

SEGURIDAD Y ALTA DISPONIBILIDAD TEMA 3: Implantación de técnicas de acceso remoto. Seguridad perimetral

Nicolás Madrid Gallego Seguridad y alta disponibilidad 26/01/2012



Contenido

SEGURIDAD PERIMETRAL:
1.NAT:4
Comprobación de la seguridad perimetral a través de un NAT (Laboratorio virtual)4
2. Router frontera:9
a) Planteamiento escenario CISCO Packet Tracert: esquema
b) Realiza una comparativa entre los routers frontera atendiendo a las opciones de seguridad perimetral (NAT,Firewall,DMZ,etc)9
3. DMZ:
a) Planteamiento de escenarios DMZ en Cisco (Packet Tracert): esquemas16
b)Planteamiento de escenarios DMZ en Linux (laboratorio virtual): esquemas17
4.VPN sobre red local
a) Instalación de un servidor VPN en Windows XP18
b) Instalación de un servidor VPN en Windows 2003/200824
c) Instalación de un servidor VPN en GNU/Linux27
d) Conexión desde un cliente Windows y GNU/Linux VPN a un servidor VPN29
5. VPN de acceso remoto
b) Configurar el router Linksys RV200 como un servidor VPN de acceso remoto35
c) Configura tu cliente VPN en Windows
REDES PRIVADAS VIRTUALES
6. VPN sitio a sitio41
TECNICAS DE CIFRADO: COMUNICACIONES SEGURAS
7. SSH
a) Instalación del servidor SSH en GNU/Linux43
b) Conexión al servidor SSH mediante cliente GNU/Linux y cliente Windows43
c) Escenario CISCO: Conexión segura a la administración de un router
SERVIDORES DE ACCESO REMOTO
8. Protocolos de autenticación:
a) Escenarios CISCO: Interconexión de redes mediante protocolos PPP,PAP,CHAP47
SERVIDORES DE ACCESO REMOTO
9. Servidores de autenticación50
a) REDES INALÁMBRICAS: WPA Personal50
b) SERVIDOR RADIUS:

1	Simulación de un entorno de red con servidor RADIUS CISCO en el Packet Tracert Route	ſ.
	5	3
2 cor <i>Cor</i>	Instalación de un servidor Radius bajo GNU/LINUX (freeradius) , para autenticar nexiones que provienen de un router de acceso Linksys WRT54GL: WPA Empresarial. mprobación en un escenario real6	1
3 pro	Instalación de un servidor Radius bajo Windows para autenticar conexiones que ovienen de un router de acceso Linksys WRT54GL. <i>Comprobación en un escenario real</i> 6	4
4 infi	Busca información sobre EDUROAM y elabora un breve informe sobre dicha raestructura. http://www.eduroam.es/6	4
c) SEF	RVIDOR LDAP:6	6
1	Instalación de un servidor OpenLDAP GNU/LINUX (OpenLDAP).	6
2	Instalación de un cliente LDAP bajo Windows o GNU/Linux para autenticarse7	8
3	Busca información sobre LDAP y su implementación en productos comerciales7	8

SEGURIDAD PERIMETRAL:

1.NAT:

Comprobación de la seguridad perimetral a través de un NAT (Laboratorio virtual)

Nuestro escenario sera el siguiente:

Esta práctica la realizaremos haciendo uso del NAT del VMWARE, para ello en primer lugar iremos a la pestaña edit/virtual Network Editor para ver la configuración de nuestro nat:



En la pantalla podremos ver que nuestro NAT usa la dirección de red 10.2.8.0 /24 para la traducción de las direcciones:

Name	Type	External Connection	Host Connection	DHCP	Subnet Address	
VMnet1	Host-only	-	Connected	Enabled	192.168.220.0	
VMnet2	Custom	-	-	-	192.168.238.0	
VMnet3	Custom	-	-	-	192.168.23.0	
/Mnet4	Custom	-	-	-	192.168.134.0	
/Mnet5	Custom	-	-	-	192.168.47.0	
/Mnet6	Custom	-	-	-	192.168.174.0	
VMnet7	Custom	-	-	-	192.168.100.0	l
VMnet8	NAT	NAT	Connected	Enabled	10.2.8.0	
/Mnet9	Custom	-	-	-	192.168.20.0	
Bridg	ed (connect Vi led to: Autor	Ms directly to the external ne	etwork)	~	Automatic Settings	
Bridg	ed (connect Vi ed to: Autor	Ms directly to the external ne natic	etwork)	*	Automatic Settings	
 Bridg Bridg NAT (Host- 	ed (connect Vi led to: Autor (shared host's only (connect	Ms directly to the external ne natic IP address with VMs) VMs internally in a private ne	etwork)	Ŧ	Automatic Settings	
Bridg NAT (Host-	ed (connect vi ed to: Autor (shared host's only (connect ect a host virt	Ms directly to the external ne natic IP address with VMs) VMs internally in a private ne ual adapter to this network	etwork)	~	Automatic Settings	
Bridg NAT (Host- Kost	ed (connect Vi ed to: Autor (shared host's only (connect ect a host virt virtual adapte	Ms directly to the external ne natic IP address with VMs) VMs internally in a private ne ual adapter to this network r name: VMware Network Ad	etwork) etwork) dapter VMnet8		Automatic Settings	
Bridg Bridg Onn Host- Host Use lo	ed (connect vi shared host's only (connect ect a host virt virtual adapte ocal DHCP ser	Ms directly to the external ne matic IP address with VMs) VMs internally in a private ne ual adapter to this network er name: VMware Network Ar vice to distribute IP address	etwork) etwork) dapter VMnet8 to VMs	~	Automatic Settings NAT Settings DHCP Settings	

El cliente Molinux está en VMnet 8 (NAT) que actua como un switch conectado a equipo con el servidor NAT integrado.

Virtual Machine Setting: Hardware Options	s	
Device Memory Processors Hard Disk (SCSI) CD/DVD (IDE) Floppy Network Adapter USB Controller Sound Card Printer Display	Summary 512 MB 1 20 GB Using file C:\Users\HP Pavilio Auto detect Custom (VMnet2) Present Auto detect Present Auto detect	Device status
	Add <u>R</u> emove	
		OK Cancel Help

El Cliente XP, actúa como NAT:

Virtual Machine Settings	a (10.000) (×.
Device Memory Processors Hard Disk (IDE) CD/DVD (IDE) Network Adapter Sound Card Printer Display	Summary 512 MB 1 30 GB Using file F:\ssooVirtuales\I NAT Present Auto detect Present Auto detect	Memory Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB. Memory for this virtual machine: 512 * MB 32 GB - 16 GB - 8 GB - 4 GB - Maximum recommended memory 2 GB - Maximum recommended memory 1 GB - 7092 MB 512 MB - 4 256 MB - Recommended memory 128 MB - 512 MB 64 MB - 128 MB 16 MB - 128 MB
	Add Remove	

El cliente Ubuntu que esta en modo Bridge es decir esta fuera del NAT.

Virtual Machine Settings	······································	-	— ×-
Hardware Options			
Device Processors Hard Disk (SCSI) CD/DVD (IDE) Floppy Sound Card Printer Display	Summary 1024 MB 1 20 GB Auto detect Auto detect Bridged Present Auto detect Present Auto detect Vresent Auto detect	Memory Specify the machine. T Memory for 32 GB - 16 GB - 8 GB - 4 GB - 2 GB - 1 GB - 2 GB - 1 GB - 512 MB - 256 MB - 128 MB - 16 MB - 8 MB - 8 MB - 4 MB -	e amount of memory allocated to this virtual The memory size must be a multiple of 4 MB. or this virtual machine: 1024 m MB MB Maximum recommended memory (Memory swapping may occur beyond this size.) 7092 MB Recommended memory 512 MB Guest OS recommended minimum 256 MB
	Add Remove		
			OK Cancel Help

La practica será la siguiente desde el cliente Molinux en VMnet8 (NAT) realizaremos un ping al cliente Bridge(Ubuntu), de modo que nos tiene que dejar:

root@molinux: /home/primoguijarro	×
<u>A</u> rchivo <u>E</u> ditar <u>V</u> er <u>B</u> uscar <u>T</u> erminal Ay <u>u</u> da	
64 bytes from 192.168.2.33: icmp_req=4 ttl=128 time=0.507 ms	▲
64 bytes from 192.168.2.33: icmp_req=5 ttl=128 time=0.577 ms	
64 bytes from 192.168.2.33: 1cmp_req=6 ttl=128 time=0.540 ms	
192 168 2 33 ping statistics	
6 nackets transmitted 6 received 0% nacket loss time 4999ms	
$r_{r_{r_{r_{r_{r_{r_{r_{r_{r_{r_{r_{r_{r$	
root/molinux·/home/primoguijarro#/ping/12/168/2/33	
PING 192, 168, 2, 33, (192, 168, 2, 33), 56(84), bytes of data	
64 bytes from 192.168.2.33: icmp reg=1 tt1=128 time=0.877 ms	
64 bytes from 192.168.2.33: icmp_reg=2 ttl=128 time=0.549 ms	
64 bytes from 192.168.2.33; icmp.reg=3 ttl=128 time=0.527 ms	
64 bytes from 192,168,2,33; jcmp req=4 ttl=128 time=0.594 ms	
^C	
192.168.2.33 ping statistics	
4 packets transmitted, 4 received, 0% packet loss, time 3000ms	
rtt min/avg/max/mdev = 0.527/0.636/0.877/0.144 ms	
root@molinux:/home/primoguijarro# ping 192.168.2.33	
PING 192.168.2.33 (192.168.2.33) 56(84) bytes of data.	
64 bytes from 192.168.2.33: icmp reg=1 ttl=128 time=1.07 ms	
64 bytes from 192.168.2.33: icmp req=2 ttl=128 time=0.494 ms	
64 bytes from 192.168.2.33: icmp req=3 ttl=128 time=0.512 ms	
64 bytes from 192.168.2.33: icmp req=4 ttl=128 time=0.528 ms	
	∇

Sin embargo, si realizamos un ping desde el Ubuntu al Molinux, no nos debe dejar, esto quiere decir que funciona correctamente la seguridad perimetral con NAT.

```
primoguijarro@primoguijarro-desktop:~$ ping 10.2.8.40
PING 10.2.8.40 (10.2.8.40) 56(84) bytes of data.
^C
--- 10.2.8.40 ping statistics ---
20 packets transmitted, 0 received, 100% packet loss, time 19010ms
primoguijarro@primoguijarro-desktop:~$ ping 10.2.8.40
PING 10.2.8.40 (10.2.8.40) 56(84) bytes of data.
```

Ahora probaremos a realizar un ping desde otro equipo que esta fuera de red que tiene activado el NAT:



Como era de esperar el ping ha fallado puesto que al estar activado el NAT los equipos que no están integrados en la red del NAT no pueden acceder a los equipos con NAT.

2. Router frontera:

a) Planteamiento escenario CISCO Packet Tracert: esquema.

