de cette option peut entraîner un ralentissement des performances du serveur.
- **use_localtime** — Lorsque cette option est activée, les listes de répertoires révèlent l'heure locale de l'ordinateur au lieu de l'heure GMT.

27

04 - Options de configurations : le transfert de fichiers

Les directives ayant un impact sur les fichiers.

- **download_enable** — Lorsque cette option est activée, le téléchargement de fichiers est autorisé.
- **chown_uploads** — Lorsque cette option est activée, tous les fichiers téléchargés vers le serveur par des utilisateurs anonymes deviennent la propriété de l'utilisateur spécifié dans la directive `chown_username`.
- **chown_username** — Spécifie la propriété de fichiers téléchargés anonymement vers le serveur si la directive `chown_uploads` est activée. La valeur par défaut est `root`.
- **write_enable** — Lorsque cette option est activée, les commandes FTP permettant de modifier le système de fichiers sont permises, telles que `DELE`, `RNFR` et `STOR`.

28

04 - Options de configurations : journalisation

Les directives ayant un impact sur le comportement de journalisation de vsftpd.

- **dual_log_enable** — Lorsque cette option est activée de concert avec xferlog_enable, vsftpd enregistre deux fichiers simultanément : un journal compatible avec wu-ftp dans le fichier spécifié dans la directive xferlog_file (par défaut /var/log/xferlog) et un fichier journal vsftpd standard spécifié dans la directive vsftpd_log_file (par défaut /var/log/vsftpd.log). La valeur par défaut est NO.
- **log_ftp_protocol** — Lorsque cette option est activée de concert avec xferlog_enable et lorsque xferlog_std_format a pour valeur NO, toutes les commandes et réponses FTP sont journalisées. Cette directive est très utilisée lors d'opérations de débogage.
- **syslog_enable** — Lorsque cette option est activée de concert avec xferlog_enable, toute journalisation normalement enregistrée dans le fichier journal standard vsftpd spécifié dans la directive vsftpd_log_file (par défaut /var/log/vsftpd.log) est envoyée à l'enregistreur du système sous le service FTPD.
- **vsftpd_log_file** — Spécifie le fichier journal vsftpd. Pour que ce fichier soit utilisé, xferlog_enable doit être activée et xferlog_std_format doit avoir pour valeur NO ou, si la valeur de xferlog_std_format est YES, l'activation de dual_log_enable est nécessaire. Il est important de noter ici que si syslog_enable a pour valeur YES, le journal du système est utilisé à la place du fichier spécifié dans cette directive. La valeur par défaut est /var/log/vsftpd.log.

29

04 - Options de configurations : journalisation

Les directives ayant un impact sur le comportement de journalisation de vsftpd.

- **xferlog_enable** — Lorsque cette commande est activée, vsftpd journalise les connexions (seulement au format vsftpd) et les informations de transfert de fichiers dans le fichier journal spécifié dans la directive vsftpd_log_file (par défaut /var/log/vsftpd.log). Si xferlog_std_format a pour valeur YES, les informations de transfert de fichiers sont journalisées mais les connexions elles ne le sont pas et le fichier spécifié dans xferlog_file (par défaut /var/log/xferlog) est utilisé à la place. Il est important de noter ici que les fichiers journaux aussi bien que les formats de journaux sont utilisés si la valeur de dual_log_enable est YES.
- **xferlog_file** — Spécifie le fichier journal compatible avec wu-ftp. Pour que ce fichier soit utilisé, xferlog_enable doit être activé et la valeur de xferlog_std_format doit être YES. Elle est également utilisée si la valeur de dual_log_enable est YES. La valeur par défaut est /var/log/xferlog.
- **xferlog_std_format** — Lorsque cette option est activée de concert avec xferlog_enable, seul un journal de transfert de fichiers compatible avec wu-ftp est enregistré dans le fichier spécifié dans la directive xferlog_file (par défaut /var/log/xferlog). Il est important de noter ici que ce fichier journalise seulement les transferts de fichiers et n'enregistre pas les connexions au serveur.

30

Serveur FTP

04 - Options de configurations : Options réseau

Les directives ayant un impact sur la manière dont vsftpd interagit avec le réseau.

- **accept_timeout** — Spécifie la durée donnée à un client utilisant une connexion passive pour se connecter. La valeur par défaut est 60.
- **connect_from_port_20** Lorsque cette option est activée, vsftpd tourne avec suffisamment de privilèges pour ouvrir le port 20 sur le serveur lors des transferts de données en mode actif. La désactivation de cette option permet à vsftpd de tourner avec moins de privilèges, mais cette option peut-être incompatible avec certains clients FTP.
- **connect_timeout** — Spécifie la durée maximale exprimée en secondes, donnée à un client utilisant un mode actif pour répondre à une connexion de données. La valeur par défaut est 60.
- **data_connection_timeout** — Spécifie la durée maximale exprimée en secondes, pendant laquelle les transferts de données peuvent s'arrêter. Une fois cette durée écoulée, la connexion au client distant est fermée. La valeur par défaut est 300.
- **ftp_data_port** — Spécifie le port utilisé pour les connexions actives aux données lorsque **connect_from_port_20** a pour valeur YES. La valeur par défaut est 20.
- **listen_address** — Spécifie l'adresse IP sur laquelle vsftpd doit être à l'écoute de connexions réseau.
- **listen_port** — Spécifie le port sur lequel vsftpd doit être à l'écoute de connexions réseau. La valeur par défaut est 21.
- **max_clients** — Spécifie le nombre maximal de clients autorisés à se connecter simultanément au serveur lorsqu'il tourne en mode autonome. Toute connexion client supplémentaire provoquerait un message d'erreur. La valeur par défaut est 0, ce qui ne limite pas les connexions.

31

Serveur FTP

04 - Options de configurations : Options réseau

Les directives ayant un impact sur la manière dont vsftpd interagit avec le réseau. (suite)

- **max_per_ip** — Spécifie le nombre maximal de clients autorisés à se connecter depuis l'adresse IP source.
- **pasv_address** — Spécifie l'adresse IP utilisée pour l'adresse IP publique du serveur aux serveurs se trouvant derrière des pare-feu NAT (Network Address Translation). Cette option permet à vsftpd de fournir la bonne adresse de retour pour des connexions en mode passif.
- **pasv_enable** — Lorsque cette option est activée, les connexions en mode passif ne sont pas permises. La valeur par défaut est YES.
- **pasv_max_port** — Spécifie le port le plus élevé possible qui est envoyé aux clients FTP pour des connexions en mode passif. Ce paramètre est utilisé pour limiter la plage de ports afin que les règles de pare-feu soient faciles à créer. La valeur par défaut est 0, ce qui ne limite pas la plage des ports passifs les plus élevés. La valeur ne doit pas dépasser 65535.
- **pasv_min_port** — Spécifie le port le plus bas possible qui est envoyé au client FTP pour des connexions en mode passif. Ce paramètre est utilisé pour limiter la plage de ports afin que les règles de pare-feu soient faciles à créer. La valeur par défaut est 0, ce qui ne limite pas la plage des ports passifs les plus bas. La valeur ne doit pas être inférieure à 1024.
- **pasv_promiscuous** — Lorsque cette option est activée, les connexions aux données ne sont pas analysées pour vérifier qu'elles proviennent bien de la même adresse IP. Ce paramètre est seulement utile pour certains types de tunnellation.
- **port_enable** — Lorsque cette option est activée, les connexions en mode actif ne sont pas permises.

32

05 - Démarrage de multiples instances de vsftpd : Configuration

- Parfois, un ordinateur est utilisé pour fournir de multiples domaines FTP. Cette technique est appelée **multihoming** (aussi appelée **hébergement multi-domaines**). Une possibilité d'effectuer du multihoming à l'aide de vsftpd consiste à exécuter de multiples copies du démon, chacune disposant de son propre fichier de configuration.
- Pour ce faire, assignez d'abord les adresses IP appropriées aux périphériques réseau des périphériques réseau du système. Ensuite, assurez-vous que le serveur DNS pour les domaines FTP est bien configuré pour référencer le bon ordinateur.
- Pour que vsftpd réponde à des requêtes sur des adresses IP, il est nécessaire que de multiples copies du démon tournent. La première copie doit être exécutée à l'aide des initscripts de vsftpd. Cette copie utilise le fichier de configuration standard, /etc/vsftpd/vsftpd.conf.
- Chaque site FTP supplémentaire doit avoir un fichier de configuration portant un nom unique dans le répertoire /etc/vsftpd/, comme /etc/vsftpd/**vsftpd-site-2.conf**. Chaque fichier de configuration ne doit être lisible et modifiable que par le super-utilisateur. Au sein de chaque fichier de configuration relatif à chaque serveur FTP écoutant sur un réseau IPv4, la directive suivante doit être unique :

listen_address=@IPV4

33

05 - Démarrage de multiples instances de vsftpd : Configuration

- Une fois que chaque serveur supplémentaire est doté d'un fichier de configuration, le démon vsftpd doit être exécuté depuis une invite du shell root à l'aide de la commande suivante :

#vsftpd /etc/vsftpd/ vsftpd-site-2.conf &

- Parmi d'autres directives pouvant faire l'objet de modifications sur une base individuelle pour chaque serveur figurent :
 - **anon_root**
 - **local_root**
 - **vsftpd_log_file**
 - **xferlog_file**

34

06 - Sécurité FTP

Le protocole de transfert de fichiers a été créé à l'origine sans aucune précaution de sécurité. Au moment du développement, Internet était encore à ses débuts et la cybercriminalité n'existait pas. Maintenant, l'utilisation du FTP est associée à de nombreux risques de sécurité, car toutes les informations transférées sont non chiffrées. C'est pourquoi deux variantes plus sûres ont été développées, qui sont depuis lors en concurrence l'une avec l'autre : **FTPS** et **SFTP**.

- Le protocole **FTPS** est le **FTP** avec **SSL**. La connexion est donc établie en combinaison avec Secure Sockets Layer (SSL) ou Transport Layer Security (**TLS**). L'échange de données est chiffré.
- Le protocole de transfert de fichiers **SSH** (**SFTP**) utilise quant à lui Secure Shell (**SSH**) pour le transfert sécurisé de fichiers. La connexion est également chiffrée. Mais alors que le FTPS nécessite deux connexions, le **SFTP** ne s'en sort qu'avec une.

