Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

# Práctica 8: Uso de Redes Privadas Virtuales (VPN)

## *1- Introducción*

Conforme ha ido pasado el tiempo las empresas han visto la necesidad de que las redes de área local superen la barrera de lo local permitiendo la conectividad de su personal y oficinas en otros edificios, ciudades e incluso países.

Desgraciadamente, en el otro lado de la balanza se encontraban las grandes inversiones que era necesario realizar tanto en hardware como en software y por supuesto, en servicios de telecomunicaciones que permitieran crear estas redes de servicios.

Afortunadamente con la aparición de Internet, las empresas, centros de formación, organizaciones de todo tipo e incluso usuarios particulares tienen la posibilidad de crear una Red Privada Virtual (VPN) que permita, mediante una moderada inversión económica y utilizando Internet, la conexión entre diferentes ubicaciones salvando la distancia entre ellas.

Las redes virtuales privadas utilizan protocolos especiales de seguridad que permiten obtener acceso a servicios de carácter privado, únicamente a personal autorizado, de una empresa, centros de formación, organizaciones, etc.; cuando un usuario se conecta vía Internet, la configuración de la red privada virtual le permite conectarse a la red privada del organismo con el que colabora y acceder a los recursos disponibles de la misma como si estuviera tranquilamente sentado en su oficina. Todo ello con unos niveles de seguridad altos a pesar de utilizar un medio no confiable como Internet.

**¿Qué es una VPN?**

Realmente una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público (no confiable a priori), pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas. Al fin y al cabo no es más que la creación, en una red pública, de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.

## *2- Objetivos*

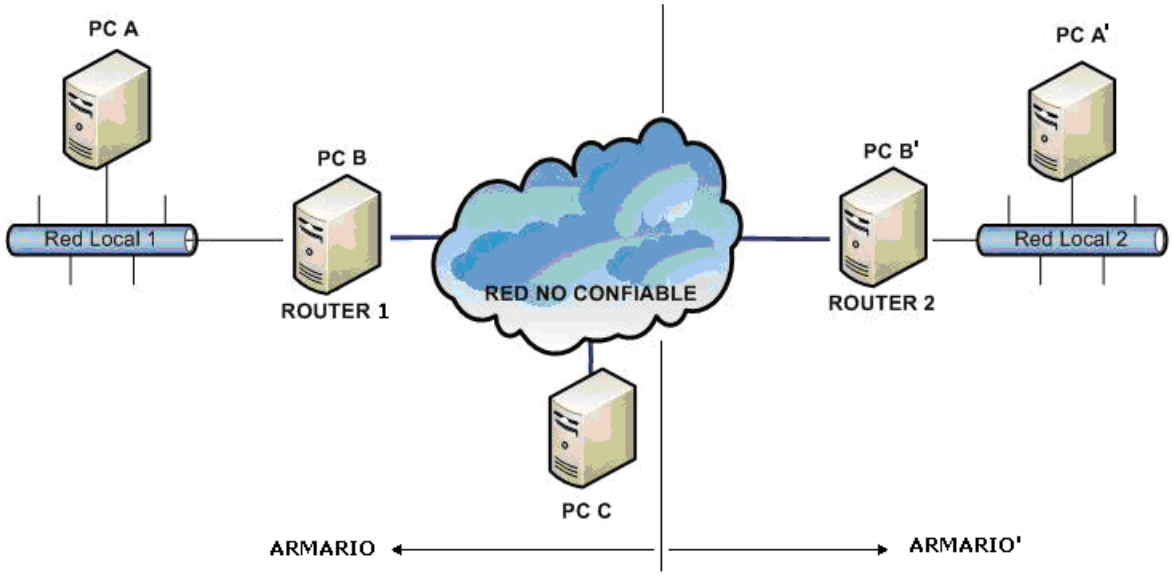
1. Conocer los riesgos de utilizar una red no confiable (como Internet) para el envío de comunicaciones empresariales.

2. Configurar una VPN de sitio a sitio creando la extensión segura de nuestra red local.

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

## *3- Escenario inseguro*




| | |
|---|---|
| ARMARIO:<br>1. Red Local 1 (VLAN1):<br>Red: 192.168.1.0/24<br>2. PC A:<br>IP: 192.168.1.2 /24<br>Router por defecto: 192.168.1.1<br>3. PCB (Router 1):<br>IP: 192.168.1.1/24 | ARMARIO ':<br>4. Red Local 2 (VLAN3)<br>Red: 192.168.2.0/24<br>5. PC A': (Router 2):<br>IP: 192.168.2.2<br>Router por defecto: 192.168.2.1<br>6. PC B'(Router 2):<br>IP: 192.168.2.1/24 |
| 7. Red No Confiable (HUB)<br>Red: 10.0.0.0/24<br>8. PC C:<br>IP: 10.0.0.3/24 | *Complete la configuración de los interfaces restantes conectados a la red no confiable ¿A qué equipos corresponderán estos interfaces?* |

*Comprueba la configuración del escenario propuesto. Debe permitirnos comunicarnos entre todos los elementos de la maqueta. ¿Qué dispositivo de red, de entre los disponibles en su armario, puede utilizar para recrear el escenario propuesto; red no confiable? Debe permitirle, desde* PC-C, (con tcpdump o wireshark) "ver" la información que viaja por la red.