En este esquema podremos apreciar 2 empresas en la que él y entre dichas empresas podremos apreciar un router que actúa como router frontera entre ambas empresas:



b) Realiza una comparativa entre los routers frontera atendiendo a las opciones de seguridad perimetral (NAT,Firewall,DMZ,...etc) Router DLINK: http://support.dlink.com/emulators/di604_reve

En este router podemos configurar varias opciones como son:

En primer lugar podremos implementar filtros en los que podremos bloquear ip, direcciones mac, puertos, e incluso podremos de elegir el momento y el dia que queramos que se realice el filtrado:

	Home	Advanced	Tools	Status	Help
Fi	lters				
Fi	lters are used to	allow or deny LAN	users from acce	ssing the Internet.	
ver (c	IP Filters	C LIRI Blog	king		
	MAC Filters	Domain I	Blocking		
ions IP	Filters				
U	se IP Filters to o	deny LAN IP addres:	ses access to th	e Internet.	
	Enabled O	Disabled Clear			
-					
	IP		-		
	Port	-			
	Protocol Type	TCP V			
	Sebedule				
	Schedule	Aiways			
		From time 00	: 00 - AM	• to 00 • : 00	▼ AM ▼
_		day Sun 💌	to Sun 💌		
				<	13 C
IP IP	Filter List			Appl	Cancel Helr
	IP Range	Protoco	al .	Schedule	y cuncer ner
1	*	TCP 20	-21	always	
	*	TCP 80		always	2
	*	TCP 44	3	always	
		UDP 53	1	always	
	*	TCP 25		always	

Otra opción de seguridad de este router en el firewall, aquí podremos permitir o denegar ciertas direcciones de origen a un destino concreto con un protocolo y unos puertos específicos y viceversa, al igual que lo que ocurría con los filtros también podremos configurar si estas configuraciones se aplicaran en un día en concreto o siempre:

	Home	Advanced	Tools	Status	Help
	Firewall Rules	s can be used to allow or	deny traffic from	passing through t	he DI-604.
Virtual Server	C	Enabled 🔘 Disabled	1		
	Name		Clear		
Applications	Action C	│ Allow	IP Range En	d Protocol	Port Range
Filters	Source *	•			
	Destination *	•		TCP 💌	
Firewall	Schedule C	Always			
	C	From time 00 - :	00 🔻 AM 💌	to 00 💌 : 00	▼ AM ▼
DMZ		day Sun 💌	to Sun 💌		
				S	- 😢 🛟
ZoneAlarm	Firewall Rule	s List		Appl	y Cancel Help
	Action Nam	ie	Source	Destination	Protocol
	Allow Allow	w to Ping WAN port	WAN,*	WAN	ICMP,8
	Allow Rem	ote Managment http S	erver WAN,*	LAN, 192. 168.0.1	TCP,80-1080
	Deny Defa	ult	*,*	LAN,*	* *
	Allow Defa	ult	LAN,*	* *	* *

Por último podremos configurar una DMZ:

	Home	Advanced	Tools	Status	Help
	DMZ DMZ (Demilitaria the Internet.	zed Zone) is used to a	allow a single con	nputer on the LAN to	be exposed to
Virtual Server		Enabled Ois	abled		
Applications	IP Address	192 . 168 . 0 . 0			
Filters				3	30
Firewall				Apply	Cancel Help
DMZ					
ZoneAlarm					

Router LINKSYS: http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm

Este router nos ofrece varias opciones de seguridad, de las cuales podemos destacar las siguientes:

En primer lugar podemos encontrar un cortafuegos, en el cual podemos realizar varios tipos de filtros:

LINKSYS [®] A Division of Cisco Systems, Inc.							Firmwa	are Version : v4.30.0
						Wireless-G Broad	Iband Router	WRT54GL
Security	Setup		Wireless	Security	Access Restriction	Applications s & Gaming	Administration	Status
	Firewall	I.	VPN					
Firewall							Firewall Prot	tection : Enable
	Firev	wall Pro	otection : 🔍	Enable 🔘 [Disable		or disable the More	SPI firewall.
Block WAN Requests	v	Block	Anonymous Ir	nternet Request	ts			
	v	Filter	Multicast					
		Filter	Internet NAT R	Redirection				
	\checkmark	Filter	IDENT(Port 113	3)				
								CISCO SYSTEMS
				S	ave Settings	Cancel Changes		antitum (1110)

Tambien podremos realizar una serie de restricciones de acceso según los puertos que configuremos:

LINKSYS [®] A Division of Cisco Systems, Inc.							Firm	ware Version : v4.30.0		
Applications		Wireless-G Broadband Router WRT54GL								
& Gaming	<mark>Setup</mark> Port Range F	Wireless orward	Secur Port Trig	ity Res gering	ccess trictions DMZ	Applications & Gaming QoS	Administration	n Status		
Port Range Forward			Por	t Range			Port Range Certain appli	Forwarding : cations may require		
	Application	Start	End	Protocol	IP Address	s Enable	for it to func Examples of	tion correctly.		
		0 to	0	Both 💌	192.168.1. 0		include servers and certain online games. When a requ	ers and certain s. When a request		
		0 to	0	Both 💌	192.168.1. 0		the Internet, the data to ti	the router will route the computer you		
		0 to	0	Both 💌	192.168.1. 0		specify. Due concerns, y	to security ou may want to limit		
		o to	0	Both 💌	192.168.1. 0		port forward ports you an	ding to only those e using, and		
		0 to	0	Both 💌	192.168.1.0		after you are More	e finished.		
			0	Both 💌	192.168.1					
		0 to	0	Both 👻	192.168.1. 0					
		0 to	0	Both 🔻	192.168.1. 0					
		0 to	0	Both 💌	192.168.1. 0					
								CISCO SYSTEMS		

También podremos configurar una DMZ:

LINKSYS [®] A Division of Cisco Systems, Inc.							Firmwa	are Version : v4.30.0
Applications					Wir	eless-G Broad	band Router	WRT54GL
& Gaming	Setup	Wireless	Security	Access Restriction	s	Applications & Gaming	Administration	Status
	Port Range	Forward	Port Triggering	DMZ	1	QoS		
DMZ	© Er DMZ	nable	le 192.168.1	I. O			DMZ : Enablin expose your n Internet. All po accessible fro More	g this option will router to the orts will be om the Internet CISCO SYSTEMS
			Sav	e Settings	Ca	ncel Changes		ավիտուդիրութ

Por últimos podremos configurar unos parámetros específicos con el objetivo de evitar los ataques QOS

Applications						
& Gaming	Setup W	ireless Securit	y Access Restrictions	Applications & Gaming	Administration	Status
	Port Range Forwa	ard Port Trigg	ering DMZ	QoS		
Wired QoS		C Enable	Disable		Two types of Q	uality of Service
	Upstream Bandwi	idth Auto 🔻	0 Kbps		features are av QoS which com plugged in to the	ailable, Wired trols devices e router with a
Device Priority		Priority	MAC Address		Ethernet cable, QoS, which cor	and Wireless trol devices that
	Device name	Low 🔻 00	: 00 : 00 : 00 : 00	: 00	router.	
	Device name	Low 🔻 00	: 00 : 00 : 00 : 00	: 00	Wired QoS	
					specify priority	for all traffic
Ethernet Port Priority		Priority	Flow Control		by giving the de	vice a Device
	Port 1	Low 🔻	Enable 💌		Name, specifyin entering its MAC	g priority and address.
	Port 2	Low -	Enable 💌		Ethernet Port	Priority : You r data rate
	Port 3	Low 👻	Enable 💌		according to wh	lich physical
	Port 4	Low 👻	Enable 🔻		LAN port your d into. You may a Low priority to o	evice is plugged ssign High or Jata traffic from
Application Priority		Ontimize (aming Applications		devices connec ports 1 through	ted on LAN 4.
		Priority	Specific Port	• #	Application Pr	iority : You may
	Application Name	Low	· 0		control your dat respect to the a consuming band	a rate with pplication that is Iwidth. Check
	Application Name	Low	▼ 0		Optimize Gam Applications to allow common g	ing o automatically jame application
	Application Name	Low	-		ports to have a	higher priority. nize up to eight

Router TP-LINK:

http://www.tplink.com/Resources/simulator/WR842ND(UN)1.0/index.ht m

Las principales medidas de seguridad de este router son las siguientes: En primer lugar podremos ver una sección de seguridad básica en la que podremos activar un firewall, vpn o alg pudiendo en estos 2 ultimos activar o desactivar ciertos protocolos:

TP-LIN	K.	300Mbps Multi-Function Wireless N Router Model No. TL-WR842ND
Status Quick Setup WPS	Basic Security	 SPF Firewall - Statelul Packet Inspection (SPI) helps to prevent opter states by tracking more state per essenti. It validates that the traffic passing through the easient conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world.
Network Wireless DHCP	Firewall SPI Firewall:	VPN - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router. • PPTP Passthrough - PPTP Passthrough, Point-G-Point Tunneling Potocol (PPTP) allows the PointAn-Point Protocol
VPN USB Settings Forwarding Security - Basic Security	VPN PTP Passthrough: Enable Disable Extra passthrough: PSec Passthrough: PSec Passthr	(PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click Enable L 2TP Desstbrough - Layer Two Tunneling Protocol (L2TP) is the method used to enable ProinteR-Poilt essension kit the internet on the Layer Two level. To allow L2TP tunnels to pass through the Router, click Enable. ■ PSec Passtbrough - Internet Protocol security (IPSec) is a
- Advanced Security - Local Management - Remote Management	ALG	over internet Protoco (P) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click Enable.
Parental Control Access Control Advanced Routing	TFTP ALG: Enable Disable H323 ALG: Enable Disable RTSP ALG: Enable Disable	ALG - it is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Attwork Address Translation (NHT) traversat filters to be plugged into the gateway to support address and port translation for certain application layer "controlidata" protocols such as FTP, ITP, IH23 etc.
Bandwidth Control IP & MAC Binding Dynamic DNS	Save	FTP ALG - To allow FTP clients and servers to transfer data across NAT, clickEnable, TTFP ALG - To allow FTP clients and servers to transfer data across NAT, clickEnable, H333 ALG - To allow Microsoft NetMeeting clients to

También encontramos unas opciones avanzadas de seguridad, aquí podremos habilitar el ICMP y varias opciones mas:

TP-LIN	< °		
<u>^</u>	Advanced Security		•
Status			
Quick Setup			
WPS	Packets Statistics Interval (5 ~ 60):	10 Seconds	
Network			
Wireless	DoS Protection:	Oisable Enable	
DHCP			
VPN	Enable ICMP-FLOOD Attack Filtering		
USB Settings	ICMP-FLOOD Packets Threshold (5 ~ 3600);	50 Packets/s	
Forwarding			
Security	Enable UDP-FLOOD Filtering		_
- Basic Security	LIDD ELCOD Backate Threehold (5 - 3600)	E00 Packete/e	
- Advanced Security	ODP-FLOOD Packets Threshold (5 ~ 5000).		
- Local Management			
- Remote Management	Enable TCP-SYN-FLOOD Attack Filtering		
Parental Control	TCP-SYN-FLOOD Packets Threshold (5 ~ 3600):	50 Packets/s	
Access Control			
Advanced Routing	Ignore Ping Packet From WAN Port		
Bandwidth Control	Forbid Ping Packet From LAN Port		
IP & MAC Binding			
Dynamic DNS -	Save Blocked DoS Host List		+

También encontramos opciones de seguridad locales en las que podremos configurar varias direcciones mac permitiendo o denegando su acceso al router

TP-LINK	
Status	
Quick Setup	Local Management
WPS	
Network	Management Bulag
Wireless	All the PCe on the LAN are allowed to access the Pouter's Web Paged Little
DHCP	An the PCs of the Data are anowed to access the Router's web-based of inty
VPN	Only the PCs listed can browse the built-in web pages to perform Administrator tasks
USB Settings	MAC 1:
Forwarding 🗧	MAC 2:
Security	MAC 3:
- Basic Security	MAC 4:
- Advanced Security	Your PC's MAC Address: 6C-62-6D-F7-32-1D Add
- Local Management	
- Remote Management	
Parental Control	Save
Access Control	
Advanced Routing	
Bandwidth Control	
IP & MAC Binding	
Dynamic DNS	

También podremos controlar el accesoa al router mediante listas de control de acceso, ya sea a nivel de host o a nivel de dirección:

TP-LINK	<					
Quick Setup						
WPS	Access Cont	rol Rule Mana	igement			
Network						
Wireless	Enable Internet	Access Control				
DHCP						
VPN						
USB Settings	Default Filter Polic	cy .				
Forwarding	Allow the packe	ts specified by any	enabled access control p	olicy to pass through the	e Router	
Security	Deny the packet	ts specified by any	enabled access control po	olicy to pass through the	Router	
Parental Control			Save			
Access Control						
- Rule	ID. Rule Name	Host	Target	Schedule	Enable	Modify
- Host		nost	larget	Scheudie	LIIUDIC	mouny
- Target	i relax	nome	parents	weenken	V	Edit Delete
- Schedule	Setup Wizard					
Advanced Routing						
Bandwidth Control	Add New	Enable All	Disable All Dele	ete All		
IP & MAC Binding						
Dynamic DNS	Move		ID To ID			
System Tools						
			Drovious	Ourrept No.	1 - Paga	

Por último como en los routers anteriores también podremos definir una DMZ:

TP-LINI	<°	
Status Quick Setup WPS Network	DMZ	
Wireless DHCP VPN	Current DMZ Status: Enable Disable	
USB Settings Forwarding - Virtual Servers	Save	
- Port Inggering - DMZ - UPnP Security		
Parental Control Access Control Advanced Routing		
Bandwidth Control IP & MAC Binding Dvnamic DNS Esperando www.tplink.com		

CONCLUSIÓN

Como conclusión podemos decir que aunque los 3 modelos de router tienen un gran abanico de opciones de seguridad, el que mas opciones de seguridad nos permite en el TP-LINK, por lo tanto en mi opinión este es el mejor router de los 3.