35

Plan

Telnet

1. Le protocole Telnet
2. Faiblesse du protocole Telnet
3. Telnet, un protocole non sécurisé
4. Capture des identifiants avec Wireshark
5. Alternatives au protocole Telnet

36

Le protocole Telnet

- ✎ Le **protocole Telnet** (**Telecommunication Network**) est un protocole utilisé sur les réseaux informatiques pour **se connecter à distance à un serveur ou à un équipement réseau**. Une fois connecté à un équipement avec le protocole Telnet, on obtient **un accès à un prompt** afin de pouvoir **saisir et exécuter des commandes**.
- ✎ Le protocole Telnet est **un protocole de type client-serveur**, où les connexions sont effectuées sur **le port 23 en TCP**.
- ✎ Une machine disposant d'un serveur telnet (ex. telnetd sous Linux) permettra à n'importe quelle machine de part le réseau de s'y connecter, au moyen d'un client telnet (peut être représenté par l'ordinateur de l'administrateur système).
- ✎ le serveur Telnet peut être représenté aussi par un équipement réseau que l'on veut administrer à distance.
- ✎ Les clients telnet existent sur la quasi-totalité des plates formes (Windows, Linux, Unix, MacOS...).

37

Le protocole Telnet

- ✎ Il s'agit de l'un des protocoles les plus anciens, puisqu'il **a été créé en 1969** avant d'obtenir sa certification RFC le 1er mai 1973 : la **RFC 495**. Par la suite, deux autres RFC ont été mises en ligne pour mieux décrire le protocole et tenir compte des améliorations : **RFC 854** et **RFC 855**.
- ✎ Aujourd'hui, le protocole Telnet est utilisé pour **se connecter à un commutateur ou un routeur en ligne de commande**, dans le but de l'administrer.

Remarque:

- Le protocole Telnet, qui reste aujourd'hui utilisé pour effectuer de l'administration à distance, bien que ce ne soit pas un protocole **sécurisé**.

38

Faiblesse du protocole Telnet

Telnet, un protocole non sécurisé

- ✎ Le protocole Telnet a été développé à une époque où la sécurité n'était pas une préoccupation. De ce fait, le protocole Telnet n'est pas sécurisé. Pour être plus précis, **toutes les données échangées via Telnet sont transmises en clair sur le réseau**, c'est-à-dire qu'elles ne sont pas chiffrées.
- ✎ Cela signifie que si l'on utilise le protocole Telnet pour se connecter à un équipement réseau ou un serveur, les informations sensibles (**nom d'utilisateur et mot de passe**) seront transmises en clair sur le réseau. Si une personne malveillante parvient à **intercepter le trafic réseau**, elle sera en mesure de **recupérer vos identifiants** et de compromettre votre équipement.
- ✎ L'utilisation du protocole Telnet reste acceptable sur un réseau local, quand il n'y a pas d'autres alternatives, mais sur Internet, c'est à bannir. Dans tous les cas, il est important d'avoir **connaissance de ce risque** et de le prendre en considération.

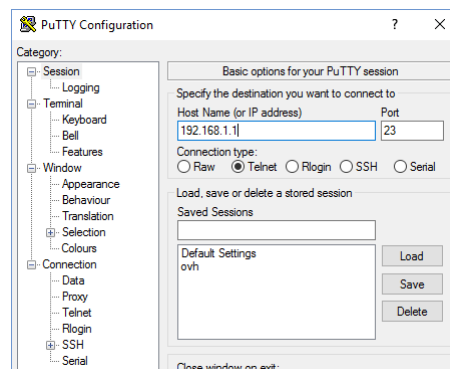
39

Faiblesse du protocole Telnet

Capture des identifiants avec Wireshark

- ✎ Soit l'exemple pratique suivant: on va établir une connexion Telnet depuis un PC Windows vers un équipement. Dans le même temps, une capture du trafic sera réalisée à partir du PC Windows qui initie la connexion Telnet.
- ✎ La connexion est initiée avec l'application PuTTY... Elle est établie, le login et le mot de passe sont saisis. Juste après, la capture Wireshark est arrêtée.

- ✎ Si l'on s'intéresse de plus près aux paquets échangés entre mon PC Windows et mon équipement, autrement dit mon client Telnet et mon serveur Telnet, on peut voir plusieurs paquets "Telnet Data...". Si l'on regarde le détail des paquets, on peut constater "Password:" comme données dans le paquet, ce qui correspond au prompt visible sur la console ci-dessus.



Faiblesse du protocole Telnet

Capture des identifiants avec Wireshark

270	10.216151	192.168.1.149	192.168.1.96	TELNET	64	Telnet Data ...
278	10.260260	192.168.1.96	192.168.1.149	TCP	54	55122 → 23 [ACK] Seq=107 Ack=108 Win=0 Len=0
339	13.277832	192.168.1.96	192.168.1.149	TELNET	70	Telnet Data ...

```

> Frame 270: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{71B8696D-6E7B-4D...}
> Ethernet II, Src: Synology_e6:ca:10 (00:11:32:e6:ca:10), Dst: AzureWav_ad:68:d7 (90:e8:68:ad:68:d7)
> Internet Protocol Version 4, Src: 192.168.1.149, Dst: 192.168.1.96
  > Transmission Control Protocol, Src Port: 23, Dst Port: 55122, Seq: 98, Ack: 107, Len: 10
    Source Port: 23
    Destination Port: 55122
    [Stream index: 10]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 10]
    Sequence Number: 98 (relative sequence number)
    Sequence Number (raw): 3895658314
    [Next Sequence Number: 108 (relative sequence number)]
    Acknowledgment Number: 107 (relative ack number)
    Acknowledgment number (raw): 351509932
    0101 ... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 229
    [Calculated window size: 29312]
    [Window size scaling factor: 128]
    Checksum: 0xc947 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (10 bytes)
  > Telnet
    Data: Password:

```

41

Faiblesse du protocole Telnet

Capture des identifiants avec Wireshark

➤ Puis, dans un autre paquet, émit depuis le client Telnet vers le serveur Telnet, on a cette valeur comme donnée : **"Tuto-Telnet-2023"** ! Il s'agit du **mot de passe de l'utilisateur** ! Au préalable, d'autres paquets ont transité, notamment pour l'identifiant (demo-telnet).

270	10.216151	192.168.1.149	192.168.1.96	TELNET	64	Telnet Data ...
278	10.260260	192.168.1.96	192.168.1.149	TCP	54	55122 → 23 [ACK] Seq=107 Ack=108 Win=0 Len=0
339	13.277832	192.168.1.96	192.168.1.149	TELNET	70	Telnet Data ...

```

> Frame 339: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{71B8696D-6E7B-4D...}
> Ethernet II, Src: AzureWav_ad:68:d7 (90:e8:68:ad:68:d7), Dst: Synology_e6:ca:10 (00:11:32:e6:ca:10)
> Internet Protocol Version 4, Src: 192.168.1.96, Dst: 192.168.1.149
  > Transmission Control Protocol, Src Port: 55122, Dst Port: 23, Seq: 107, Ack: 108, Len: 16
    Source Port: 55122
    Destination Port: 23
    [Stream index: 10]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 16]
    Sequence Number: 107 (relative sequence number)
    Sequence Number (raw): 351509932
    [Next Sequence Number: 123 (relative sequence number)]
    Acknowledgment Number: 108 (relative ack number)
    Acknowledgment number (raw): 3895658324
    0101 ... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 1026
    [Calculated window size: 262656]
    [Window size scaling factor: 256]
    Checksum: 0x0b40 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (16 bytes)
  > Telnet
    Data: Tuto-Telnet-2023

```

42

Faiblesse du protocole Telnet

Capture des identifiants avec Wireshark

Si l'on utilise la **fonction de suivi de flux TCP de Wireshark**, c'est encore plus flagrant et rapide : toutes les données sont visibles, en clair, dans une fenêtre récapitulative.

On peut récupérer l'identifiant et le mot de passe très facilement.

The image shows a Wireshark window titled "Wireshark - Suivre le flux TCP (tcp.stream eq 10) - Wireshark D mo 1.pcapng". It displays a summary of a TCP stream. The text "login: demo-telnetdemo-telnet" is visible, with an orange arrow pointing to it. Below it, the text "Password: Tuto-Telnet-2023" is also visible, with an orange arrow pointing to it. The rest of the stream content is also visible in plain text, including a warning about data storage and a shell prompt.

Cela montre qu'il est **tr s facile de lire les donn es au sein d'une communication entre un client et un serveur** lorsque le protocole Telnet est utilis . Ici, la capture est effectu e depuis le PC qui joue le r le de client Telnet, mais il pourrait s'agir d'une autre machine sur le r seau (qui parvient   se positionner de fa on   intercepter le trafic).

43

Alternatives au protocole Telnet

Pour des raisons de s curit , il est pr f rable d'utiliser d'autres protocoles sur le protocole Telnet, afin d'utiliser un protocole plus moderne et s curiser. La meilleure alternative au protocole Telnet, c'est le protocole **SSH** (Secure SHell). Contrairement au Telnet, le protocole SSH chiffre tous les  changes entre le client et le serveur, offrant ainsi une protection adapt e contre l' coute r seau et l'interception de trafic.

Le protocole SSH, au m me titre que le protocole Telnet, permet de se connecter   distance, en ligne de commande,   un  quipement pour l'administrer. Ceci est vrai pour un  quipement r seau, mais aussi une machine sous Linux ou Windows.

L'exemple ci-dessous montre que les paquets SSH sont chiffr s et le contenu n'est pas lisible.

