GUIA DE CONNEXIÓ A LA XARXA (Linux/Unix)

Objectiu

Aquesta guia descriu el procediment complet per connectar ordinadors portàtils amb sistemes operatius Unix/Linux a la xarxa de la Universitat; la connexió segura s'estableix mitjançant un programari específic (FreeSwan) que facilita la configuració de la capacitat VPN del mateix sistema operatiu. Tot i amb això, cal remarcar que tota la configuració és pot fer directament amb el suport d'IPSEC del kernel, mitjançant l'activació dels mòduls de suport corresponents.

Cal tenir present, que la xarxa sense fils és insegura, de manera que si voleu garantir la confidencialitat en les comunicacions, heu de fer servir el mètode de connexió segura.

Aquest procediment serà el mateix tant si la connexió es fa a través d'una comunicació sense fils (targeta de xarxa basada en l'estàndard 802.11b i certificada WiFi) com si es fa des de cablejat estructurat (targeta Ethernet 10/100 i el corresponent cable).

Procediment de connexió

1. Connexió no segura

El procediment de connexió descrit a continuació caldrà realitzar-lo únicament la primera vegada que s'accedeixi a la xarxa així com quan, per qualsevol motiu, hagin estat modificades les configuracions resultants d'aquest procediment.

- **Configuració TCP/IP**

Aquesta primera consisteix en verificar que es té configurat el protocol TCP/IP de l'ordinador portàtil de manera dinàmica, mitjançant el protocol DHCP. La xarxa està preparada per rebre peticions dinàmiques dels clients i respondre el conjunt de paràmetres que configuraran correctament l'entorn TCP/IP.

2. Connexió segura

El procediment de connexió descrit a continuació caldrà realitzar-lo únicament la primera vegada que s'accedeixi a la xarxa així com quan, per qualsevol motiu, hagin estat modificades les configuracions resultants d'aquest procediment.

L'objectiu d'aquesta fase és crear la connexió segura mitjançant un programari específic que faciliti la configuració de la capacitat VPN del mateix sistema operatiu.

Durant aquest procés, i depenent de la configuració inicial, pot ser necessari reiniciar l'ordinador diverses vegades. En aquest cas, cal reprendre aquest procés de connexió en el punt on ha quedat interromput.

Així, i un cop configurada correctament aquesta connexió, l'activació per accedir a la xarxa en el treball diari i la desactivació es realitzarà d'acord amb les indicacions de l'apartat **Activació de la connexió** d'aquest mateix document i no requerirà la repetició del procediment de connexió actual.

El procediment que cal seguir és el següent:

0. Configuració TCP/IP:

Aquesta primera consisteix en verificar que es té configurat el protocol TCP/IP de l'ordinador portàtil de manera dinàmica, mitjançant el protocol DHCP. La xarxa està preparada per rebre peticions dinàmiques dels clients i respondre el conjunt de paràmetres que configuraran correctament l'entorn TCP/IP.

1. Descarregar he instal·lar els paquets de FreeSwan. Trobareu tota la informació necessària als següents links:

   - Site general de FreeSwan http://www.freeswan.org
   - Documentació de FreeSwan http://www.freeswan.org/doc.html
   - Descàrrega de paquets ftp://ftp.xs4all.nl/pub/crypto/freeswan/

2. Fitxers de configuració específics per la xarxa oberta de la Universitat:

   2.1. Descripció genèrica de la VPN

   El túnel VPN que s'estableix entre el client i l'extrem de la xarxa, empra l'estàndard IPSEC, amb encriptació ESP i secret compartit.

   2.1. Fitxer ***/etc/ipsec.secrets***

```
#
# Configuració de la clau compartida
#

10.100.100.2          10.100.200.231          "urvpassword"
```

   On:

   10.100.100.2 És l'extrem de la xarxa, aquest paràmetre és fix

   10.100.200.231 És l'adreça IP dinàmica que ens ha assignat la xarxa. Aquest paràmetre caldrà verificar-ho cada cop que reiniciem l'ordinador.

   "urvpassword" És la clau compartida, aquest paràmetre és fix

   2.2. Fitxer ***/etc/ipsec.conf***

```
#
# Configuració del túnel VPN
#

config setup
        interfaces=”ipsec0=eth0”
        klipsdebug=none
        plutodebug=none
        manualstart=
        plutoload=
        plutostart=

conn linux-tunnel
        type=tunnel
        left=%defaultroute
        right=10.100.100.2
        rightsubnet=0.0.0.0/0
        authby=secret
        keyexchange=ike
        auth=esp
        pfs=no
```

On:

eth0 És el nom de la interfície de xarxa a emprar

10.100.100.2 És la ruta per defecte de la xarxa oberta

%defaultroute És substitueix automàticament per l'adreça IP dinàmica que ens ha assignat la xarxa. Aquest paràmetre caldrà verificar-ho cada cop que reiniciem l'ordinador.

- **Activació de la connexió**

Per a cada sessió de treball caldrà realitzar les següents actuacions:

- Comprovar que la configuració disponible a l'ordinador portàtil és la resultant del **Procediment de connexió** descrita a l'apartat anterior

- Activar la connexió segura, prèviament configurada:
  /etc/init.d/ipsec stop
  /etc/init.d/ipsec start
  ipsec auto –-add linux-tunnel
  ipsec auto --up linux-tunnel

- Obrir el navegador d'Internet

- Indicar la pàgina web desitjada

- Inserir la identificació d'usuari requerida per accedir al servei

- El servei permetrà l'accés a diferents serveis i recursos electrònics de la Universitat i, per extensió, d'Internet

- Per tancar la sessió, desactivar la connexió segura establerta a l'inici de la sessió