3. DMZ:

a) Planteamiento de escenarios DMZ en Cisco (Packet Tracert): esquemas.

En este esquema podremos ver una DMZ simple en la que se observamos una zona de la empresa local, luego una zona de internet y por útimo una zona desmilitarizada donde se situan los servidores de la empresa:



Otro esquema mas complejo es el siguiente en el que entre el router frontera de la empresa y otro router que es el que da acceso a la red a los equipos encontramos la DMZ:



b)Planteamiento de escenarios DMZ en Linux (laboratorio virtual):

esquemas.

En este esquema podremos ver una DMZ simple en la que se observamos una zona de la empresa local, luego una zona de internet y por útimo una zona desmilitarizada donde se situan los servidores de la empresa:



Otro esquema mas complejo es el siguiente en el que entre el router frontera de la empresa y otro router que es el que da acceso a la red a los equipos encontramos la DMZ:



4.VPN sobre red local

a) Instalación de un servidor VPN en Windows XP.

En primer lugar nos dirigimos a inicio/todos los programas/comunicaciones/conexiones de red:



En la ventana que nos aparece nos dirigimos a archivo/nueva conexión:



Pulsamos sobre siguiente:

Asistente para conexión n	ueva		
S	Éste es el Asistente para conexión nueva		
	Este asistente le ayuda a:		
	Conectarse a Internet.		
	 Conectarse a una red privada, como la de su lugar de trabajo. 		
	 Configurar una red doméstica o de oficina pequeña. 		
	Haga clic en Siguiente para continuar.		
	< <u>A</u> trás Siguiente > Cancelar		

Seleccionamos la opción configurar una conexión avanzada:

Asistente para conexión nueva
Tipo de conexión de red ¿Qué desea hacer?
 Conectarse a Internet Conectarse a Internet para poder examinar el Web y leer correo electrónico. Conectarse a la red de mi lugar de trabajo Conectarse a una red de negocios (usando acceso telefónico o red privada virtual) para que pueda trabajar desde casa, oficina de campo u otra ubicación. Configurar una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a una red doméstica o de oficina pequeña Conectarse a otro equipo directamente utilizando su puerto serie, paralelo o de infrarrojos, o configurar este equipo para que otros equipos puedan conectarse a él.
< Atrás Siguiente > Cancelar

Seleccionamos la opción aceptar conexiones entrantes:



Seleccionamos el dispositivo de conexiones entrantes:

Asistente para conexión nueva
Dispositivos de conexiones entrantes Puede elegir los dispositivos que su equipo utiliza para aceptar conexiones entrantes.
Active la casilla de verificación situada junto a cada dispositivo que desee utilizar para conexiones entrantes. Dispositivos de conexión: I J Paralelo directo (LPT1)
Propiedades
Atrás Siguiente > Cancelar

También seleccionamos la opción permitir conexiones privadas virtuales:



Ahora seleccionamos los usuarios que pueden acceder:

Asistente para conexión nueva
Permisos de usuarios Puede específicar los usuarios que pueden conectarse a este equipo.
Seleccione la casilla de verificación situada junto a cada uno de los usuarios a los que se les deba permitir la conexión a este equipo. Tenga en cuenta que otros factores, tales como una cuenta de usuario deshabilitada, pueden afectar la capacidad del usuario para conectarse. Usuarios a los que se permite la conexión:
Administrador Asistente de ayuda (Cuenta de asistente de Ayuda de escritorio remoto) Si Invitado Asistente
✓ Tricolas
Agrega <u>r</u> Quitar <u>P</u> ropiedades
< <u>A</u> trás Siguien <u>t</u> e > Cancelar

En la siguiente pantalla en el protocolo indicamos el rango de ips de nuestra vpn:

rod
Asistente para conexión nueva
Software de red El software de red permite que este equipo acepte conexiones de otro tipo de equipos.
Active la casilla de verificación situada junto a cada tipo de software de red que desee habilitar para conexiones entrantes. Software de red:
✓ Y Protocolo Internet (TCP/IP)
🗹 🚚 Compartir impresoras y archivos para redes Microsoft 🛛 👘
Programador de paquetes QoS
Instalar Desinstalar Propiedades
Descripción:
Protocolo TCP/IP. El protocolo de red de área extensa predeterminado que permite la comunicación entre varias redes conectadas entre sí.
< Atrás Siguiente > Cancelar

Aquí indicamos el rango:

Propiedades TCP/IP	de entrada	<u>?</u> ×	
Acceso a la red Permitir a quienes	llaman tener acceso a mi red de área local		
Asignación de direccio	nes TCP/IP		
🔿 Asignar automátic	amente direcciones TCP/IP usando DHCP		
 Especificar direct 	iones TCP/IP		
De:	10 . 33 . 1 . 100		
Para:	10 . 33 . 1 . 110		
Total:	11		
Permitir al equipo que llama especificar su propia dirección IP			
	Aceptar Car	ncelar	

Ahora finalizaremos el proceso:

Asistente para conexión nueva		
Ĩ	Finalización del Asistente para conexión nueva	
	Se han finalizado correctamente los pasos necesarios para crear la siguiente conexión:	
	Conexiones entrantes	
	La conexión se guardará en la carpeta Conexiones de red. Para crear la conexión y cerrar este asistente, haga clic en Finalizar	
	< <u>A</u> trás Finalizar Cancelar	

Ahora en conexiones de red nos habrá aparecido nuestra nueva VPN:



b) Instalación de un servidor VPN en Windows 2003/2008.

EN WS2008

EN primer lugar nos dirigimos a conexiones de red, una vez allí seleccionamos la configurar conexión de red y seleccionamos la opción nueva conexión entrante:



Ahora seleccionamos los usarios autorizados:



En esta pantalla configuramos el protocolo TPC para indicar el rango de ips de servidor VPN:



Rangos de ips

Propiedades IP de entra	ada	x
Acceso a la red	a red de área local a autores de llamada	
Asignación de direccione	es IP	
O Asignar automátic	amente direcciones IP usando DHCP	
Especificar direcció	ones IP	
De:	10 . 33 . 1 . 100	
Para:	10 . 33 . 1 . 110	
Total:	11	
Permitir al equipo o	que llama especificar su propia dirección IP	
	Aceptar Cancelar	

Ahora se configurara nuestra VPN:

🍠 Pe	ermitir conexiones con e	ste equipo		_ 🗆 🗙
\bigcirc	Permitir conexione	s con este equipo		
	Dando acceso a las per	sonas seleccionadas		
			-	
				Cancelar

Ahora finalizaremos el proceso de instalación:

Las personas seleccionadas pueden conectarse ahora a este equipo.				
P	Para conectarse, necesitarán la siguiente información:			
	Nombre de equipo: SRV200801DC01			
[ے Imprimir esta información			
L				

Ahora podemos apreciar que se ha creado la conexión VPN:



c) Instalación de un servidor VPN en GNU/Linux

Primero instalaremos el paquete pptpd:

root@molinux1:/etc/apache2# apt-get install pptpd Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paguetes extras: bcrelav Se instalarán los siguientes paquetes NUEVOS: bcrelay pptpd 0 actualizados, 2 se instalarán, 0 para eliminar y 134 no actualizados. Necesito descargar 116kB de archivos. Se utilizarán 446kB de espacio de disco adicional después de esta operación ¿Desea continuar [S/n]? s 0% [Conectando a repositorios.molinux.info] Una vez instalado accederemos y modificaremos el archivo /etc/ppp/pptpdoptions con los valores remarcados en la imagen: Archivo: /etc/ppp/pptpd-options GNU nano 2.2.4 # Authentication # Name of the local system for authentication purposes # (must match the second field in /etc/ppp/chap-secrets entries) name molinux1 require-mschap-v2 require-mppe-128 ms-dns 10.33.1.1 ms-dns 8.8.8.8 proxyarp nodefaultroute lock # Optional: domain name to use for authentication # domain mydomain.net

Strip the domain prefix from the username before authentication.

Ahora en el archivo /etc/pptpd.conf introducimos las siguientes líneas:



Ahora en /etc/ppp/chap-secrets y agregamos un nombre de usuario que deseamos permitir:

ć	root@n	olinux1: /etc/a	apache2	
<u>A</u> rchivo <u>E</u> ditar	<u>V</u> er <u>B</u> uscar <u>T</u> er	minal Ay <u>u</u> da		
GNU nano 2.2	.4 Archi	vo: /etc/ppp/	chap-secrets	Modificado
# Secrets for a # client niko	authentication server secre molinux1	using CHAP t inves	IP addresses *	

Ahora reiniciamos el servicio:

root@molinux1:/etc/apache2# /etc/init.d/pptpd restart Restarting PPTP: Stopping PPTP: pptpd. Starting PPTP Daemon: pptpd.

COnfiguracion de un cliente Linux:



Ahora introducimos los datos del servidor VPN y el nombre de usuario y contraseña:

8 Editando Conexión VPN 1
Nombre de la conexión: Conexión VPN 1
Conectar automáticamente
VPN Ajustes de IPv4
General
Gateway: 10.33.1.3
Optional
User name: niko
Contraseña: •••••
Show password
NT Domain:
🔀 Advanced
Disponible para todos los usuarios Cancelar Guardar

Ahora habilitaremos la configuración VPN creada:



Configuración de cliente en WINDOWS XP:

d) Conexión desde un cliente Windows y GNU/Linux VPN a un servidor VPN.

EN WINDOWS XP:

En primer lugar nos dirigimos a conexiones de red; una vez allí pulsamos sobre la opción nueva conexión de red:

Pulsamos sobre siguiente:

Asistente para conexión n	ueva
S	Éste es el Asistente para conexión nueva
	Este asistente le ayuda a:
	Conectarse a Internet.
	 Conectarse a una red privada, como la de su lugar de trabajo.
	 Configurar una red doméstica o de oficina pequeña.
	Haga clic en Siguiente para continuar.
	< <u>A</u> trás Siguiente > Cancelar

Ahora pulsamos la opción conectarse a la red de mi lugar de trabajo:



 < Atrás</th>
 Siguiente >
 Cancelar

 Ahora le damos un nombre a la organización:

A	sistente para conexión nueva
	Nombre de conexión Especifique un nombre para esta conexión a su oficina.
	Escriba un nombre para esta conexión en el cuadro siguiente.
	Nombre de la orga <u>n</u> ización
	Puede escribir, por ejemplo, el nombre de su oficina o el del servidor al que se conectará.
	< <u>A</u> trás Siguiente > Cancelar

Ahora pondremos la ip del equipo al que queremos conectarnos:



Ahora seleccionaremos la opción crear esta conexión solo para este usuario:



Ahora finalizaremos el proceso:

1	Asistente para conexión nueva			
		Finalización del Asistente para conexión nueva Se han finalizado correctamente los pasos necesarios para crear la siguiente conexión: asir		
		La conexión se guardará en la carpeta Conexiones de red. Agregar en mi escritorio un acceso directo a esta conexión Para crear la conexión y cerrar este asistente, haga clic en Finalizar.		
		< Atrás Finalizar Cancelar		

Ahora pondremos el nombre de usuario y contraseña:



Ahora deberemos de volver a poner la contraseña:

Conectarse a asir		? 🔀	
Windows no se pudo conectar a la red utilizando el nombre de usuario y la contraseña que proporcionó. Vuelva a escribirlos.			
Puede escribir un nombre en el campo de dominio o dejarlo en blanco. (Las conexiones a Internet no requieren nombre de dominio)			
Nombre de usuario:	administrador		
Contraseña:	•••••		
Dominio:			
	🔲 Guardar nombre de usuario y con	traseña	
	Accestor Concertor		
L	Aceptar Lancelar		

Como se ve en la imagen ya se ha establecido la conexión:



Cliente en Ubuntu:

EN primer lugar nos dirigimos a	conexiones	VPN/configurar	VPN:
---------------------------------	------------	----------------	------

	14	((ا≱	\sim	16:14	🔉 niko	Ċ
	Re		cable	adas		
	Conexión cableada 1					
	Desconectar					
	Auto eth0					
Configurar VPN Desconectar VPN	Conexiones VPN					
	✓ A	ctivar	red			
0:da:a7 Másc:255.255.255.0	In Ec	form litar l	ación las co	de la c nexion	onexión es	
4 Alcance:Enlace 1500 Métrica:1						

Ahora pulsamos sobre añadir:

Nombre	Usada por última vez Añadi
	Edita
	Elimina
	Import
	Export

Ahora pulsamos sobre crear:

8	
	Elegir un tipo de conexión VPN
	Seleccione el tipo de VPN que quiere usar para la nueva conexión. Si el tipo de conexión VPN que quiere crear no aparece en la lista, puede que no tenga instalado el complemento de VPN correcto.
	Point-to-Point Tunneling Protocol (PPTP)
	Compatible with Microsoft and other PPTP VPN servers.
	Cancelar Crear

Ahora rellenamos los siguientes campos con la dirección del servidor VPN y el nombre y contraseña del usuario y pulsamos sobre guardar:

🥹 Edicando asir				
Nombre de la conexión: asir				
Conectar automáticamente				
VPN Ajustes de IPv4				
General				
Gateway: 10.33.1.20				
Optional				
User name: administrador				
Contraseña:				
Show password				
NT Domain:				
🔀 Advanced				
Disponible para todos los usuarios Cancelar Guardar				

Ahora en advance configuramos lo que aparece en pantalla:

PPTP Advanced Options				
Authentication				
Allow the following authentic	cation methods:			
Machar				
MSCHAPv2				
EAP				
Security and Compression				
☑ Use <u>P</u> oint-to-Point encryption (MPPE)				
Seguridad: All Available (Default) ‡				
Allow stateful encryption				
Permitir compresión de datos <u>B</u> SD				
Permitir compresión de datos <u>d</u> eflate				
Usar compresión de ca <u>b</u> eceras TCP				
Echo				
<u>C</u> ancelar	<u>A</u> ceptar			

Ahora podemos ver que la conexión ha sido creada:



Ahora la activaremos, para ello nos dirigimos a conexiones VPN y seleccionamos asir:



5. VPN de acceso remoto

b) Configurar el router Linksys RV200 como un servidor VPN de acceso remoto.