No.	Time	Source	Destination	Protocol	Length	Info
120	1.853409	192.168.3...	239.255.2...	SSDP	431	NOTIFY * HTTP/1.1
121	1.854056	192.168.3...	239.255.2...	SSDP	494	NOTIFY * HTTP/1.1
428	9.068392	192.168.3...	vps-3c28d...	SSH	210	Client: Encrypted packet (len=64)
431	9.302819	192.168.3...	vps-3c28d...	SSH	118	Client: Encrypted packet (len=64)
444	9.611153	192.168.3...	vps-3c28d...	SSH	118	Client: Encrypted packet (len=64)
447	9.806782	vps-3c28d...	192.168.3...	SSH	118	Server: Encrypted packet (len=64)
450	9.812252	vps-3c28d...	192.168.3...	SSH	118	Server: Encrypted packet (len=64)
457	9.823951	vps-3c28d...	192.168.3...	SSH	118	Server: Encrypted packet (len=64)
459	9.828403	vps-3c28d...	192.168.3...	SSH	262	Server: Encrypted packet (len=208)
480	10.327282	vps-3c28d...	192.168.3...	SSH	228	Server: Encrypted packet (len=224)
483	10.351217	vps-3c28d...	192.168.3...	SSH	118	Server: Encrypted packet (len=64)
487	10.359541	vps-3c28d...	192.168.3...	SSH	166	Server: Encrypted packet (len=112)
852	17.149966	192.168.3...	vps-3c28d...	SSH	134	Client: Encrypted packet (len=80)
858	17.258284	vps-3c28d...	192.168.3...	SSH	166	Server: Encrypted packet (len=112)
650	12.582308	192.168.3...	195.122.1...	SSL	448	Continuation Data
658	12.676560	195.122.1...	192.168.3...	SSL	189	Continuation Data
767	14.645383	192.168.3...	195.122.1...	SSL	464	Continuation Data

44

Alternatives au protocole Telnet

- ✎ Pour des appareils prenant en charge d'autres protocoles, l'administration peut être effectuée via les protocoles HTTP, HTTPS ou RDP, mais l'utilisation dans la pratique sera différente.
- ✎ Le protocole Telnet est à maîtriser, car il fait partie des indispensables protocoles: bien qu'il soit à éviter, vous avez des chances de le croiser alors c'est important d'en savoir un minimum à son principe de fonctionnement.

45

Plan

SSH

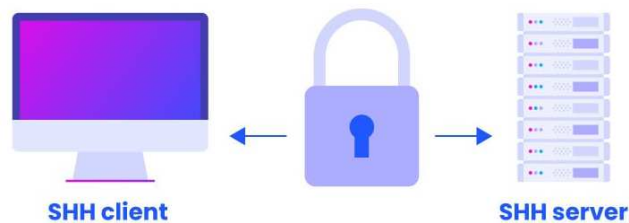
1. Le protocole SSH
2. Les principaux composants de SSH
3. Installation du SSH côté Serveur
4. Configuration du SSH côté Serveur
5. Installation du SSH côté Client
6. Connexion a un Serveur via ssh

46

SSH

SSH (Secure SHell)

- ✎ **Secure Shell** (SSH) est un programme mais aussi un protocole de communication **sécurisé**. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur.
- ✎ Le protocole SSH a été conçu avec l'objectif de **remplacer** les différents protocoles non chiffrés comme rlogin, telnet, rcp et rsh.



47

SSH

SSH (Secure SHell)

Secure Shell SSH est capable de :

- échange de clés de chiffrement
- toutes les trames sont chiffrées
- impossible de lire les trames sur le réseau via un snifer



48

Le Protocole SSH3

En 2023, une alternative à SSH, baptisée SSH3 car elle offre les mêmes services que SSH et s'appuie sur **HTTP/3** et **QUIC** a été proposée.

- **QUIC** est un protocole de transport fiable et sécurisé, en mode connecté, mis au point par Jim Roskind chez Google.
- **HTTP/3** : Une nouvelle version d'HTTP, qui est la troisième et prochaine version majeure du protocole de transfert hypertexte utilisé pour échanger des informations sur le World Wide Web. Celle-ci repose sur le protocole QUIC, développé par Google en 2012.

49

SSH (Secure SHell)

SSH permet de faire, en usage de base :

- ✎ Accès à distance sur la console en ligne commande (shell), ce qui permet, entre autres, d'effectuer la totalité des opérations courantes et/ou d'administration sur la machine distante.
- ✎ Déporter l'affichage graphique de la machine distante.
- ✎ Transferts de fichiers en ligne de commande.
- ✎ Montage ponctuel de répertoire distant, soit en ligne de commande, soit via **Nautilus**, sous Gnome par exemple Montage automatique de répertoires distants.
- ✎ **Remarque:** Nautilus est le gestionnaire de fichiers par défaut d l'environnements GNOME Shell, Il s'agit de l'équivalent de "l'Explorateur Windows" (sur Windows) ou de "Finder" (sur MacOS).

50

SSH

Les principaux composants de SSH

- ✂ sshd : le logiciel serveur, actif sur le port 22, qui ouvre une session à partir d'une connexion d'un client ssh.
- ✂ ssh : le logiciel client qui remplace rsh et rlogin.
- ✂ scp : le logiciel client qui remplace rcp.
- ✂ ssh-keygen : le logiciel qui permet de créer un couple de clés publique/privée

51

SSH

Installation du SSH coté Serveur

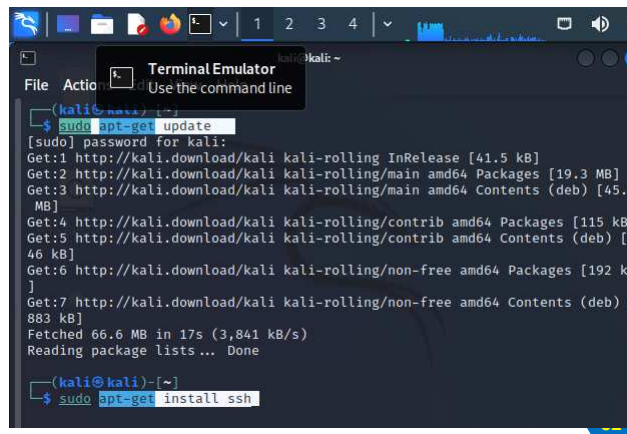
SSH (secure shell) service on Kali Linux

Instructions : Install SSH

From the terminal use apt-get command to install SSH packages:

sudo apt-get update

sudo apt-get install ssh



```
(kali@kali: ~)$ sudo apt-get update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [
46 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 k
]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb)
883 kB]
Fetched 66.6 MB in 17s (3,841 kB/s)
Reading package lists... Done

(kali@kali)~$ sudo apt-get install ssh
```

Installation du SSH coté Serveur

SSH (secure shell) service on Kali Linux

Instructions : Install SSH

```
(kali@kali) [~]
$ sudo apt-get install ssh
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5
  libqt5multimediawidgets5 libwireshark15 libwiretap12 libwsutil13
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  ssh
0 upgraded, 1 newly installed, 0 to remove and 1917 not upgraded.
Need to get 155 kB of archives.
After this operation, 167 kB of additional disk space will be used.
Get:1 http://kali.download/kali Kali-rolling/main amd64 ssh all 1:9.6p1-4 [155 kB]
Fetched 155 kB in 1s (218 kB/s)
Selecting previously unselected package ssh.
(Reading database ... 300319 files and directories currently installed.)
Preparing to unpack .../ssh_1%3a9.6p1-4_all.deb ...
Unpacking ssh (1:9.6p1-4) ...
Setting up ssh (1:9.6p1-4) ...

(kali@kali) [~]
$
```

53

Installation du SSH coté Serveur

SSH (secure shell) service on Kali Linux

Instructions : Enable and Start SSH

To make sure that secure shell starts after reboot use systemctl command to enable it: # sudo systemctl enable ssh

To start SSH for a current session execute: # sudo service ssh start

```

Fetched 155 kB in 1s (218 kB/s)
Selecting previously unselected package ssh.
(Reading database ... 300319 files and directories currently installed.)
Preparing to unpack .../ssh_1%3a9.6p1-4_all.deb ...
Unpacking ssh (1:9.6p1-4) ...
Setting up ssh (1:9.6p1-4) ...

(kali@kali) [~]
$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh

(kali@kali) [~]
$ sudo service ssh start

(kali@kali) [~]
$
```

54

Installation du SSH coté Serveur

SSH (secure shell) service on Kali Linux

Instructions :Allow SSH Root Access

- By default SSH would not allow you to SSH login as root user, thus the following error message will appear: **Permission denied, please try again.**
- edit or insert the following line within the **sudo nano /etc/ssh/sshd_config** SSH config file:

```

Ond nano 0.2 /etc/ssh/sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying

```

55

Installation du SSH coté Serveur

SSH (secure shell) service on Kali Linux

Instructions :Allow SSH Root Access

- insert the following line within the **/etc/ssh/sshd_config** SSH config file:
- FROM: **#PermitRootLogin prohibit-password** TO: **PermitRootLogin yes**

```

Ond nano 0.2 /etc/ssh/sshd_config *
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
File Name to Write: /etc/ssh/sshd_config

```

56

SSH

Configuration du SSH coté Serveur

Autoriser/Interdire des utilisateurs

Pour autoriser une liste de certains utilisateurs à se connecter. Modifier ou ajouter cette ligne dans le sshd_config : **AllowUsers user1 user2 user3**

Pour autoriser seulement certains membres de groupes à avoir accès via SSH en modifiant la ligne : AllowGroups groupe1 groupe2

Pour refuser la connexion que de certains utilisateurs. Modifier ou ajouter cette ligne dans le sshd_config : **DenyUsers user1 user2 user3**

Modifier le port d'écoute

Par défaut, le serveur openSSH écoute sur le port 22, pour change le port d'écoute du serveur openSSH modifier ou ajouter cette ligne dans le sshd_config : **Port numéro_du_port**

Limiter le nombre de tentative d'authentification

Pour limiter le nombre de de tentative d'authentification par exemple à 4 , modifier la ligne suivante : **MaxAuthTries 4**

57

SSH

Configuration du SSH coté Serveur

Modifier le port d'écoute

Par défaut, le serveur openSSH écoute sur le port 22, pour change le port d'écoute du serveur openSSH modifier ou ajouter cette ligne dans le sshd_config : **Port numéro_du_port**

Autoriser /interdire mot de passe vide :

Pour interdire la connexion au mot de passe vide modifier ou ajouter cette ligne dans le sshd_config : **PermitEmptyPasswords no**

Les valeurs possibles sont donc yes pour autoriser l'accès mot de passe vide, no (par défaut) pour le refuser.

Autoriser / interdire authentification par mot de passe

L'option suivante permet d'autoriser ou non des connexion avec un couple identifiant/mot de passe **PasswordAuthentication yes**

Les valeurs possibles sont donc yes pour autoriser l'authentification par mot de passe , no pour le refuser.