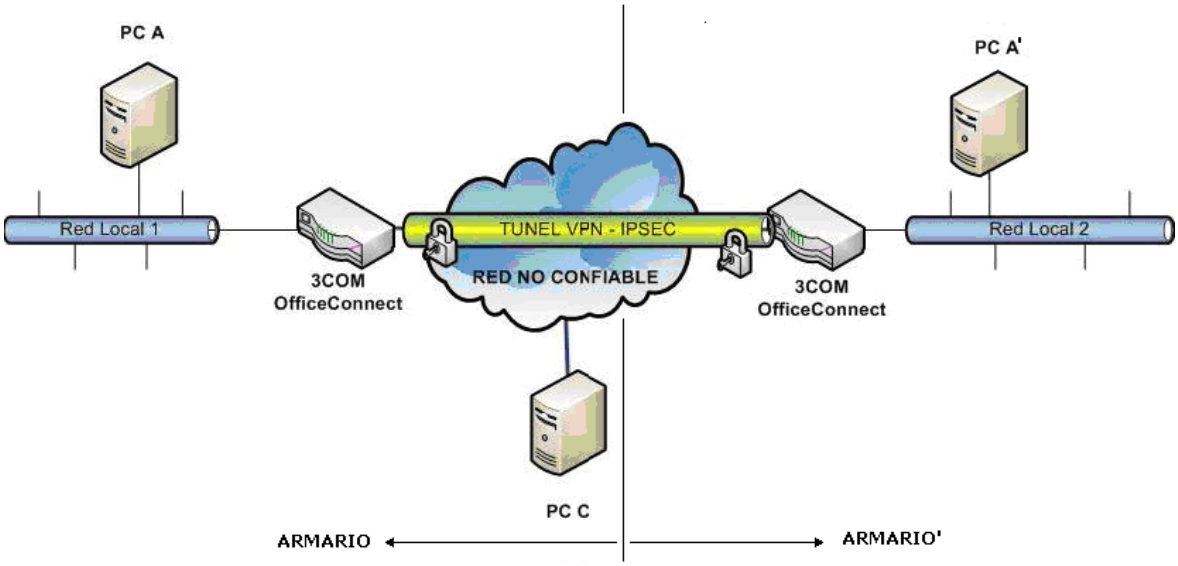
Establece una comunicación entre los equipos PC-A y PC-A' abriendo un socket(nc –l <puerto>) en uno de ellos (por ejemplo en PC-A') y una conexión (telnet o nc) desde el otro (PC-A).

Checkpoint 8.1: Mostrar al profesor que puedes ver los datos de la comunicación desde "Internet".

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

## *3- Escenario seguro*




ARMARIO:

1. Red Local 1 (VLAN1):
   Red: 192.168.1.0/24
2. PC A:
   IP: 192.168.1.2
   Router por defecto: 192.168.1.1

ARMARIO':

3. Red Local 2 (VLAN3)
   Red: 192.168.2.0/24
4. PC A':
   IP: 192.168.2.2
   Router por defecto: 192.168.2.1

5. Red No Confiable (HUB)
   Red: 10.0.0.0/24
6. PC C:
   IP: 10.0.0.3/24

*El resto de la configuración, relativa a los interfaces WAN de los equipos 3COM, se indica, a continuación, en el siguiente punto.*

**Configuración de los 3COM OfficeConnect**

Dispone de dos "3com Office Connect VPN Firewall". Por defecto, para su configuración, la IP a la que responden es: http://192.168.1.1 *en cualquiera de sus interfaces LAN*. La password de administración es ***admin***.

Tenga en cuenta que cuando cambie en "OfficeConnect 2" su dirección IP LAN, debe cambiar también la dirección IP del equipo desde el que lo gestiona, ¿Por qué?

Departamento de
Automática y Computación
*Automatika eta*
*Konputazio Saila*

Campus de Arrosadía
*Arrosadiko Campusa*
31006 Pamplona - *Iruñea*
*Tfno. 948 169113, Fax. 948 168924*
*Email: ayc@unavarra.es*

| 3com OfficeConnect 1 (OC1) | 3com OfficeConnect 2 (OC2) |
|---|---|
| IP LAN: 192.168.1.1/24 | IP LAN: 192.168.2.1/24 |
| IP WAN:<br>(Internet Settings), estática: 10.0.0.1/24 | IP WAN:<br>(Internet Settings), estática: 10.0.0.2/24 |
| Gateway por defecto: 10.0.0.254 | Gateway por defecto: 10.0.0.254 |
| DNS1: 10.0.0.10 | DNS1: 10.0.0.10 |
| Servidor DHCP: desactivado | Servidor DHCP: desactivado |

*Nota: No intente realizar una comunicación entre todos los elementos antes de establecer la red VPN ya que estos aparatos tienen integrado un FireWall que evita el tráfico entrante y además hace NAT por lo que habría que configurarlo antes… (no es el objetivo de esta práctica).*

Configura una red VPN entre OC1 y OC2 de red a red, para ello deberás utilizar IPSEC ya que es el único protocolo soportado para una comunicación Red a Red.

*Nota: en su interfaz web, el 3COM OfficeConnect, dispone de un botón de ayuda en cada campo de configuración. Recurra también a su manual de usuario colgado en la página web de la asignatura, así como a los conceptos que, sobre VPNs, ha adquirido en clase de teoría.*

Establece la conexión VPN y compruébala. Revisa los logs de los "3COM OfficeConnect". Comprueba la comunicación entre PC-A y PC-A'. Abre un socket en uno de ellos y conéctate desde el otro.

Intenta sniffar información desde PC-C ¿Ves algo?

Checkpoint 8.2: Muestre al profesor que ha establecido la conexión a través del túnel y lo que se ve desde PC-C. ¿Explique el significado de la captura de PC-C?

¿Podría realizar un ataque "MITM" en la comunicación ipsec al estilo del ataque "Man in the Middle" sobre el protocolo ssh? ¿Por qué?