Utiliza el simulador

http://ui.linksys.com/files/WRV200/1.0.29/SetupDHCP.htm

En primer lugar crearemos el usuario niko con la contraseña inves:

A Division of Cisco Systems, Inc.	9					http://o	de inforaction cursos.infora	/a: Entrar ar situ ictiva.es/login/
						Wirele	ess-G VPN Rou	uter with RangeBo
VPN	Setup		Wireless	Firewall	v	PN	QoS	Administra
	VPN Client	Access	VPN Passth	rough IPSe	e VPN	VPN Sumn	nary	
VPN Client Access								
	Username:			niko				
	P	assword:		••••				
	R	e-enter to	confirm:			Ad	d/Save	
	Allow user to change password? O Yes O No							
VPN Client List Table								
	No.	Active	Username	Password	Edit	t/Remove		
	1				Edit	Remove		
	2				Edit	Remove		
	3				Edit	Remove		
	4				Edit	Remove]	
	5				Edit	Remove		
	6				Edit	Remove		
	7				Edit	Remove		
	8				Edit	Remove		
	9				Edit	Remove		
	10				Edit	Remove		

Ahora configuramos la dirección IP del cliente y pulsamos sobre settings:

LINKSYS [®] A Division of Cisco Systems, Inc.				
VPN Client	WARNING: In order to ensure proper functionality, the router will need to change its Local IP address differs from 192.168.1.x to avoid conflicts with the remote network. You will need to reboot all PCs and network devices connected to the router. If you have set static IP addresses on any device or if you are using port forwarding, you will need to update its IP address to the new IP range to proper operation. Please input new Local IP Address below and press Save Settings to store your configuration.			
	Local IP Address: Subnet Mask:	192 . 168 . 2 . 1 255 . 255 . 255 . 0		
	Save Sattir	nos Close		

c) Configura tu cliente VPN en Windows.

EN WINDOWS XP:

En primer lugar nos dirigimos a conexiones de red; una vez allí pulsamos sobre la opción nueva conexión de red:

Pulsamos sobre siguiente:

Asistente para conexión ni	ueva		
S.	Éste es el Asistente para conexión nueva		
	Este asistente le ayuda a:		
	Conectarse a Internet.		
	 Conectarse a una red privada, como la de su lugar de trabajo. 		
K	 Configurar una red doméstica o de oficina pequeña. 		
	Haga clic en Siguiente para continuar.		
	< <u>A</u> trás Siguiențe > Cancelar		
Ahora pulsamos la opción conectarse a la red de mi lugar de trabajo:



Ahora le damos un nombre a la organización:

< <u>A</u>trás Siguien<u>t</u>e >

Cancelar

Asistente para conexión nueva
Nombre de conexión Especifique un nombre para esta conexión a su oficina.
Escriba un nombre para esta conexión en el cuadro siguiente.
Nombre de la orga <u>n</u> ización
Puede escribir, por ejemplo, el nombre de su oficina o el del servidor al que se conectará.
< <u>A</u> trás Siguien <u>t</u> e > Cancelar

Ahora pondremos la ip del equipoal que queremos conectarnos:



Ahora seleccionaremos la opción crear esta conexión solo para este usuario:





Ahora pondremos el nombre de usuario y contraseña:

Conectarse a a	asir	? 🔀
C		
Nombre de usuario: Contraseña:	administrador	
Guardar este siguientes us Sólo yo Cualquie	e nombre de usuario y contraseña para suarios: ra que use este equipo	los
Conectar	Cancelar Propiedades	Ayuda

Ahora deberemos de volver a poner la contraseña:

Conectarse a asir 🛛 🔹 🔀							
Windows no se pudo conectar a la red utilizando el nombre de usuario y la contraseña que proporcionó. Vuelva a escribirlos.							
Puede escribir un nombre en el campo de dominio o dejarlo en blanco. (Las conexiones a Internet no requieren nombre de dominio)							
Nombre de usuario:	administrador						
Contraseña:	•••••						
Dominio:							
🔄 Guardar nombre de usuario y contraseña							
Aceptar Cancelar							

Como se ve en la imagen ya se ha establecido la conexión:

🛸 Conexiones	de red						_ 2	×
Archivo Edició	n Ver Favorito:	s Herramientas Opciones	avanzadas Ay	ıda				1
G Atrás 🔹	🕤 - 🎓 🍃	🔎 Búsqueda 🛛 🍋 Carpeta	s 🕼 🎯	× 9	•			
Dirección 🔇 Co	nexiones de red						💌 🄁 I	ir
Asistente								
Asis	tente para conexiór	n nueva						
LAN o Intern	t de alta velocid:	ad						
Cor Cor VMV	exión de área local ectado, Con servido vare Accelerated A№	or de s 10 PCN						
Red privada	/irtual							
sir Con Min	ectado, Con servido puerto WAN (PPTP)	or de s						
					i asir estă Haga clic aquí j	á ahora conectado para obtener más inf	ormación	
🦺 Inicio	N 10 C	Símbolo del sistema	S Conexio	nes de red			 16: 	38

REDES PRIVADAS VIRTUALES

6. VPN sitio a sitio

b) En cada sitio existe un router Linksys RV042.
 Configurar cada sitio - router Linksys RV042 utilizando el simulador

http://ui.linksys.com/files/RV042/1.2.3/home.htm

CONFIGURACIÓN ROUTER Central:

	Tunnel No. 1	By setting this page, users one add the new tunnel
	Tunnel Name sitio a sito	between two VPN devices.
	Interface WAN1	Tunnel No.: The tunnel
	Enable 🗸	automatically from 1~30.
		Tunnel Name: Enter the
		Office, Branch Site,
Local Group Setup	Local Security Gateway Type IP Only	Corporate Site, etc.
	IP address 0 . 0 . 0	More
	Local Security Group Type Subnet	
	IP address 192 . 168 . 1 . 0	
	Subnet Mask 255 . 255 . 255 . 0	
Remote Group setup	Remote Security Gateway Type IP Only	.
	IP address 209 . 165 . 202 . 129	
	Remote Security Group Type Subnet	
	IP address 192 . 168 . 101 . 0	
	Subnet Mask 255 . 255 . 255 . 0	
ID Page Patron		
in sec serub	Keying Mode IKE with Preshared key	
	Phase1 DH Group Group1	
	Phase1 Encryption DES	
	Phase1 Authentication MDS	
	Phase1 SA Life Time 28800 seconds	
	Perfect Forward Secrecy	
	Phase2 DH Group Group1	
	Phase2 Encryption DES	
	Phase2 Authentication MD5	
	Phase2 SA Life Time 3600 Seconds	
	Preshared Key cisco123	
	Advanced +	
		Cisco Systems
	Save Settings	Cancel Changes

CONFIGURACIÓN ROUTER SUCURSAL

Add a new Tunnel		SITEMAP
	Tunnel No. 1	By setting this page, users
	Tunnel Name sitio a sito	can add the new tunnel between two VPN devices.
	Interface WAN1 _	Tunnel No.: The tunnel
	Enable	number will be generated automatically from 1~30.
		Tunnel Name: Enter the
		Office, Branch Site,
Local Group Setup	Local Security Gateway Type IP Only	Corporate Site, etc.
	IP address 0 . 0 . 0	wore
	Local Security Group Type Subnet	
	IP address 192 . 168 . 1 . 0	
	Subnet Mask 255 . 255 . 255 . 0	
Remate Group Astron		
Remote Group Setup	Remote Security Gateway Type	
	IP address 209 . 165 . 202 . 129	
	Remote Security Group Type Subnet	
	IP address 192 . 168 . 101 . 0	
	Subnet Mask 255 . 255 . 255 . 0	
IP Sec Setup	Varian Mate IVE with Drawbard Var	
	Phase1 DH Gmun Grown1	
	Phase1 Encryotion DES	
	Phase1 Authentication MD5	
	Phase1 SA Life Time 28800 seconds	
	Perfect Forward Secrecy	
	Phase2 DH Group Group1	
	Phase2 Encryption DES	
	Phase2 Authentication MD5	
	Phase2 SA Life Time 3800 seconds	
	Preshared Key cisco123	
	Advanced +	
		Passa Passasa

TECNICAS DE CIFRADO: COMUNICACIONES SEGURAS

7. SSH

a) Instalación del servidor SSH en GNU/Linux

En primer lugar deberemos de introducir el comando apt-get install opensshserver:

niko@ubuntu1:~\$ sudo apt-get install openssh-server
sudo: unable to resolve host ubuntu1
Leyendo lista de paquetes Hecho
Creando árbol de dependencias
Leyendo la información de estado Hecho

Una vez instalado el openssh-server los clientes ssh podrán acceder a nuestro equipo con cualquier usuario dado de alta en el equipo que actua como servidor ssh.

b) Conexión al servidor SSH mediante cliente GNU/Linux y cliente

Windows.

EN LINUX

Para realizar una conexión deberemos de introducir en el terminal ssh niko@10.33.1.5 y posteriormente introducir la contraseña del usuario niko como aparece en la imagen:

root@molinux1:/home/niko# ssh niko@10.33.1.5 niko@10.33.1.5's password: Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686) * Documentation: https://help.ubuntu.com/

New release 'oneiric' available. Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Jan 11 19:10:44 2012 from ubuntu1-20.local niko@ubuntu1:~\$ ■

Ahora podemos hacer labores administrativas de forma remota:

niko@ubuntu1:~\$ ls
Descargas Escritorio Imágenes Plantillas Vídeos
Documentos examples.desktop Música Público
niko@ubuntu1:~\$

EN WINDOWS

Para poder realizar	una conexión	en Windows	deberemos	de instalar l	а
herramienta putty:					



Ahora nos aparecerá una ventana en la que deberemos de proceder a poner el nombre de usuario y la contraseña para establecer la conexión ssh:



Ahora podemos realizar tareas administrativas en nuestros equipos.

c) Escenario CISCO: Conexión segura a la administración de un router.