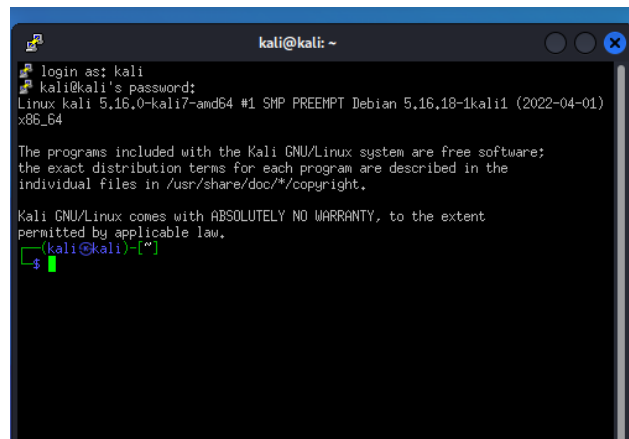
58

Installation du SSH coté Serveur

SSH (secure shell) service on Kali Linux

Instructions :restart ssh service

sudo service ssh restart

A terminal window titled 'kali@kali: ~' showing the Kali Linux login process. It prompts for a login as 'kali', then for the password. After successful login, it displays the system version 'Linux kali 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali1 (2022-04-01) x86_64'. It then shows the standard Kali GNU/Linux disclaimer about free software and warranty. Finally, it shows the user prompt '(kali@kali)-[~]' with a green cursor on the '\$' prompt.

```
kali@kali: ~  
login as: kali  
kali@kali's password:  
Linux kali 5.16.0-kali7-amd64 #1 SMP PREEMPT Debian 5.16.18-1kali1 (2022-04-01)  
x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
(kali@kali)-[~]  
$
```

59

Se connecter par la commande SSH

Authentification par mot de passe

C'est la méthode la plus simple. Depuis la machine cliente,
taper : ssh login@nom du domaine ou adresse IP du serveur

Ensuite, entrez votre mot de passe... et vous verrez apparaître
le prompt, comme si vous vous étiez connecté en local sur la
machine.

En IPV6 ajouter l'option -6

ssh -6 <nom_utilisateur>@<adresse ipv6>

60

Se connecter par la commande SSH**Authentification par clef**

Au lieu de s'authentifier par mot de passe, les utilisateurs peuvent s'authentifier grâce à la cryptographie asymétrique et son couple de clefs privée/publique, comme le fait le serveur SSH auprès du client SSH.

Générer la clefs

La création de la paire de clé se fait avec ssh-keygen.

Il existe 2 types de clés : RSA et DSA. Chacune pouvant être de longueur différente : 1024, 2048, 4096 bits (les clés inférieures à 2048 bits sont à proscrire... surtout les RSA). Pour créer une clé DSA de 2048 bits : `ssh-keygen -t dsa -b 2048`. Sans paramètres, les options par défaut sont type RSA en 2048 bits. `$ssh-keygen -t rsa -b 2048`

61

Se connecter par la commande SSH**Se connecter (solution avec ssh-agent)**

- La commande est la même que pour une authentification par mot de passe mais sans demander le mot de passe
- Le serveur SSH est maintenant plus sécurisé, mais taper des passphrases à longueur de journée peut se révéler être très pénible surtout si on a choisi une « vraie » passphrase.
- L'agent SSH permet de taper la passphrase une seule fois et de la conserver en mémoire pendant tout son fonctionnement. Les communications SSH fonctionneront donc de façon transparente.
- Il faut lancer l'agent avec un shell (le plus simple étant de le lancer avec la variable \$SHELL qui contient le shell courant).
- Ensuite le programme ssh-add permet de charger les clé présentes dans ~/.ssh/. La passphrase est demandée, toutes les connexions nécessitant les clés chargées par l'agent seront transparentes.

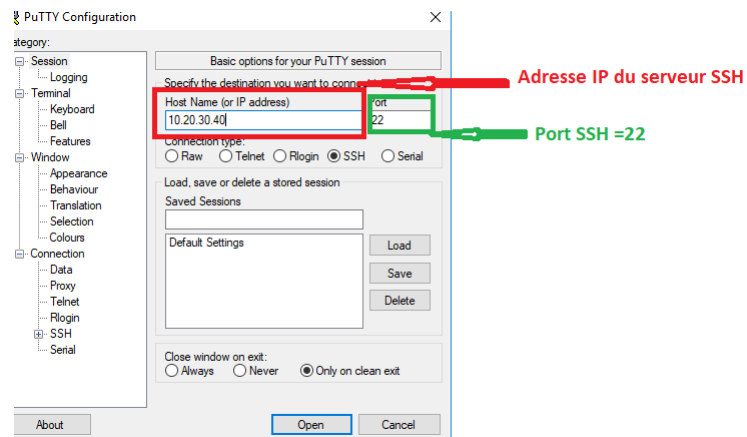
```
$ ssh-agent $SHELL
```

```
$ ssh-add
```

62

Installation du SSH coté Client

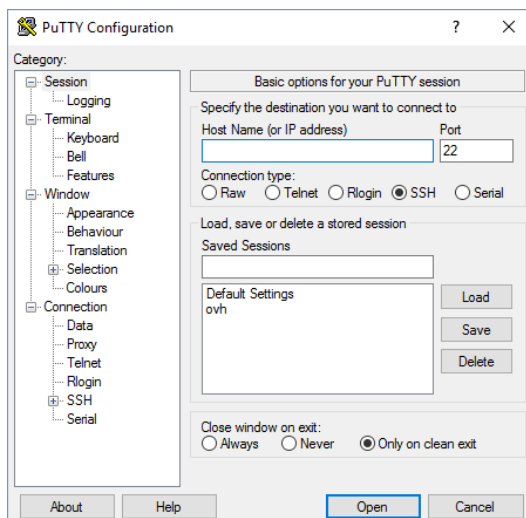
Se connecter par Putty (client Windows)



63

Installation du SSH coté Client

Se connecter par Putty (client Windows)



64

Installation du SSH coté Client Se connecter par Tera Term (client Windows)

Tera Term: Nouvelle connexion

☒ TCP/IP Hôte: localhost

☒ Historique

Service ☐ Telnet TCP port#: 22

☒ SSH SSH version: SSH2

☐ Autre IP version: AUTO

☐ Série Port: COM3: Intel(R) Active Management Te

OK Effacer Aide

65

Plan

Serveur HTTP Apache (Serveur Web)

1. Présentation du serveur web
2. Les serveurs HTTP les plus utilisés sont
3. Hypertext Transfer Protocol (HTTP)
4. Hypertext Transfer Protocol Secure (HTTPS)
5. Apache :Installation on Kali linux (Python 3, php,...)
6. Configuration du serveur Web

66

Qu'est-ce qu'un serveur web ?

- Un **serveur web** est soit un logiciel de service de ressources web (**serveur HTTP**), soit un serveur informatique (ordinateur) qui répond à des requêtes du World Wide Web sur un réseau public (Internet) ou privé (intranet), en utilisant principalement le protocole HTTP.
- Un serveur informatique peut être utilisé à la fois pour servir des ressources du Web et pour faire fonctionner en parallèle d'autres services liés, comme l'envoi de courriers électroniques, l'émission de flux en streaming, le stockage de données dans des bases de données, le transfert de fichiers par FTP.

67

Présentation du serveur web

- Les serveurs web publics sont reliés à Internet et hébergent des ressources (**pages web**, images, vidéos, etc.) du **Web**. Ces ressources peuvent être statiques (servies telle quelles) ou dynamiques (construites à la demande par le serveur).
- Certains serveurs sont seulement accessibles sur des réseaux privés (intranets) et hébergent des sites utilisateurs, des documents, ou des logiciels, internes à une entreprise, une administration, etc.
- La fonction principale d'un serveur Web est de stocker et délivrer des pages web qui sont généralement rendues en HTML. Le protocole de communication Hypertext Transfer Protocol (HTTP) permet le dialogue via le réseau avec le logiciel client, généralement un navigateur web.
- Techniquement il serait possible qu'un même ordinateur remplisse ces deux fonctions, mais c'est rarement le cas pour des raisons de sécurité.

68

Les serveurs HTTP les plus utilisés sont

1. **Apache** : HTTP serveur de la Apache Software Foundation.
 - **Apache HTTP Server** de la Apache Software Foundation, successeur du **NCSA HTTPd** ;
 - **Apache Tomcat** de l'Apache Software Foundation, évolution de Apache pour **J2EE** ;
2. **IIS** : Internet Information Services de Microsoft (IIS)
3. **Oracle iPlanet Web Server** de Sun Microsystems ;
4. **Google Web Server** de Google ;
5. **Node.js** sous licence MIT conçu par Ryan Lienhart Dahl en lignes de programmation en JavaScript ;
6. Hiawatha de Hugo Leisink
7. **Zeus Web Server** de Zeus Technology ;
8. **Gunicorn** est un serveur web HTTP WSGI écrit en Python pour Unix ;
9. **Abyss Web Server**, un serveur gratuit, multi-plateforme (Linux, Windows, MacOS, BSD).
10.

69

Présentation du serveur web

- Un serveur HTTP est à l'écoute des connections sur un port
- donne.
- Le port standard pour un serveur HTTP est le numéro 80.
- Le client d'un serveur HTTP est le navigateur Internet.
- A chaque requête qu'il reçoit le serveur présente à l'utilisateur la page demandée.

Remarque:

Sur certains serveurs le port d'écoute n'est pas 80 mais par exemple 1600. Dans ce cas on accedera au serveur par l'adresse suivante : `http://www.site.com:1600/` .

70

Serveur web : Hypertext Transfer Protocol (HTTP)

- L'**HyperText Transfer Protocol**, généralement abrégé HTTP, littéralement « protocole de transfert hypertexte », est un protocole de communication client-serveur développé pour le World Wide Web. HTTPS (avec S pour secure, soit « sécurisé ») est la variante sécurisée par le chiffrement et l'authentification.
- **HTTP** est un protocole de la couche application dans le modèle TCP/IP. Il peut fonctionner sur n'importe quelle connexion fiable. Dans les faits on utilise le protocole TCP comme couche de transport.
- Un serveur **HTTP** utilise alors par défaut le port 80 (443 pour HTTPS).
- Les **clients HTTP** les plus connus sont les navigateurs Web. Il est aussi utilisé dans des interfaces de programmation d'application (API) pour accéder aux données d'un serveur ainsi que des systèmes pour récupérer automatiquement le contenu d'un site tels que les aspirateurs de site Web et les robots d'indexation.

71

Hypertext Transfer Protocol (HTTP) : Historique

- HTTP a été inventé par **Tim Berners-Lee** avec les adresses Web et le langage HTML pour créer le World Wide Web. À cette époque, le File Transfer Protocol (FTP) était déjà disponible pour transférer des fichiers, mais il ne supportait pas la notion de format de données telle qu'introduite par Multipurpose Internet Mail Extensions (MIME).

HTTP 0.9

Au début du **World Wide Web**, il était prévu d'ajouter au protocole HTTP des capacités de négociation de contenu, en s'inspirant notamment de MIME. En attendant, le protocole HTTP 0.9 était extrêmement simple.

- connexion du client HTTP
- envoi d'une requête de méthode GET
- réponse du serveur HTTP
- le serveur ferme la connexion pour signaler la fin de la réponse.

HTTP 1.0

Le protocole HTTP 1.0, décrit dans la RFC 1945, prévoit l'utilisation d'entêtes spécifiés dans la RFC 822. La gestion de la connexion reste identique à HTTP 0.9 : le client établit la connexion, envoie une requête, le serveur répond et ferme immédiatement la connexion.

72

Hypertext Transfer Protocol (HTTP) : Historique

HTTP/2 : Hypertext Transfer Protocol/2.

- Une nouvelle version d'HTTP, HTTP/2, a été développée au sein du groupe de travail « Hypertext Transfer Protocol Bis » (httpbis) de l'Internet Engineering Task Force, et approuvée comme RFC standard le 18 février **2015**. Le développement d'HTTP/2 a débuté à la suite de la création du protocole **SPDY** proposé par **Google** afin de réduire le temps de chargement des pages Web (avec notamment des implémentations dans deux des principaux navigateurs Web, Google Chrome et Mozilla Firefox).
- SPDY constituait une option naturelle pour servir de base à HTTP/2. Deux autres propositions concurrentes ont été ensuite transmises à l'IETF : le protocole « HTTP Speed+Mobility » par Microsoft et une proposition de mise à jour d'HTTP (« Network-Friendly HTTP Upgrade »). En juillet 2012, httpbis a publié un appel à expression d'intérêt (« Call for Expression of Interest ») afin de recueillir l'avis d'acteurs du Web sur les propositions. Parmi les réponses obtenues figure celle de Facebook qui a signifié sa préférence pour SPDY. En novembre 2012, l'IETF a publié le premier draft d'HTTP/2, qui est une copie directe de SPDY.
- Après plus de 2 ans de discussions, la RFC est approuvée en février 2015 par le groupe de pilotage de l'IETF, et est publiée en mai 2015.
- Le module permettant la prise en charge du protocole HTTP/2 est disponible depuis la version 2.4.17 du serveur Web Apache, et depuis la version 1.9.5 de Nginx.

73

Hypertext Transfer Protocol (HTTP) : Historique

HTTP/3 : Hypertext Transfer Protocol/3

- Une nouvelle version d'HTTP, HTTP/3, est la troisième et prochaine version majeure du protocole de transfert hypertexte utilisé pour échanger des informations sur le World Wide Web. Celle-ci repose sur le protocole **QUIC**, développé par Google en 2012.
- La sémantique HTTP est cohérente d'une version à l'autre. En effet, les mêmes méthodes de requête, codes de statut et champs de message sont généralement applicables à toutes les versions.
- Si HTTP/1 et HTTP/2 utilisent tous deux TCP comme protocole de transport, HTTP/3 quant à lui utilise le protocole **QUIC**, un protocole de la couche transport qui est plus adapté au Web. Le passage à **QUIC** vise à résoudre un problème majeur de HTTP/2 appelé "Head-of-line Blocking" grâce à une encapsulation des paquets dans UDP. En effet, avec HTTP/2 reposant sur TCP, une connexion permet d'accéder aux ressources demandées une à une (une seule à la fois). Lorsque l'envoi d'une ressource est perturbé (par exemple par une perte de paquets), la livraison globale des ressources est ralentie.
- Avec HTTP/3 reposant sur le protocole QUIC, ce problème n'est plus, puisque tous les flux sont indépendants étant encapsulés dans UDP, protocole de transport ne nécessitant pas de connexion.

74

Hypertext Transfer Protocol (HTTP) : Implémentation

Méthodes

- Dans le protocole HTTP, une méthode est une commande spécifiant un type de requête, c'est-à-dire qu'elle demande au serveur d'effectuer une action. En général l'action concerne une ressource identifiée par l'URL qui suit le nom de la méthode.

il existe de nombreuses méthodes, les plus courantes étant **GET, HEAD et POST** :

- **GET** : c'est la méthode la plus courante pour demander une ressource. Une requête GET est sans effet sur la ressource, il doit être possible de répéter la requête sans effet.
- **HEAD** Cette méthode ne demande que des informations sur la ressource, sans demander la ressource elle-même.
- **POST** Cette méthode est utilisée pour transmettre des données en vue d'un traitement à une ressource (le plus souvent depuis un formulaire HTML). L'URI fourni est l'URI d'une ressource à laquelle s'appliqueront les données envoyées. Le résultat peut être la création de nouvelles ressources ou la modification de ressources existantes.

75

Hypertext Transfer Protocol Secure (HTTPS)

- L'HyperText Transfer Protocol Secure (HTTPS, littéralement « protocole de transfert hypertextuel sécurisé ») est la **combinaison** du **HTTP** avec une couche de chiffrement **TLS3**.
- **HTTPS** permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable (et faisant généralement partie de la liste blanche des navigateurs internet et des systèmes d'exploitation).
- Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur. Il peut permettre de valider l'identité du visiteur, si celui-ci utilise également un certificat d'authentification client émis par une autorité fiable.
- **HTTPS** est aussi utilisé pour la consultation de données privées, comme les courriers électroniques, par exemple.

76

Hypertext Transfer Protocol Secure (HTTPS)

- **HTTPS** est maintenant utilisé plus souvent par les utilisateurs Web que le HTTP non sécurisé d'origine, principalement pour protéger l'authenticité des pages sur tous les types de sites Web, comptes sécurisés, et pour garder les communications des utilisateurs, l'identité et la navigation Web privées.
- 2010 : le HTTPS s'est généralisé sur les réseaux sociaux.
- Par défaut, les serveurs HTTPS sont connectés au port TCP 443. C'est un port très souvent ouvert derrière les pare-feux.
- En janvier 2017, Google Chrome et Mozilla Firefox ont commencé à identifier et signaler les sites Web qui recueillent des informations sensibles sans utiliser le protocole HTTPS. Ce changement a pour but d'augmenter de manière significative l'utilisation du HTTPS.

77

Apache

- Ecrit en C (portable), plate forme UNIX (ou Linux) recommandée
- Multi-processus / multi-thread (daemon httpd)
- Configuration très flexible
- Architecture modulaire
- Comment obtenir Apache ?
 - inclu dans la plupart des distributions linux (httpd)
 - sources et binaires sur <http://www.apache.org/dist/httpd>
- première version décembre 1995
- dernière version : Apache 2.4.59 (4 avril 2024)

78

Apache :Modules

- compiles (statiques) ou lies dynamiquement (.so ou .dll)
- permettent d'ajouter des fonctionalites, exemples:
 - mod_speling : correction des URL erronees
 - mod_ssl : gestion SSL (https)
 - mod_cgi : gestion protocole CGI
 - mod_alias : definition d'alias (URL)
 - etc... plusieurs dizaines de modules
- directives de configuration specifiques a chaque module
- l'API des modules est documentee: on peut definir de nouveaux modules (en langage C) si besoin.

79

Apache :Les répertoires importants

- /usr/local/bin/httpd : l'executable Apache
- /etc/apache : les fichiers de configuration httpd.conf
- /www : le site web
- /var/log/apache/logs : les journaux

80

Apache :Installation on Kali linux (Python 3, php,...)

- Pour installer Python 3 sur Kali Linux :
 - \$ sudo apt install python3
- Pour installer Apache sur Kali Linux :
 - \$ sudo apt install apache2

```

(kali@kali)-[~]
$ sudo apt-get install apache2
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libqt5multimedia5 libqt5multimedia5-plugins libqt5multimedia5-sttools5 libqt5multimedia5-widgets5 libwireshark15
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libnghttp2-14
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following packages will be upgraded:
  apache2 apache2-bin apache2-data apache2-utils libnghttp2-14
5 upgraded, 0 newly installed, 0 to remove and 1912 not upgraded.
Need to get 2,028 kB of archives.
After this operation, 102 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libnghttp2-14 amd64 1.59.0-1 [74.3 kB]

```

81

Apache :Installation on Kali linux (Python 3, php,...)

- Pour installer Apache sur Kali Linux :
 - \$ sudo apt install apache2
- Pour installer Python 3 sur Kali Linux :
 - \$ sudo apt install python3

```

(kali@kali)-[~]
$ sudo service apache2 status
[sudo] password for kali:
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-04-23 07:48:50 EDT; 1min 37s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2308 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2324 (apache2)
     Tasks: 6 (limit: 2245)
    Memory: 17.5M
       CPU: 113ms
   CGroup: /system.slice/apache2.service
           └─2324 /usr/sbin/apache2 -k start
             └─2326 /usr/sbin/apache2 -k start
               └─2327 /usr/sbin/apache2 -k start
                 └─2328 /usr/sbin/apache2 -k start
                   └─2329 /usr/sbin/apache2 -k start
                     └─2330 /usr/sbin/apache2 -k start

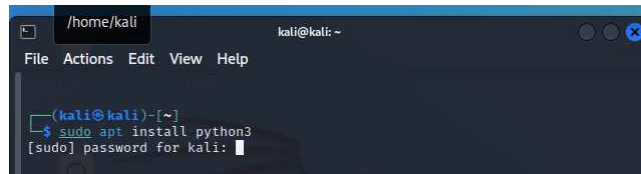
Apr 23 07:48:49 kali systemd[1]: Starting The Apache HTTP Server ...
Apr 23 07:48:50 kali apachectl[2323]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Apr 23 07:48:50 kali systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)

```

82

Apache :Installation on Kali linux (Python 3, php,...)