En primer lugar configuraremos la interfaz f0/0 del router:

Port Status	asternemeto/0	
Port Status		
		🔽 On
Bandwidth		🔽 Auto
10 Mbps	100 Mbps	
Duplex		🛛 Auto
Full Duplex	Half Duplex	
MAC Address	0060.3E2	2C.7901
IP Address	10.33.1.	1
Subnet Mask	255.255.	.255.0
Tx Ring Limit	10	
mmands		
Shucuown		
	10 Mbps Duplex Full Duplex MAC Address IP Address Subnet Mask Tx Ring Limit mmands snacuom	10 Mbps 10 Mbps 100 Mbps Duplex Full Duplex MAC Address 10.33.1. Subnet Mask 255.255. Tx Ring Limit 10 mmands sauceen

Ahora deberemos de configurar un nombre en el router:

Router(config) #hostname niko

Ahora deberemos de **Configurar dominio y generar llaves rsa mediante los** siguientes comandos:

Ahora deberemos de Especificar que protocolos se dejan pasar por la línea VTY:

```
niko(config)#line vty 0 4
*mar 1 0:5:53.937: %SSH-5-ENABLED: SSH 1.99 has been enabled
niko(config-line)#transport input ssh
```

Ahora deberemos de dar de dar de alta a un usuario con su contraseña:

```
niko(config-line)#login local
niko(config-line)#username niko privilege 15 password inves
niko(config)#
```

Configuración del equipo cliente:

En primer lugar configuraremos la tarjeta de red del equipo:

RC0	
Physical Config	Desktop
IP Configurati	on X
O DHCP	
Static	
0	
IP Address	10.33.1.5
Subnet Mask	255.255.255.0
Default Gateway	10.33.1.1
DNS Server	

Ahora nos dirigimos a la consola de comandos y ejecutamos el comando SSH –l niko 10.33.1.1. Posteriormente introducimos la contraseña y ya habremos accedido de forma remota al router de forma segura:



SERVIDORES DE ACCESO REMOTO

8. Protocolos de autenticación:

a) Escenarios CISCO: Interconexión de redes mediante protocolos PPP,PAP,CHAP.

Configuración de PPP:



En primer lugar configuraremos las direcciones de red de los enlaces seriales:

```
Ahora estableceremos la encapsulación ppp:
```

```
Router(config-if) #interface Serial0/0/0
Router(config-if) #ip address 10.33.2.1 255.0.0.0
Router(config-if) #encapsulation ppp
```

Ahora estableceremos la encapsulación ppp en el router inverso:

```
Router(config) #interface Serial0/1/0
Router(config-if) #ip address 10.33.1.1 255.0.0.0
Router(config-if) #encapsulation ppp
Router(config-if) #
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
```

Ahora comprobaremos su funcionamiento con un ping: Router#ping 10.33.2.1

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.33.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/38/40 ms
```

Autenticación con PAP



Como utilizaremos el escenario base anterior no realizare configuración de ips. Ahora realizaremos la configuración de la autenticación PAP:

```
Router(config) #username niko password inves
Router(config) #interface Serial0/1/0
Router(config-if) #encapsulation ppp
Router(config-if) #ppp authentication pap
Router(config-if) #ppp pap sent-username nikol password inves
Router(config-if) #
```

Ahora realizamos lo mismo en el router contrario:

```
Router(config)#username nikol password inves
Router(config)#interface Serial0/0/0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp pap sent-username niko password inves
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

Ahora probaremos el funcionamiento de la autenticación con un ping:

```
Router#ping 10.33.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.33.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
```

PPP con autenticación CHAP



Como utilizaremos el escenario base anterior no realizare configuración de ips. Ahora realizaremos la configuración de la autenticación chap:

```
R1(config)#username R2 password inves
R1(config)#int s0/1/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication CHAP
```

Ahora realizamos lo mismo en el router contrario:

```
Router(config) #hostname R2
R2(config) #username R1 password inves
R2(config) #int s0/1/0
R2(config-if) #encapsulation ppp
R2(config-if) #
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
R2(config-if) #ppp authentication CHAP
```

49

SERVIDORES DE ACCESO REMOTO

9. Servidores de autenticación

a) REDES INALÁMBRICAS: WPA Personal

Configurar router inalámbrico Linksys WRT54GL en modo seguro: (Cambia el SSID por defecto y desactivar el broadcasting SSID, deshabilitar DHCP, cambiar nombre de usuario y contraseña, activar el filtrado de MAC, WPA2, cifrado TKIP+AES).
Configurar la tarjeta de red de un cliente inalámbrico con dichas medidas de seguridad y comprobar la autenticación a dicho router inalámbrico.

Una vez accedido al menú de administración de nuestro router inalámbrico procede a deshabilitar el dhcp, para ello en la pestaña setup/basic setup seleccionamos el botón radio disable en la sección dhcp server:

					Wireless-G Broad	band Router	WRT54GL
Setup	Setup Wir	eless	Security	Access Restrictions	Applications & Gaming	Administration	Status
	Basic Setup	I.	DDNS	1	MAC Address Clone	Advanc	ed Routing
Internet Setup							
Internet Connection Type	Automatic	Configurati	ion - DHCP	•		Automatic C	onfiguration -
Optional Settings (required by some ISPs)	Router Name:	WRT	54GL			commonly use operators.	d by Cable
	Host Name:					Host Name :	Enter the host
	Domain Name:					name provided	i by your ise.
	MTU:	Auto	•			Domain Nam domain name r	e : Enter the provided by your
	Size:	1500)			ISP. More	
						morem	
Network Setup							
Router IP	Local IP Addre	ss: 192	. 168 . 3	. 142		Local IP Add address of the	ress: This is the router.
	Subnet Mask:	255	. 255 . 255 . 0	•		Cubrat Mari	. This is the
Network Address Server Settings (DHCP)	DHCP Server:	© En	able 🖲 Disab	le		subnet mask o	f the router.
	Starting IP Address:	192.10	58.3. 100				
	Maximum Num DHCP Users:	per of 50]			DHCP Server router to mana	: Allows the ge your IP
	Client Lease Ti	me: 0	minutes (0 me	eans one day)		addresses.	
	Static DNS 1:	0	. 0 . 0	. 0		Starting IP A address you y	ddress:The vould like to start
	Static DNS 2:	0	. 0 . 0	. 0		with.	
	Static DNS 3:	0	.0.0	. 0		Maximum nu	mber of DHCP
	WINS:	0	. 0 . 0	. 0		Users : You n number of add	ay limit the resses your

Ahora nos dirigiremos a la pestaña wireless /basic wireless Settings y allí elegimos el nombre deseado de SSID, asu vez desactivamos la difusión del SSID:

LINKSYS [®] A Division of Cisco Systems, Inc.					ware Version: v4.30.7
			Wireless-G Broadb	and Router	WRT54GL
Wireless	Setup Wireless	Security Access Restriction	Applications s & Gaming	Administration	Status
	Basic Wireless Settings	Wireless Security	Wireless MAC Filter	Advanced Wireles	ss Settings
Wireless Network	Wireless Network Mode: Wireless Network Name (SSD): Wireless Channel: Wireless SSID Broadcast:	Mixed asir01 11-2.462GHZ Fnable Disable Status: SES hactive Reset Security]	Wireless He you wish to e clents, choos you would like wireless acct Disable. More	twork Mode : If xclude Wreless-G e B-Onty Mode. If to disable sss, choose Sss, choose
		Save Settings	Cancel Changes		aulluanullua

Ahora en la pestaña wirelss security el modo de seguridad y la contraseña de acceso:

LINKSYS [®] A Division of Cisco Systems, Inc.						Firmw	are Version: v4.30.7	
					Wireless-G Broad	band Router	WRT54GL	
Wireless	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status	
	Basic Wirele	ess Settings	Wireless Se	ecurity V	Vireless MAC Filter	Advanced Wireles	s Settings	
Wireless Security						Security Mod	e:You may	
	Security Mod	e:	WPA2 Personal TKIP+AES			choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your		
	WPA Algorith	ms:						
	WPA Shared	Key:	1234567890			security mode	ise the same in order to	
	Group Key R	Renewal:	3600	seconds		communicate. More		
							CISCO SYSTEMS	
			Sav	ve Settings	Cancel Changes		a.ullu	

Ahora activamos el filtrado de mac:

LINKSYS [®] A Division of Cisco Systems, Inc.						Firm	ware Version: v4.30.7
					Wireless-G Broa	dband Router	WRT54GL
Wireless	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration	Status
	Basic Wirel	ess Settings	Wireless Sec	urity Wi	reless MAC Filter	Advanced Wireles	ss Settings
Wireless MAC Filter						More	
	Wireless MA	AC Filter: 🔘 [Enable 🍥 Disal	ble			Cisco Systems
			Save	Settings	Cancel Changes		ավիստուլիստ

Acceso con un cliente w7:

En primer lugar elegimos la red a la que nos queremos conectar:

Conectado actualmente a Identificando (a : Sin acceso a Intern	: *** sir01) et	•
Conexión de red inalámbri	ica 🔺	
asir01	Conectado 🔐	
ALTHIA	.atl	E
DPTOINFORMATICA	all.	
jeruraes	all.	
VACACIONES	.all	
STI	.all	-
Telefonia	att	
WLAN_29	all	Ŧ
Abrir Centro de redes y r	ecursos compartidos	

Ahora introducimos la contraseña :

😰 Conectarse a una re	d	
Escribir la clave d	le seguridad de red	
Clave de seguridad:	1234567890	
	Ocultar caracteres	
	Aceptar	Cancelar

b) SERVIDOR RADIUS:

1.- Simulación de un entorno de red con servidor RADIUS CISCO en el Packet Tracert Router.

En primer lugar presentaremos el escenario:



Ahora realizaremos la configuración del servidor DNS y http: En primer lugar añadiremos los registros al servidor dns y lo activamos:

R www_DNS						
Physical Config	Desktop	Software/S	ervices			
GLOBAL				DNS		
Algorithm Settings SERVICES	DNS S	DNS Service On Off				
НТТР	Resou	Irce Records				
DHCP	Name			Туре	A Rec	cord 👻
DNS	Addre	ISS				
AAA		Add		Save	Remov	/e
NTP	No.	Name	Тур	e	Details	
EMAIL	= 1	dns.asir.es	A Re	cord	30.30.30.1	
INTERFACE	= 2	radius.asir.es	A Re	cord	30.30.30.2	
FastEthernet	3	www.asir.es	A Re	cord	30.30.30.1	
	, DNS	Cache				

Ahora configuramos el servidor web:

R www_DNS					×	
Physical Config	Desktop	Software/Services				
GLOBAL Settings	*		нттр			
SERVICES	HTTP-		HTTPS		n	
HTTP	On	Off	On	Off		
DHCP	File Nam	e: index html				
TFTP	ab trails	e. mucx.num				
DNS		<pre>color</pre>	='blue'>Cisco Pa	icket		
SYSLOG	Tracer			icket		
AAA	<hr/> We	come to Cisco Packe	t Tracer. Openin	g doors to new		
NTP	opport	unities. Mind Wide Op	en.			
EMAIL	Qui	ck Links:				
FTP		href='helloworld.html'	>A small page <td>3></td> <td></td>	3>		
FastEthernet	RFACE 					
Page: 1/3 < > + X						

Por último configuramos la ip:

Physical Config Desktop Software/Services	
IP Configuration X	
http:	
© DHCP	
Static	
Web Brow	wser
IP Address 30.30.30.1	
Subnet Mask 255.0.0.0	
Default Gateway 30.30.30.5	
DNS Server	

Ahora configuramos el servidor radius: En primer lugar definiremos la ip:

RADIUS					
Physical	Config	Desktop	Software/Services		
IP Co	nfigurati	ion		X	
					http:
© D	HCP				
© S	tatic				
-					Web Browser
IP Add	lress	30.30	0.30.2		
Subne	t Mask	255.0	0.0.0		
Defaul	t Gateway				
DNS S	erver				

Ahora configuramos la autenticación radius añadiendo los usuarios autorizados y los clientes disponibles:

RADIUS				400				
Physical	Config	Desktop	Softwa	re/Services				
GLO	BAL	h.	AAA					
Sett	ings							
Algorithm	Settings	Service	۲	On 🔘 Off	Rad	ius Port	1645	
SERV	ICES	Network	Configure	ation				
	1P	INCLWON	Conngun	ation				
		Client Na	me		Clie	ent IP		
		Secret			Se	erverType	Radius	•
SYS			ClientName ClientID ServerTune Kay					
	A		•	20.20.20.5				+
NT	ΓP	1 WSR	1	30.30.30.5	Kadii	us	inves	
EM	AIL							
FT	P	-User Se	tun					
INTER	FACE	0000100						
FastEt	hernet	UserNam	e		Pa	assword		
	UserName Password				+			
		1 usuario1		inves				
		2 usuario2			inves			-
	-	· · · · · ·						
					-		and the second second	

Una vez realizados los pasos anteriores configuramos el router: En primer lugar configuramos la ip estatica, en las que a su vez indicaremos la dirección del servidor DNS:

💐 WSR1	and the second s	and the second se
Physical Config	GUI	
Setup	Setup Wireless Security Access Applications Adminis Basic Setup DDNS MAC Address Clone Ad	tration Status
Internet Setup Internet Connection type	Static IP Internet IP Address: 30 30 5 Subnet Mask: 255 0 0 0 Default Gateway: 30 30 30 5 DNS 1: 30 30 30 1 DNS 2 (Optional): 0 0 0 0 DNS 3 (Optional): 0 0 0 0	Help
Optional Settings (required by some internet service providers)	Host Name: Domain Name: MTU: Size: 1500	
Network Setup Router IP	IP Address: 192 . 168 . 0 . 1 Subnet Mask: 255.255.255.0 -	
DHCP Server Settings	DHCP Server: Enabled Disabled DHCP Reservation Start IP Address: 192.168.0. 100	

En la configuración del dhcp configuramos los rangos de ips y la dirección del dns:

DHCP Server Settings	DHCP Server:	
	Start IP Address: 192.168.0. 100 Maximum number 50 of Users: 50 IP Address Range: 192.168.0. 100 - 149 Client Lease Time: 0 minutes (0 means one day) Static DNS 1: 30 30 1 Static DNS 2: 0 0 0 Static DNS 3: 0 0 0 WINS: 0 0 0	
	Save Settings Cancel Changes	ath, ath

.INKSYS° Firmware Version: v0.93 Wireless-N Broadband Router Applications Acce Wireless Setup Wireless Security Administration S Restrictions & Gaming Wireless Security Security Mode: WPA2 Enterprise 👻 Help... AES Encryption: Ŧ RADIUS Server: 30 . 30 . 30 . 2 RADIUS Port: 1645 Shared Secret: inves 3600 seconds Key Renewal:

Ahora configuraremos el router como cliente radius:

Ahora configuraremos los clientes:

En primer lugar nos dirigimos a los perfiles de la tarjeta wifi, una vez allí pulsamos sobre default y seleccionamos la opción edit:

A Division of C	KSYS [®] Xisco Systems, Inc.				0	
Link Inform	ation Connect		Profiles			
To connect to or edit a profi	a network, select the profile na le, use the menu bar at the botto	me ther om of th	n click the Connect but ne screen.	tton. To create	2.4 ^{GHz}	
Profile	Wireless Network Nam	e	Site Informa	ation	· · · · · · · · · · · · · · · · · · ·	
Default WSR1	Default WSR1	•	Wireless Mode Ir Wide Channel Ar Standard Channel Security Di Authentication Ar	nfrastructure uuto uuto iisable uuto		
Wireles	New Edit Import Export Delete Adapter is Active Wireless Network Monitor v1.0 Model Me. WPC300N					

Ahora pulsamos sobre advance setup:

Available Wireles	oo Notworko			
	ss welworks	1		
Please select the wireless continue. If you are not sur	network that you w e which network to	ant to connect to, choose, first try ti	then click the Conn te one with the stro	ect button to ngest signal.
Wireless Network Name	e CH Signal	Security		
WSR1	1 100%		Re	fresh
			Co	nnect
			Exit	Advanced Set
rologo N. Natabad	k Adortor	Mirelana Matura	Exit	Advanced Set
reless-N Noteboo	k Adapter	Wireless Netwo	Exit	Advanced Set
r eless-N Notebool pantalla que no	k Adapter N s aparece s	Wireless Netwo	Exit *k Monitor v1.0 mos la prin	Advanced Set Model No. WPC mera opción
pantalla que no	k Adapter N s aparece s	Wireless Netwo selecciona	Exit K Monitor v1.0 mos la prir	Advanced Set Madel No. WPC Mera opción
Cless-N Notebool pantalla que no INKEYS [®] sion of Cisco Systems, Inc.	k Adapter N s aparece s	Wireless Netwo selecciona	Exit *k Monitor v1.0 mos la prin	Advanced Set Model No. WPC nera opción
CORSS-N Notebool pantalla que no INKEYS® sion of Cisco Systems, linc.	k Adapter N s aparece s	Wireless Netwo selecciona	Exit % Monitor v1.0 mos la prir	Advanced Set
reless-N Notebool pantalla que no INKEYS [®] sion of Cisco Systems, Inc. Creating a Profile	k Adapter N s aparece s	Wireless Netwo	Exit k Monitor v1.0 mos la prir	Advanced Set
Creating a Profile	k Adapter N s aparece s	Wireless Netwo	Exit K Monitor v1.0 mos la prir	Advanced Set
reless-N Notebool pantalla que no INKEYS sion of Cisco Systems, Inc. Creating a Profile Wireless Mode	k Adapter N s aparece s	Wireless Netwo	Exit k Monitor v1.0 mos la prir	Advanced Set
Creating a Profile	k Adapter N s aparece s Adde that best suits Select Infrastructu	Wireless Netwo selecciona your needs, re Mode if you want t	Exit K Monitor v1.0 mos la prir	Advanced Set
Creating a Profile Wireless Mode Please choose the Wireless A	k Adapter S S aparece s Adde that best suits Select Infrastructu router or access p	Wireless Netwo Selecciona Selecciona your needs. re Mode if you want t oint.	Exit *k Monitor v1.0 mos la prin	Advanced Set
Creating a Profile Wireless Mode Please choose the Wireless Mode On Infrastructure Mode On Ad-Hoc Mode	k Adapter N S aparece s Adde that best suits Select Infrastructur router or access p Select Ad-Hoc Mor device directly wit	Wireless Netwo Selecciona your needs. re Mode if you want to oint. de if you want to conn hout using a wireless	Exit K Monitor v1.0 mos la prir o connect to a wireless router or access point.	Advanced Set
Image: Constraint of the second se	k Adapter S aparece s Adde that best suits Select Infrastructu router or access p Select Ad-Hoc Mor device directly wit twork name (SSID) fr	Wireless Networ Selecciona your needs. re Mode if you want to oint. de if you want to conn hout using a wireless or your wireless net	Exit k Monitor v1.0 mos la prin o connect to a wireless router or access point. work.	Advanced Set

Le indicamos que obtenga las configuración por DHCP:

	LINKSYS [®] A Division of Cisco Systems, Inc.	
	Creating a Profile	
	Network Settings Obtain network settings automatic Select this option to have your netwo Specify network settings Select this option to specify the netw IP Address Subnet Mask Default Gateway 	cally (DHCP) rk settings assigned automatically. ork settings for the adapter. DNS 1 DNS 2
onfiqu	Wireless-N Notebook Adapter ramos la seguridad WPA2 E	Back Next Wireless Network Monitor v1.0 Model No. WPC300N Enterprise:
	LINKSYS A Division of Cisco Systems, Inc.	
	Creating a Profile	
	Wireless Security Security WPA2-Enterprise -	Please select the wireless security method used by your existing wireless network. WEP stands for Wired Equivalent Privacy. WPA-Personal, also known as Pre-shared Key, is a security standard stronger than WEP encryption. WPA2-Personal is the newer version with stronger encryption than WPA-Personal. WPA-Enterprise, WPA2-Enterprise and RADIUS use Remote Authentication Dial-In User Service (RADIUS).
		Back Next

Ahora introducimos la cuenta de usuario que esta dada de alta en el sevidor radius:

Creating a Profile	
Wireless Security - WPA	2 Enterprise
Authentication PEAP	Please select the authentication method that you use to acces
Login Name usuario1	Enter the Login Name used for authentication.
Password •••••	Enter the Password used for authentication.
Server Name	Enter the Server Name used for authentication. (Optional)
Certificate Trust Any	Please select the certificate used for authentication.
Inner Authen. TOKEN CARD	Please select the inner authentication method used inside the PEAP tunnel.

Una vez realizado estos pasos la configuración del radius abra finalizado.



2.- Instalación de un servidor Radius bajo GNU/LINUX (freeradius), para autenticar conexiones que provienen de un router de acceso Linksys WRT54GL: WPA Empresarial. *Comprobación en un escenario real.*

En primer lugar instalaremos el freeradius:

```
root@ubuntu1:/home/niko# apt-get install freeradius
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Levendo la información de estado... Hecho
```

Aquí vemos como se crea los parámetro DH durante el proceso de instalación:

Nee	.000	ubuni	cu1: /non	пе/піко	
<u>A</u> rchivo	<u>E</u> ditar	<u>V</u> er	<u>B</u> uscar	<u>T</u> erminal	Ay <u>u</u> da
Procesan Configur Añadiend Configur dpkg-sta adius Updating Añadiend Generati This is	do disp ando li ando fr o al us ando fr toverri defaul o al us ng DH p going t	arado bfree eerad uario eerad de: a t SSL uario arame o tak	res par radius2 lius-com freera lius (2. viso: s certif freera ters, 1 e a lon	a ureadah (2.1.10+ mon (2.1. d al grup 1.10+dfsg e ha util icate set d al grup 024 bit l o time	ead dfsg-2ubuntu2) 10+dfsg-2ubuntu2) o shadow -2ubuntu2) izadoupdate pero no existe /var/run/freer tings, if any o ssl-cert ong safe prime, generator 2
			· .+		·····+·····+·····+·····
+		+.			······+·····+····
			· · · · · · · · · · · · · · · · · · ·	+	
· · · · · · · · · · · · · · · · · · ·					······+·····
••••				······ ······	
		+			

Ahora nos dirogimos al archivo /etc/freeradius/users y añadimos el nombre del usuario que podrá acceder al freeradius:



Ahora nos dirigiremos al archivo /etc/freeradius/clients.conf y una vez allí introducimos la dirección del cliente radius y la palabra secreta:



Configuramos la red inalámbrica del Router:

A Division of Cisco Systems, Inc.							Firmv	vare Version: v4.30.7
					v	Vireless-G Broa	dband Router	WRT54GL
Wireless	Setup	Wireless	Security	Acc Restri	ess ctions	Applications & Gaming	Administration	Status
	Basic Wirele	ess Settings	Wireles	s Security	Wire	less MAC Filter	Advanced Wireles	s Settings
Wireless Network	Wireless Ne Wireless Ne (SSID): Wireless Ch Wireless SS	twork Mode: twork Name annel: ID Broadcast:	Mixed asir01 11 - 2.4 © Enat Status: Rese	↓ H62GHZ ↓ Disab	e		Wireless Net you wish to ex clients, choos you would like wireless acce Disable. More	Cisco Systems
				Save Setting	s Ca	ancel Changes		ավիստուլիրութ

Modo WPA2 Enterprise, indicamos la IP del servidor RADIUS, y la contraseña:

A Division of Cisco Systems, Inc.								Firmw	are Version: v4.30.7
						Wireless-G Bro	adban	d Router	WRT54GL
Wireless	Setup	Wireless	Secur	ity	Access Restriction	Applications as & Gaming	Ad	ministration	Status
	Basic Wirele	ess Settings	Wirel	ess Secu	irity	Wireless MAC Filter	Adv	vanced Wireless	s Settings
Wireless Security	Security Mod WPA Algorith RADIUS Serv RADIUS Port: Shared Key: Key Renewa	e: ms: rer Address: I Timeout:	WPA2 E TKIP+A 192.1 1812 inves 3600	Enterpri ES V 168.2	se ▼ . 150 seconds			Security Mod choose from D Pre-Shared Ke or RADIUS. All network must u security mode communicate. More	e : You may sable, WEP, WPA y, WPA RADIUS, devices on your use the same in order to <u>Clisco Systems</u>
				Save	Settings	Cancel Changes	6		ավիտավիտ

Configuración manual de un cliente w7, para una autenticación RADIUS:

			X				
Conectarse manualment	e a una red inalámbrica						
Escriba la información de la red inalámbrica que desea agregar.							
Nombre de la red:	asir01						
Tipo de seguridad:	WPA2-Enterprise						
Tipo de cifrado:	AES ▼						
Clave de seguridad:	Ocultar caracteres						
🔽 Iniciar esta conexión a	automáticamente						
🔲 Conectarse aunque la	red no difunda su nombre						
Advertencia: esta opo	ión podría poner en riesgo la privacidad del equipo.						
	Siguiente	Ca	ncelar				

3.- Instalación de un servidor Radius bajo Windows para autenticar conexiones que provienen de un router de acceso Linksys WRT54GL. *Comprobación en un escenario real.*

4.- Busca información sobre EDUROAM y elabora un breve informe sobre dicha infraestructura. <u>http://www.eduroam.es/</u>

¿Qué es eduroam?

eduroam (contracción de education roaming) es el servicio mundial de movilidad segura desarrollado para la comunidad académica y de investigación. eduroam persigue el lema *"abre tu portátil y estás conectado"*.

El servicio permite que estudiantes, investigadores y personal de las intituciones participantes tengan conectividad Internet a través de su propio campus y cuando visitan otras instituciones participantes.

eduroam ES es una iniciativa englobada en el proyecto RedIRISque se encarga de coordinar a nivel nacional los esfuerzos de instituciones académicas con el fin de conseguir un espacio único de movilidad. En este espacio de movilidad participa un amplio grupo deorganizaciones que en base a una política de uso y una serie de requerimientos tecnológicos y funcionales, permiten que sus usuarios puedan desplazarse entre ellas disponiendo en todo momento de conectividad.

Por otro lado, eduroam ES forma parte de la iniciativa eduroam a nivel internacional, financiada a trav&ecute;s de GEANT 3, y operada por varias redes académicas europeas y TERENA. Esta iniciativa amplía el espacio de movilidad al ámbito académico europeo, a través de eduroam Europa, y tiende puentes con eduroam Canadá,eduroam US, y eduroam APAN (Asia y Pacífico).



Mapa de localizaciones de EUROROAM en España:

Instituciones y centros participantes en eduroam ES

Aquí puede encontrar un listado de todas las instituciones y centros participantes en la iniciativa eduroam ES, ordenado por orden alfabético. En total suman **116** instituciones y centros del CSIC conectados hasta la fecha.

c) SERVIDOR LDAP:

1.- Instalación de un servidor OpenLDAP GNU/LINUX (OpenLDAP). http://www.openIdap.org/

En primer lugar instalaremos openIdap:

root@alvaroniko:/home/alvaroniko# apt-get install slapd ldap-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 odbcinst odbcinstldebian2 unixodbc
Paquetes sugeridos:
 libmyodbc odbc-postgresql tdsodbc unixodbc-bin
Se instalarán los siguientes paquetes NUEVOS:
 ldap-utils odbcinst odbcinstldebian2 slapd unixodbc
0 actualizados, 5 se instalarán, 0 para eliminar y 108 no actualizados.
Se utilizarán 5652 kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s

Durante el proceso de instalación nos pedirá una contraseña para el usuario administrador del Idap, en nuestro caso introduciremos inves.

Una vez instalado reconfiguraremos el Idap para así configurar ajustes como el nombre del dominio DNS, el nombre de la organización...Para ello ejecutamos el comando que aparece en la imagen:

Tooleactaronitico./nonen apra reconnitigare scapa r	root@al	varoniko:	/home#	dpkg-	reconfigure	slapd	
---	---------	-----------	--------	-------	-------------	-------	--

Ahora elegiremos la opcion no a la pregunta de la segunda pantalla para asi poder configurar nuestro servidor ldap:



La segunda pantalla que nos aparece es la que nos permite cambiar el nombre de dominio DNS, en nuestro caso será asir.com:

Configuració El nombre de dominio DNS se utiliza directorio LDAP. Por ejemplo, si in directorio se creará con un DN base Introduzca su nombre de dominio DNS	n de slapd para construir el DN base del troduce «mi.dominio.org» el de «dc=mi, dc=dominio, dc=org». :					
asir.com						
<aceptar></aceptar>						

Ahora introducimos el nombre de nuestra compañía, en nuestro caso asir:



La siguiente pantalla que nos aparecerá será para para cambiar la contraseña del administrador:



Deberemos de volver a introducir la contraseña:

Por favor, introduzca de su directorio LDAP para	verificar que la introdujo correctamente.				
Verificación de contraseña:					
<aceptar></aceptar>					



Ahora en la pantalla que nos permite borrar la base de datos elegimos la opción si:

Configuración de slapd
Existen ficheros en «/var/lib/ldap» que probablemente interrumpan el proceso de configuración. Si activa esta opción, se moverá los ficheros de las bases de datos antiguas antes de crear una nueva base de datos.
¿Desea mover la base de datos antigua?
<sí><no></no></sí>

Por último deberemos de elegir la opción no a la pregunta de si usaremos clientes Idap con la versión 2:

🗕 Configuración de slapd 🛏

El protocolo obsoleto LDAPv2 se ha desactivado de manera predeterminada en slapd. Los programas y los usuarios deberían actualizarse a LDAPv3. Debe seleccionar esta opción si aún tiene programas antiguos que no utilicen LDAPv3. Si lo hace, se añadirá la opción «allow bind_v2» al fichero de configuración «slapd.conf». ¿Desea permitir el protocolo LDAPv2? <Sí> Una vez configurado el Idap ejecutamos un slapcat para comprobar que los cambios se han realizado de una forma satisfactoria:



Una vez comprobados que la configuración se ha aplicado instalaremos jxplorer que es una aplicación que nos permitirá crear usaurios y unidades organizativas en open Idap de forma grafica:

```
root@alvaroniko:/home/alvaroniko# apt-get install jxplorer
```

Una vez instalado ejecutamos la aplicación jxplorer:

Una vez ejecutada en primer lugar deberemos de configurar una conexión, para ello pulsamos sobre el icono resaltado en la imagen e introducimos los valores de la imagen:

O Aplicaciones Lugares	Sistema 🔊 🗟	🛛 🏘 🔎 dom 8 de ene, 17:18 🏟 🞄
<i>₩</i>	JXplorer	_ 🗆 🗙
<u>File E</u> dit <u>V</u> iew <u>B</u> ookmark	Search LDIF Options Tools Security Help	
💋 🖉 🍏 X 🖿 🖿		
(cn 💙 =	Quick Search	
	Open LDAP/DSML Connection	<u> </u>
Explore - E Results gra	Host: localhost Port:	(389
🖉 no entries	Protocol: LDAP v3	
	DSML Service:	
	Optional Values	
	Base DN: dc=asir,dc=com	
	Security	
	Level: User + Password	✓
	User DN: cn=admin,dc=asir,dc=com	
	Password: *****	
	Use a Template	
	Save Dele	te Default
	OK Cancel Help	

En host deberemos de indicar localhost puesto que es el equipo en el que se encuentra el servidor Idap.

- En la casilla protocol elegimos LDAP v3 puesto que es la versión que utilizaremos.
- Por último en la sección security deberemos de elegir en la casilla level la opcion User + Password.
- En Base Dn introducimos dc=nombre del dominio, dc=com, es decir el nombre de nuestro dominio. En User DN introducimos cn=admin,dc=asir,dc=com. Y en password la cotraseña de nuestro usuario administrador de Idap.

Una vez conectado podremos ver el arbol de directorios de nuestro Idap:

O Aplicaciones Lugares	Sistema 🔊 🗟	📲 搚 🔎 dom 8 de ene, 19:34 🏟 🞄
<i>₽</i>	JXplorer	_ • ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u>	earch <u>L</u> DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
x x 4 k b b i	A 🛛 🗙 🗅 🗰 😽 🔍	
[.c.n] 💙 😑	✔] Quick Search	
Explore 📲 Results 🚧 Sche	Set Entry Object Classes	×
V 🚱 World	☑ Suggest Classes?	^
	Parent DN: dc=asir,dc=com	nalUnit
Þ © _∏ admin	Enter RDN: ou=grupos	
	Available Classes: Selected Classes:	

Ahora procederemos a crear una unidad organizativa para los grupos y otra para los usuarios. Para ello en primer lugarnos situaremos sobre el nombre de nuestro dominio en nuestro caso asir y pulsamos botón derecho y pulsamos la opción new:

O Aplicaciones Lugares Sistema		🏘 🔎 dom 8 de ene, 16:10 🏟 🞄
۸	JXplorer	
<u>F</u> ile <u>E</u> dit ⊻iew <u>B</u> ookmark <u>S</u> earch <u>L</u>	DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
ø ø 🚑 🗼 🖻 🛍 🔳	X D 🔤 🚸 🗉	
cn v= v Q	uick Search	
Explore 📲 Results 🚧 Schema 🖓	HTML View 🖻 Table Editor 🗎	
v 🚱 World v • com	organization/Main.html 💙	
 ✓ O asign1 ▷ I + Add to Bookmarks 	Ctrl+B JXploi	rer and
🐴 Search	Ctrl+F Main Addres	s Other
L New	Ctrl+N	
Crock a pow entry	Ctrl+Y organiza	ation
Create a new entry.	Ctrl+U Organization:	
🗎 Copy Branch	Ctrl+O	
💼 Paste Branch	Ctrl+P Description:	
Paste Alias	User Password:	
🗙 Delete	Ctrl+D Talanbana Number	
Rename	Ctrl+M	
🚸 Refresh	Ctrl+R Facsimile Number:	
	Locality Name:	
	Sub	nit Restablecer
Connected To 'ldap://localhost:389'		
📷 🔳 Terminal (como super) 👩 Problema al cargar la) 🚸 💢 plorer		

EN la pantalla que nos aparece deberemos de introducir las siguientes configuraciones. En la casilla Parent DN deberemos de introducir el nombre de nuestro dominio, es decir dc=asir,dc=com. Y en enter RDN introduciremos ou=grupos, es decir el nombre de la UO. Por ultimo deberemos de elegir el tipo de clase en nuestro caso OrganizationalUnit:

O Aplicaciones Lugares S	Sistema 🔊 🗟	📲 🏘 🔎 dom 8 de ene, 19:34 🏟 🞄
₩	JXplorer	_ • ×
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> e	earch <u>L</u> DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
x x 🖶 🗼 🖻 🗎		
cn 💙 = `	 ✓ Quick Search 	
Explore Results M Sche	le Set Entry Object Classes	
V 😡 World	☑ Suggest Classes?	
✓ O asir	Parent DN: dc=asir,dc=com	nalUnit
🕨 🖉 admin	Enter RDN: ou=grupos	
v 🚵 usuarios	Available Classes: Selected Classes:	
	person	
	Add Bemove	
	OK Cancel Help	
	registeredAddress	
	searchGuide	
	seeAlso	V
	Submit Reset Cha	ungo Class
		Fiopercies
Connected To 'ldap://localhost::	389'	
📷 🛛 🖾 Terminal (como supe	r 🧑 JXplorer	

Ahora realizamos los mismos pasos para crear la UO usuarios.

Una vez creada las 2 UO procederemos a la creación del grupo Profesores, para ello nos colocamos sobre la UO grupo/ botón derecho/new. En la pantalla introcucimos los valores que se muestran en la imagen:

Explore 📲 Results 🚧 Sche	🚸 Set Entry Object Classes 🛛 🛛	
▼ 🚱 World	☑ Suggest Classes?	^
▼ ● asir	Parent DN: ou=grupos.dc=asir.dc=com	nalUnit
P 📲 admin	Enter RDN: cn=profesores	
<table-of-contents> usuarios</table-of-contents>	Available Classes: Selected Classes: pKICA pkiUser posixAccount qualityLabelledData	
	Add Remove	

En la siguiente pantalla deberemos de añadir el gidNumber que es el numero del grupo, en nuestro caso será 1001, cuando finalizemos pulsamos submit:

📀 Aplicaciones Lugares Sistema 👰		🙀 🔎 dom 8 de ene, 19:37 🏟 🙏
♠	JXplorer	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DIF	<u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
x x 💩 x 🖻 🖻 🖷 🛛 🗙	🗅 📼 🚸 🕒	
	Search	
Explore 📲 Results 🏘 Schema 🖫	Table Editor 🗈	
▼ 🚱 World	attribute type	value
✓ • com	cn	profesores
▶ [©] admin	gidNumber	1001
🚊 grupos	objectClass	posixGroup
is usuarios	objectClass	top
	description	
	memberUid	
	Submit Reset Cha	ange Class Properties
Connected To 'ldap://localhost:389'		
📷 🛛 🖾 Terminal (como super 🛛 🞄 👂	plorer	<u></u>

Ahora crearemos el grupo alumnos:

O Aplicaciones Lugares	Sistema 🔊 🗟	🏘 🔎 dom 8 de ene, 19:40 🏟 🞄
<i>₩</i>	JXplorer	_ • ×
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>B</u> ookmark <u>S</u> e	earch <u>L</u> DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
X X 🖨 🗼 🖻 🖷	1 🛛 🕇 X 🗠 📼 🛛 🚸 🖢	
cn 💙 = 🗎	✔] Quick Search	
Explore • 🗄 Results 🏟 Sche	Set Entry Object Classes	
V 🚱 World	☑ Suggest Classes?	^
v • com v • asir	Parent DN: ou=grupos,dc=asir,dc=com	nalUnit
D © admin	Enter RDN: cn=alumnos	
P_∎ profesores	Available Classes: Selected Classes:	
🎇 usuarios	account posixGroup	
	alias	
	applicationEntity	
	Add Remove	
	OK Cancel Help	
	I I I a state a state	
En el grupo alumnos asignaremos el gid 1002:

📀 Aplicaciones Lugares Sistema 🥷		🏘 🔎 sáb 14 de ene, 20:01 🌒 🞄
*	JXplorer	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DI	F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
x x 💩 🗼 🖻 🖻 🔳 🗄	X D 📾 🚸 🜑	
cn V= V Qui	ck Search	
Explore 📲 Results 🏘 Schema 🖓	Table Editor 🖺	
🗢 🚱 World	attribute type	value
	cn	alumnos
D [®] ⊟ admin	gidNumber	1002
🕨 🦂 grupos	objectClass	posixGroup
🕨 🤉 🎆 usuarios	objectClass	top
	description	
	memberUid	
	userPassword	

Una vez creado los grupos deberemos de crear usuarios, en el grupo profesores crearemos al usuario niko1 y en el grupo alumnos crearemos al alumno1.