- Pour installer Apache sur Kali Linux :
 - \$ sudo apt install apache2
- Pour installer Python 3 sur Kali Linux :
 - \$ sudo apt install python3



```
(kali@kali)-[~]  
$ sudo apt install python3  
[sudo] password for kali:   
$
```

83

Configuration du serveur Web

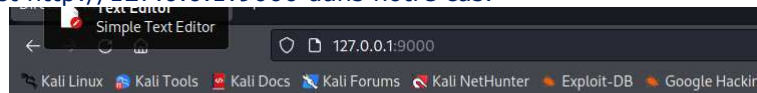
Pour démarrer un serveur Web à l'aide de Python 3, utilisez la commande suivante.

\$ python3 -m http.server --bind 127.0.0.1 9000



```
(kali@kali)-[~]  
$ python3 -m http.server --bind 127.0.0.1 9000  
Serving HTTP on 127.0.0.1 port 9000 (http://127.0.0.1:9000/) ...  
$
```

Ensuite ouvrir un navigateur et accéder à l'adresse que vous avez configurée, qui est `http://127.0.0.1:9000` dans notre cas.



Directory listing for /

- [.bash_history](#)
- [.bash_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.cache/](#)
- [.config/](#)
- [.dmrc](#)

84

Configuration du serveur Web

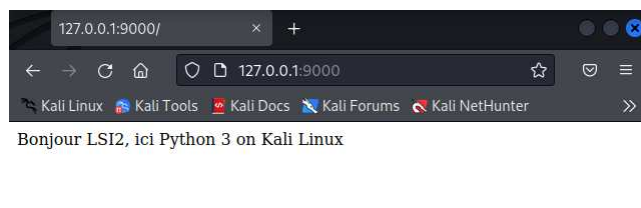
Vous souhaitez proposer ici une sorte de site Web HTML. Vous pouvez donc générer un document de test à utiliser.

\$Echo Bonjour LSI2, ici Python 3 on Kali Linux > ~/index.html



```
kali@kali: ~  
$ echo Bonjour LSI2, ici Python 3 on Kali Linux > ~/index.html  
$
```

Ensuite actualiser le site Web pour voir la page que nous venons de créer.



85

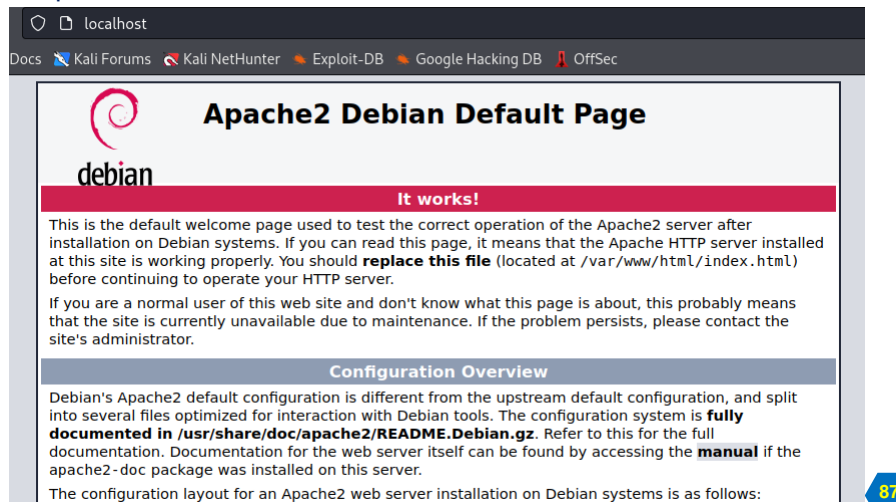
Configuration du serveur Web

- ❑ Une fois Apache installé, vous pouvez utiliser les commandes **systemctl** de **systemd** pour contrôler le service. Activez ou désactivez le démarrage d'Apache au démarrage du système :
 - \$ sudo systemctl enable apache2
 - OR
 - \$ sudo systemctl disable apache2
- ❑ Démarrez ou arrêtez le serveur Web Apache :
 - \$ sudo systemctl start apache2
 - OR
 - \$ sudo systemctl stop apache2
- ❑ Une fois que vous avez démarré le serveur Web Apache à l'aide de la commande systemctl présentée ci-dessus, vous pouvez tester pour vous assurer que tout fonctionne correctement en accédant à <http://localhost> sur votre système.
- ❑ Vous devriez être accueilli par la page Apache par défaut, comme indiqué ci-dessous.

86

Configuration du serveur Web

- ❑ Vous devriez être accueilli par la page Apache par défaut, comme indiqué ci-dessous.

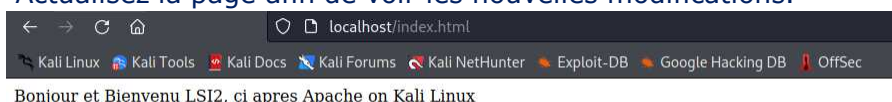


Configuration du serveur Web

- ❑ Avec Apache opérationnel, nous sommes prêts à configurer notre site Web. Le répertoire par défaut des fichiers de notre site Web est **/var/www/html**.
- ❑ Déplacez vos fichiers ici ou commencez par remplacer la page de vœux index.html par défaut. Dans cet exemple, nous allons simplement créer un simple document HTML pour voir les modifications reflétées sur le site Web.
 - \$ echo Bonjour et bienvenu LSI2, ci apres Apache on Kali Linux > index.html
 - \$ sudo mv index.html /var/www/html

```
(kali@kali)-[~]
└─$ sudo echo Bonjour et Bienvenu LSI2, ci apres Apache on Kali Linux > index.html
[sudo] password for kali:
└─$ sudo mv index.html /var/www/html
```

- ❑ Actualisez la page afin de voir les nouvelles modifications.



Plan

VPN & OpenVPN

1. Présentation du Réseau privé virtuel
2. Protocole PPTP
3. Protocole IPSec
4. OpenVPN

89

Réseau privé virtuel

Réseau privé virtuel

- ❑ Les risques de sécurité apparaissent lorsqu'un télétravailleur ou un employé d'un bureau distant utilise les services haut débit pour accéder au WAN d'entreprise via Internet.

---- > **Pour remédier à ces problèmes de sécurité, les services haut débit permettent l'utilisation de connexions VPN à un serveur VPN, qui se trouve habituellement sur le site de l'entreprise.**

- ❑ **Un VPN est une connexion chiffrée entre réseaux privés sur un réseau public, par exemple Internet. Au lieu d'utiliser une connexion de couche 2 dédiée comme une ligne louée, le VPN utilise des connexions virtuelles appelées tunnels VPN, qui passent via Internet depuis le réseau privé de la société vers l'employé ou le site distant.**



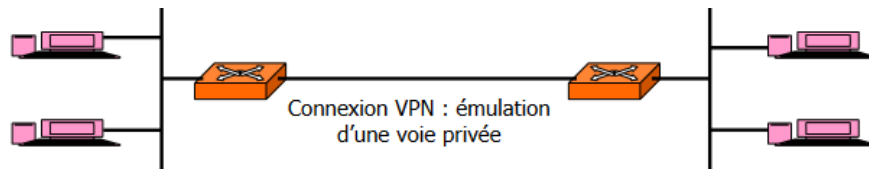
90

Réseau privé virtuel

Solution VPN



Cette Solution fonctionnellement équivalente à



91

Réseau privé virtuel

Objectif

Réaliser un réseau privé sécurisé en utilisant l'infrastructure d'un réseau partagé (ouvert).

1. Réseau (network)

- Interconnecter un ensemble de **systèmes informatiques dispersés**.
- Résoudre des **problèmes de commutation/routage (niveau 2/3)**.

2. Privé (private)

- Transporter des flots de messages d'une communauté **privée** de façon indépendante de ceux d'autres usagers.
- Les usagers doivent recevoir une garantie de sécurité (confidentialité, intégrité ou protection) sur leurs données.
- Les usagers autorisés peuvent communiquer en utilisant des adresses, une topologie, un routage privés.

3. Virtuel (virtual)

- Le réseau physique ne correspond pas forcément au réseau visé.
- Le réseau privé est réalisé en partageant les ressources d'un (ou de plusieurs) fournisseur d'accès

92

Principe

Un réseau VPN repose sur un protocole appelé "protocole de tunneling".

- Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire.
- **Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.**
- Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.
- Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local.
- La source chiffre les données et les achemine en empruntant ce chemin virtuel.
- Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.
- Les données à transmettre peuvent être prises en charge par un protocole différent d'IP.
- Dans ce cas, le protocole de tunneling **encapsule** les données en ajoutant une en-tête.
- Un VPN crée des connexions temporaires ou tunnels entre 2 machines, ou une machine et un réseau, ou 2 réseaux.

93

Les avantages d'un VPN

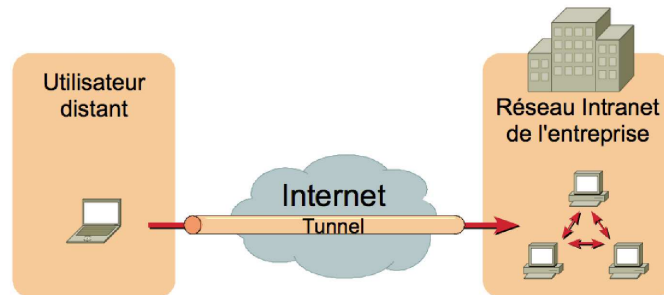
- ❑ Économies : les VPN permettent aux organisations d'utiliser Internet pour connecter des bureaux et des utilisateurs distants au site principal, éliminant ainsi les liaisons WAN dédiées et les batteries de modems, très coûteuses.
- ❑ Sécurité : les VPN offrent le plus haut niveau de sécurité grâce au chiffrement et aux protocoles d'authentification avancés qui protègent les données de l'accès non autorisé.
- ❑ Évolutivité : comme les VPN utilisent l'infrastructure Internet des FAI et des périphériques, l'ajout de nouveaux utilisateurs est simple. Les grandes entreprises peuvent ajouter des volumes importants de capacité sans ajouter d'infrastructure importante.
- ❑ Compatibilité avec la technologie haut débit : la technologie VPN est prise en charge par les fournisseurs de services haut débit, par exemple via DSL ou câble, donc les travailleurs mobiles peuvent profiter de leur Internet haut débit à la maison pour accéder au réseau d'entreprise. Des connexions pour entreprises et à haut débit peuvent également être une solution rentable pour connecter des bureaux distants.

94

Fonctionnalité des VPN

❑ VPN d'accès à distance

Permettre aux utilisateurs d'accéder au réseau local (Nomade ou Road Warrior)

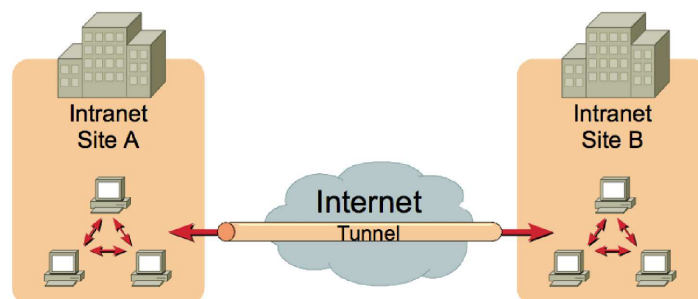


95

Fonctionnalité des VPN

❑ Intranet VPN

Relier plusieurs sites distants entre eux (LAN to LAN)

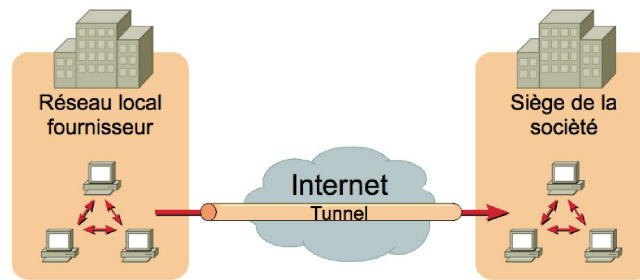


96

Fonctionnalité des VPN

☐ Extranet VPN

Ouvrir son réseau local à ses partenaires (LAN to LAN)



97

Bilan des caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

☐ Authentification d'utilisateurs.

Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

☐ Gestion d'adresses.

Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle.

☐ Cryptage des données.

Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.

☐ Gestion de clés.

Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

☐ Prise en charge multi-protocole.

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

98

Protocoles utilisés pour réaliser une connexion VPN

Les protocoles étudiés sont deux catégories:

- Les protocoles de niveau 2 comme PPTP et L2TP
- Les protocoles de niveau 3 comme IPSEC ou MPLS.

❑ Il existe 3 protocoles de niveau 2 permettant de réaliser des VPN
PPTP (de Microsoft), L2F (développé par CISCO) & L2TP.

L2F ayant aujourd'hui quasiment disparu.

- PPTP aurait sans doute lui aussi disparu Microsoft l'intègre à ses systèmes d'exploitation Windows.
- L2TP est une évolution de PPTP et de L2F, reprenant les avantages des deux protocoles.

99

PROTOCOLE PPP

PPP (Point to Point Protocol) est un protocole de transfert des données sur un lien synchrone ou asynchrone.

- ❑ Il garantit l'**ordre d'arrivée** des paquets.
- ❑ Il **encapsule** les paquets IP des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point.
- ❑ PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau (NAS).

❑ Remarque:

- Le protocole PPP n'est pas un protocole permettant l'établissement d'un VPN; Mais
- Il est très souvent utilisé pour transférer les informations au travers d'un VPN.

100

PROTOCOLE PPTP (Point-to-point tunneling protocol)

- ☐ PPTP (Point-to-point tunneling protocol - RFC 2637), protocole de tunnel point-à-point, est un protocole d'encapsulation PPP sur IP conçu en 1999 par Microsoft.
- ☐ PPTP est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un VPN.
- ☐ PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows.
- ☐ PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression.
- ☐ Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse

101

PROTOCOLE PPTP

- ☐ Ce protocole ouvre deux canaux de communication entre le client et le serveur :
- ☐ un canal de contrôle pour la gestion du lien, qui consiste en une connexion TCP sur le **port 1723** du serveur ;
- ☐ un canal de données transportant les données du réseau privé et utilisant le protocole IP **numéro 47**.
- ☐ Le canal de données consiste en une version non standard du protocole Generic Routing Encapsulation (GRE). Les paquets GRE modifiés transportent des trames PPP. Enfin, les trames PPP encapsulent les paquets IP transportés par le tunnel.
- ☐ Le flux PPP peut être chiffré, authentifié et compressé à l'aide des mécanismes standard de PPP, auxquels Microsoft a ajouté l'authentification MS-CHAP, le chiffrement Microsoft Point-to-Point Encryption (MPPE) et la compression Microsoft Point-to-Point Compression (MPPC).

102

PROTOCOLE PPTP

- ❑ L'authentification se fait grâce au protocole Ms-Chap de Microsoft.
 - MS-CHAP est la version Microsoft du protocole CHAP (Challenge-Handshake Authentication Protocol).
 - Ce protocole existe en deux versions :
 1. MS-CHAPv1, défini par la RFC 2433, et
 2. MS-CHAPv2, défini par la RFC 2759.
 - Le protocole MS-CHAP-v1 souffre de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire. Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de Ms-Chap plus sûre.
- ❑ La partie chiffrement des données s'effectue grâce au protocole MPPE (Microsoft Point-to-Point Encryption).

103

PROTOCOLE PPTP : Fonction de hachage

- ❑ Une fonction de **hachage** (fonction de condensation) est une fonction permettant d'obtenir un condensé (haché ou en anglais message digest) d'un texte, i.e une suite de caractères assez courte représentant le texte qu'il condense.
- ❑ La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair.



104

PROTOCOLE L2TP

Layer 2 Tunneling Protocol (L2TP) signifie protocole de tunnellation de niveau 2.

- ☐ Il s'agit d'un protocole réseau utilisé pour créer des réseaux privés virtuels (VPN), le plus souvent entre un opérateur de collecte de trafic (dégroupeur ADSL ou opérateur de téléphonie pour les accès RTC) et les fournisseurs d'accès à Internet.
- ☐ Le protocole combine des fonctionnalités de deux protocoles tunnel : **Layer 2 Forwarding (L2F)** de Cisco et **Point-to-point tunneling protocol (PPTP)** de Microsoft.

105

PROTOCOLE IPSec

- ☐ IPsec (Internet Protocol Security) est un ensemble de règles ou de protocoles de communication permettant d'établir des connexions sécurisées sur un réseau. Le protocole Internet (IP) est la norme commune qui détermine comment les données circulent sur Internet. IPsec ajoute le chiffrement et l'authentification pour rendre le protocole plus sûr.
- ☐ Le protocole IP Sec, développé par l'IETF (Internet Engineering Task Force) dans les années 1990, il a pour but de **Sécuriser** TCP/IP par l'authentification et le chiffrement des paquets IP afin de protéger les transmissions de données.
- ☐ IPsec natif sur IPv6 et optionnel sur IPv4. Adaptée à IPv4, vu la lenteur de déploiement IPv6 et les besoins forts des entreprises.
- ☐ Normalisation d'IPsec
Série de RFC : 2401, 2402, 2406, 2408

106

Exemples des utilisations d'IPSec

IPsec peut être utilisé pour les fonctions suivantes :

- ☐ Chiffrer les données des applications.
- ☐ Sécuriser une connexion de succursale sur Internet
- ☐ Accès à distance sécurisé sur Internet. Assurer la sécurité du routeur lors de l'envoi de données sur l'Internet public.
- ☐ Etablir des liens Intranet et Extranet avec des partenaires
- ☐ Améliorer la sécurité du e-commerce. Protéger les données du réseau en mettant en place des circuits chiffrés, appelés tunnels IPsec, qui chiffreront toutes les données envoyées entre deux points de terminaison.
- ☐ Authentifier rapidement les données si elles proviennent d'un expéditeur connu.

107

Modes d'exploitation d'Ipsec

1. Mode Transport

Il existe deux modes (mode Transport et mode Tunnel) pour IPsec :

- ☐ Le **mode transport** permet de protéger principalement les protocoles de niveaux supérieurs :
 - IPsec récupère les données venant de la couche 4 (TCP/transport), les signe et les crypte puis les envoie à la couche 3 (IP/réseau).
 - Cela permet d'être transparent entre la couche TCP et la couche IP et d'être relativement facile à mettre en place.
 - Il y a des inconvénients :
l'entête IP est produite par la couche IP et donc IPsec ne peut pas la contrôler.

108

Modes d'exploitation d'Ipsec

2. Mode tunnel

Il permet d'encapsuler des datagrammes IP dans des datagrammes IP

- les paquets descendent dans la pile jusqu'à la couche IP et c'est la couche IP qui passe ses données à la couche IPSec.
- Il y a donc une entête IP encapsulée dans les données IPSec et une entête IP réelle pour le transport sur Internet

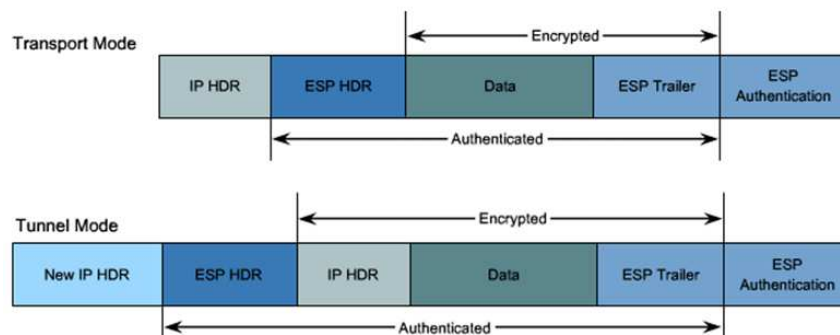
Avantages :

- l'entête IP réelle est produite par la couche IPSec. Cela permet d'encapsuler une entête IP avec des adresses relatives au réseau virtuel et en plus de les crypter de façon à être sûr qu'elles ne sont pas modifiées.
- On a des adresses IP virtuelles tirant partie au mieux du concept de VPN.
- On a le contrôle total sur l'entête IP produite par IPSec pour encapsuler ses données et son entête IPSec.

109

Modes d'exploitation d'Ipsec

Mode transport vs Mode tunnel



110

Composants d'IPsec

❑ Protocoles de sécurité :

- Authentication Header (AH)
- Encapsulation Security Payload (ESP)

❑ Protocole d'échange de clefs :

- Internet Key Exchange

❑ Bases de données internes :

- Security Policy Database (SPD)
- Security Association Database (SAD)

111

Protocoles de sécurité :

Authentication Header (AH)

❑ Le protocole d'en-tête d'authentification (AH) ajoute un en-tête qui contient les données d'authentification de l'expéditeur et protège le contenu du paquet contre toute modification par des parties non autorisées. Il avertit le destinataire d'éventuelles manipulations du paquet de données d'origine. Lorsqu'il reçoit le paquet de données, l'ordinateur compare le calcul du hachage cryptographique de la charge utile avec l'en-tête pour s'assurer que les deux valeurs correspondent. Un hachage cryptographique est une fonction mathématique qui résume les données en une valeur unique.

- Defined in RFC 1826
- Integrity: Yes, including IP header,
- Authentication: Yes
- Non-repudiation: Depends on cryptography algorithm.
- Encryption: No
- Replay Protection: Yes

112

Protocoles de sécurité :

Encapsulation Security Payload (ESP)

- ❑ Selon le mode IPSec sélectionné, le protocole ESP effectue le chiffrement de l'ensemble du paquet IP ou uniquement de la charge utile. ESP ajoute un en-tête et une bande de fin au paquet de données lors du chiffrement.
- ❑ Définit dans le RFC 2406
- ❑ Seules les données sont protégées (pas de protection en-tête)
- ❑ Garantit:
 - l'authentification.
 - l'unicité (anti-rejeu)
 - l'intégrité
 - la confidentialité

113

Protocole d'échange de clés :

Internet Key Exchange (IKE)

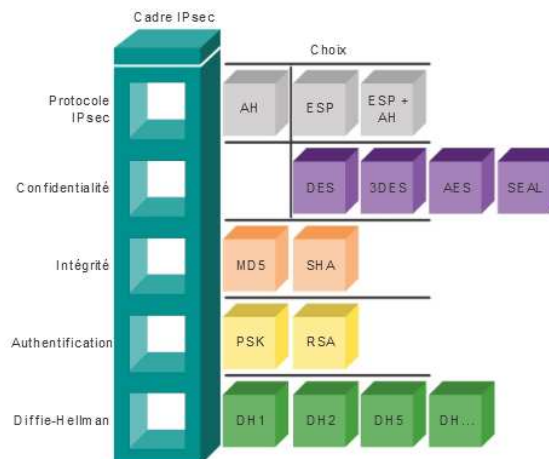
- ❑ L'Internet Key Exchange (IKE) est un protocole qui établit une connexion sécurisée entre deux appareils sur Internet. Les deux appareils établissent une association de sécurité (SA), qui implique la négociation de clés et d'algorithmes de chiffrement pour transmettre et recevoir les paquets de données suivants.
- ❑ Prend en charge la gestion des clés de cryptographie.
- ❑ Port UDP 500
- ❑ RFC 4306

114

PROTOCOLE IPsec : Cadre du protocole IPsec

❑ La Figure suivante illustre les composants de la configuration IPsec. Le cadre IPsec comporte quatre éléments constitutifs de base qui doivent être sélectionnés.

- Confidentialité (en cas d'implémentation du protocole IPsec avec la technologie ESP)
- Intégrité
- Authentification
- Groupe d'algorithmes DH



PROTOCOLE IPsec : Cadre du protocole IPsec (suite)

- ❑ **Cadre du protocole IPsec** : lors de la configuration d'une passerelle IPsec en vue de fournir des services de sécurité, un protocole IPsec doit être sélectionné. Les choix possibles sont des combinaisons des technologies ESP et AH. De manière réaliste, les options ESP ou ESP+AH sont presque toujours sélectionnées, car la méthode AH elle-même ne permet pas le chiffrement, comme le montre la Figure.
- ❑ **Confidentialité (en cas d'implémentation du protocole IPsec avec la technologie ESP)** : l'algorithme de chiffrement sélectionné doit de préférence correspondre au niveau de sécurité souhaité : DES, 3DES ou AES. L'algorithme AES est fortement recommandé, avec AES-GCM pour une sécurité maximale.
- ❑ **Intégrité** : garantit que le contenu n'a pas été modifié lors du transit. Implémenté par le biais de l'utilisation d'algorithmes de hachage. Les choix possibles incluent les algorithmes MD5 et SHA.
- ❑ **Authentification** : représente la manière selon laquelle les périphériques sont authentifiés à chaque extrémité du tunnel VPN. Les deux méthodes sont PSK ou RSA.
- ❑ **Groupe d'algorithmes DH** : représente la manière selon laquelle une clé secrète partagée est établie entre des homologues. Diverses options sont possibles, mais l'algorithme DH24 est celui qui offre le plus de sécurité.
- ❑ La combinaison de ces éléments constitutifs offre les options de confidentialité, d'intégrité et d'authentification des VPN IPsec.

PROTOCOLE IPSec : Fonctionnement

Lors de l'établissement d'une connexion IPsec, plusieurs opérations sont effectuées :

❑ Échange des clés

un canal d'échange de clés, sur une connexion UDP depuis et vers le port 500 (ISAKMP (en) pour Internet Security Association and Key Management Protocol).

- Le protocole IKE (Internet Key Exchange) est chargé de négocier la connexion. Avant qu'une transmission IPsec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées. Ce protocole permet deux types d'authentifications, PSK (secret prépartagé ou secret partagé) pour la génération de clefs de sessions RSA ou à l'aide de certificats.
 - Ces deux méthodes se distinguent par le fait que l'utilisation d'un certificat signé par une tierce-partie appelée Autorité de certification (CA) assure l'authentification. Tandis qu'avec l'utilisation de clefs RSA, une partie peut nier être à l'origine des messages envoyés.
 - IPsec utilise une association de sécurité (Security association) pour dicter comment les parties vont faire usage de AH (Authentication header), protocole définissant un format d'en-tête spécifique portant les informations d'authentification, et de l'encapsulation de la charge utile d'un paquet.

117

PROTOCOLE IPSec : Fonctionnement

Lors de l'établissement d'une connexion IPsec, plusieurs opérations sont effectuées :

❑ Transfert des données

Un ou plusieurs canaux de données par lesquels le trafic du réseau privé est véhiculé, deux protocoles sont possibles :

- le protocole AH, (Authentication Header) fournit l'intégrité et l'authentification. AH authentifie les paquets en les signant, ce qui assure l'intégrité de l'information. Une signature unique est créée pour chaque paquet envoyé et empêche que l'information soit modifiée.
- le protocole ESP (Encapsulating Security Payload), en plus de l'authentification et l'intégrité, fournit également la confidentialité par l'entremise de la cryptographie.

118

OpenVPN

Qu'est ce que l'open vpn ?

- ❑ **OpenVPN** est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Son développement a commencé le 13 mai 2001 grâce à James Yonan.
- ❑ OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe.
- ❑ Il utilise de manière intensive la bibliothèque d'authentification **OpenSSL** ainsi que le protocole **SSLv3/TLSv1**.
- ❑ Disponible avec une multitude d'environnements tel que Solaris, OpenBSD, FreeBSD, NetBSD, Linux (**Debian**, Redhat, Ubuntu, etc.), Mac OS X, **Windows** 7, 8, 10 et 11 il offre de nombreuses fonctions de sécurité et de contrôle.
- ❑ OpenVPN **n'est pas compatible** avec **IPsec** ou d'autres logiciels VPN. Le logiciel contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie.

119

OpenVPN

Principe

- ❑ Open VPN est une solution relativement complète qui permet plusieurs modes de fonctionnement, plusieurs modes d'encapsulation et plusieurs méthodes d'authentification. Le point fort d'Open VPN est sa capacité à fonctionner presque sans configuration dès lors que l'on possède une PKI. Ce qui le rend très attractif pour la mise en place d'une solution de connexion à distance pour les employés d'une entreprise.
- ❑ **Openvpn** est une solution de **tunnelisation Open Source**, il utilise la bibliothèque d'**OpenSSL**.
- ❑ Il existe 2 configurations possibles d'OpenVPN suivant le type de réseau que l'on souhaite mettre en place et suivant le contexte réseau :
 1. VPN ponté (couche 2)
 2. VPN routé (au dessus de la couche 2)
 - La configuration VPN routé est plus performant et plus fiable que le ponté.
 - Le VPN ponté est utilisé dans une architecture réseau local, alors que le VPN routé peut aussi bien être utilisé dans cette architecture que pour relier 2 réseaux à travers l'internet.

120

Avantages et Inconvénients

Avantages

- ❑ Nombreux sont les avantages du open VPN. D'abord, c'est un service qui permet à l'utilisateur de crypter sa connexion. Elle permet aussi de changer d'IP. Open VPN offre la meilleure vitesse et une plus grande sécurité pendant votre connexion VPN.

Inconvénients

- ❑ Open VPN est moins facile à installer que d'autres protocoles VPN, et l'installation d'un VPN avec Open VPN peut être complexe pour certains clients, vu qu'elle nécessite d'installer une application spéciale pour le client. Le protocole Open VPN n'est pas non plus pris en charge par certains appareils mobiles, ce qui peut être un inconvénient important pour l'utilisation d'un VPN mobile. Nombreux sont ses points faibles : bande passante limitée, temps de connexion limitée, taux de chiffrement très bas, très peu de serveurs VPN disponible support client non professionnel, coupures fréquentes de la connexion....

121

Bibliographie

1. <http://eventus-networks.blogspot.com/2013/11/les-topologies-physiques-et-logiques.html>
2. https://fr.wikipedia.org/wiki/IEEE_802.3
3. Hardware support : <http://www.cisco.com/public/support/tac/hardware.shtml>
4. <http://www.cisco.com/>
5. <https://fr.scribd.com/doc/142546820/PresentationVPN-ppt>
6. <http://cisco.ofppt.info/ccna4/course/module2/2.2.3.5/2.2.3.5.html>
7. http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours_secu_2_3_VPN.pdf
8. <http://cisco.ofppt.info/ccna4/course/module7/index.html#7.1.2.2>
9. <https://lazaarsaiida.wordpress.com/wp-content/uploads/2015/11/vpn1.pdf>
10. https://helios2.mi.parisdescartes.fr/~mea/cours/DU/IPsec_DUsec.pdf
11. <https://aws.amazon.com/fr/what-is/ipsec/>
12. <http://cisco.ofppt.info/ccna4/course/module7/7.3.2.6/7.3.2.6.html>
13. <https://fr.scribd.com/document/480077575/Expose-Open-VPN-pdf>

122