En primer lugar crearemos al usuario niko1, para ello nos situaremos sobre la UO usuarios/botón derecho/new.

🜔 Aplicaciones Lugares Sistema 🐔		🏘 🔎 dom 8 de ene, 19:57 🏟 🚸
*	JXplorer	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DIF	<u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
ø ø 💩 🗼 🖻 🖻 🖷 🔺 🗙	(🗅 📼 🚸 🕒	
	< Search	
Explore 📲 Results 🏘 Schema 🗣	HTML View 🗈 Table Editor 🖺	
Vorld	attribute type	value
✓ ● com	objectClass	organizationalUnit
▷ ^Q _□ admin	objectClass	top
∽ grupos	ou	usuarios
D Bannos	businessCategory	
v ♥ profesores		
 Add to Bookmarks 	Ctrl+B	
💏 Search	Ctrl+F tionaliSDNNumber	
D New	Ctrl+N	
Copy DN	Ctrl+Y	
人 Cut B Copy the distin	guished name of an entry to the clipboa	ard
	Ctrl+O iceBox	
	ctul p edDeliveryMethod	
Paste Branch	redAddress	
Paste Alias	Guide	
X. Delete	Ctrl+D 2	
📼 Rename	Ctrl+M	
📃 🎻 Refresh	Ctrl+R Submit Reset Ch	ange Class Properties
Connected To 'ldap://localhost:389'		
🔯 🕼 JXplorer 🔳 Te	rminal (como super	<u>^</u>

En la pantalla que nos ha aparecido debremos de introducir los siguientes valores. EN Pren DN introduciremos el nombre de la UO y el nombre del dominio y en RDN introduciremos el nombre del usuario:

O Aplicaciones Lugares Si	stema 🔊 🗟	🏘 🔎 dom 8 de ene, 19:58 🏟 🞄
<i>₽</i>	JXplorer	
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>B</u> ookmark <u>S</u> ea	arch <u>L</u> DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
x x 🖶 🗼 🖻 🛍 📾	🔳 🗙 🗅 📼 💰 🕒	
	Quick Search	
Explore 📲 Results 🏘 Sche	Set Entry Object Classes	
▼ Sworld ▼ • com ● asir ● ⊕ admin ▼ ● □ □ □	✓ Suggest Classes? Parent DN: ou=usuarios,dc=asir,dc=com Enter RDN: cn=niko Available Classes: Selected Classes: pRICA price posixGroup price qualityLabelledData posixAccount Add Remove	nalUnit
	OK Cancel Help registeredAddress searchGuide seeAlso Submit Reset Char	nge Class) Properties
Connected To 'Idap://localhost:3	89'	
📖 💑 Jxplorer	erminal (como super	

Ahora deberemos de indicar el numero del usuario(uidnumber) y del grupo(gidnumber), ambos valores serán 1001, a su vez el sn y el uid son campos obligatorios a rellenar. Otro campo a rellenar será el homeDirectory que será el directorio del usario:

O Aplicaciones Lugares Sistema	2		🏶 🔎 dom 8 de ene, 20:00 🏟 4	þ
*		JXplorer		3
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u>	DIF	<u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp		
x x 💩 🗼 🖻 🛍 🔳 🗎	×	🗋 🗅 📼 🛛 🚸 🖢		
cn 💙 = 💙 🛛 Qu	uicl	Search		
Explore 📲 Results 🏘 Schema 🖓		Table Editor 🗈		
🗢 🚱 World		attribute type	value	-
✓ • com	L	cn	niko1	
	L	gidNumber	1001	
		homeDirectory	/home/niko1	
▷ 📴 alumnos		objectClass	InetOrgPerson	
▶ [®] profesores		objectClass	organizationalPerson	1
🏯 usuarios		objectClass	person	
		objectClass	top	
		op	Copzoloz	
		uid	nikol	
		uidNumber	1001	
		audio		
		businessCategory		
		carLicense		
		departmentNumber		
		description		
		destinationIndicator		1
		Submit Reset C	hange Class Properties	
Connected To 'ldap://localhost:389'				
🔯 🕀 JXplorer 🛛 🖪	Te	rminal (como super	<u></u>	

Ahora crearemos el usuario alumno1 que estará integrado en el grupo alunos:

O Aplicaciones Lugares S	istema 🔊 🗟 🏾 🖉 🦊	dom 8 de ene, 20:04 🏟 🚸
<i>₩</i>	JXplorer	
<u>F</u> ile <u>E</u> dit <u>∨</u> iew <u>B</u> ookmark <u>S</u>	earch <u>L</u> DIF <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
\$ \$ # B B B		
(cn) =		
Explore 📲 Results 🚧 Sche	🚷 Set Entry Object Classes 🛛 🗙	
Vorld	✓ Suggest Classes?	^
v ● com v ● _asir	Parent DN: ou=usuarios,dc=asir,dc=com	nalUnit
▶ ® admin	Enter RDN: cn=alumno1	
D ∎ alumnos	Available Classes: Selected Classes:	
D B profesores	account 🚔 inetOrgPerson	=
Þ © _∃ niko1	alias 📃 person	
	applicationEntity posixAccount	
	Add Remove	
	OK Cancel Help	
	registeredAddress	
	searchGuide	
	Submit Reset Change Class	Properties
Connected To 'Idap://localhost:	389'	
💿 \land IXplorer	🔳 Terminal (como super	

Ahora introducimos los números de usuario y del grupo:

🕐 Aplicaciones Lugares Sistema 🐔	▶ 6₫	🏶 🔎 dom 8 de ene, 20:07 🏟 🞄
*	JXplorer	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>B</u> ookmark <u>S</u> earch <u>L</u> DI	F <u>O</u> ptions <u>T</u> ools Secur <u>i</u> ty <u>H</u> elp	
x x 💩 🗼 🖻 🛍 🔳 🔀	K 🗅 🔤 🚸 🕒	
	k Search	
Explore 📲 Results 🏘 Schema 🖓	Table Editor 🗈	
🗢 🚱 World	attribute type	Value
✓ • com	cn	alumpo 1
V ∎ admin	gidNumber	1002
	homeDirectory	/home/alumno1
N [™] alumnos	objectClass	inetOrgPerson
▶ ® _∎ profesores	objectClass	organizationalPerson
🔽 🧟 usuarios	objectClass	person
🕨 🖉 nikol	objectClass	posixAccount
	objectClass	top
	sn	
	uidNumber	1002
	audio	
	businessCategory	
	carLicense	
	departmentNumber	
	description	
	destinationIndicator	
	Submit Reset Ch	nange Class Properties
Connected To 'ldap://localhost:389'	-	
🔯 🔥 JXplorer 🛛 🔳 1	erminal (como super	4

Una vez creados los usuarios y los grupos ejecutaremos uns slapcat para ver que la configuración ha sido implementada correctamente:

O Aplicaciones	s Lugares Sistema 👩 줐	🙀 🔎 dc
A.	JXplorer	
	Terminal (como superusuario	o) 🗌
<u>A</u> rchivo <u>E</u> dita	r <u>∨</u> er <u>T</u> erminal Ay <u>u</u> da	
creatorsName: createTimesta entryCSN: 201 modifiersName modifyTimesta	cn=admin,dc=asir,dc=com mp: 20120108183514Z 20108183514.502785Z#000000#000#000000 : cn=admin,dc=asir,dc=com amp: 20120108183514Z	
dn: cn=profes cn: profesore gidNumber: 10 objectClass: structuralObj entryUUID: 85 creatorsName: createTimesta entryCSN: 201 modifiersName modifyTimesta	cores,ou=grupos,dc=asir,dc=com 201 posixGroup top ectClass: posixGroup 2066524-ce73-1030-93b4-0773b15569d7 c cn=admin,dc=asir,dc=com amp: 20120108183717Z L20108183717.918891Z#000000#000#0000000 e: cn=admin,dc=asir,dc=com amp: 20120108183717Z	

Ahora creamos los directorios de conexión de nuestros usuarios:

root@alvaroniko:/home/alvaroniko# touch prueba /home/alumnol root@alvaroniko:/home/alvaroniko# mkdir /home/nikol

Por último reiniciaremos el openLdap:

root@alvaroniko:/home/alvaroniko# service slapd restart Stopping OpenLDAP: slapd. Starting OpenLDAP: slapd. root@alvaroniko:/home/alvaroniko# Ahora ejecutaremos un Idapsearch para comprobar que los usuarios se han creado satisfactoriamente:

Usuario niko1:

Circuiso Edirai Zei Terrunai VAñaa	
root@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=nikol)' # extended LDTE	
#	
# LDAPv3 # base <dc=asir.dc=com> with scope subtree</dc=asir.dc=com>	
# filter: (cn=nikol)	
# requesting: ALL #	
<pre># nikol, usuarios, asir.com dn: cn=nikol,ou=usuarios,dc=asir,dc=com cn: nikol gidNumber: 1001 homeDirectory: /home/nikol objectClass: inetOrgPerson objectClass: organizationalPerson objectClass: person objectClass: person objectClass: top sn: Gonzalez uid: nikol uidNumber: 1001</pre>	
# search result	
search: 2 result: 0 Success	
# numResponses: 2 # numEntries: 1	Usuario
alumno1:	Coddino
ioot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF #	
pot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3	
<pre>[pot@alvaron1k0:/home/alvaron1ko# ldapsearch -x -b 'dc=as1r,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=as1r,dc=com> with scope subtree # filter: (cn=alumno1)</dc=as1r,dc=com></pre>	
<pre>noot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL</dc=asir,dc=com></pre>	
<pre>doot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL #</dc=asir,dc=com></pre>	
<pre>pot@alvaron1k0:/home/alvaron1ko# ldapsearch -x -b 'dc=as1r,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # alumno1. usuarios. asir.com</dc=asir,dc=com></pre>	
<pre>pot@alvaron1k0:/home/alvaron1ko# ldapsearch -x -b 'dc=as1r,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com</dc=asir,dc=com></pre>	
<pre>pot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL # # alumnol, usuarios, asir.com dn: cn=alumnol,ou=usuarios,dc=asir,dc=com cn: alumnol idta in the state is a s</dc=asir,dc=com></pre>	
<pre>igot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL # # alumnol, usuarios, asir.com dn: cn=alumnol,ou=usuarios,dc=asir,dc=com cn: alumnol gidNumber: 1002 homeDirectory: /home/alumno1</dc=asir,dc=com></pre>	
<pre>dot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL # # alumnol, usuarios, asir.com dn: cn=alumnol,ou=usuarios,dc=asir,dc=com cn: alumnol gidNumber: 1002 homeDirectory: /home/alumnol objectClass: inetOrgPerson </dc=asir,dc=com></pre>	
<pre>pot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL # # alumnol, usuarios, asir.com dn: cn=alumnol,ou=usuarios,dc=asir,dc=com cn: alumnol gidNumber: 1002 homeDirectory: /home/alumnol objectClass: organizationalPerson objectClass: person</dc=asir,dc=com></pre>	
<pre>dot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL # # alumnol, usuarios, asir.com dn: cn=alumnol,ou=usuarios,dc=asir,dc=com cn: alumnol gidNumber: 1002 homeDirectory: /home/alumnol objectClass: inetOrgPerson objectClass: person objectClass: posixAccount </dc=asir,dc=com></pre>	
<pre>pot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumnol)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumnol) # requesting: ALL # # alumnol, usuarios, asir.com dn: cn=alumnol,ou=usuarios,dc=asir,dc=com cn: alumnol gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: posixAccount objectClass: top sn: 1</dc=asir,dc=com></pre>	
<pre>dot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com cn: alumno1 gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: organizationalPerson objectClass: posixAccount objectClass: top sn: 1 uid: alumno1</dc=asir,dc=com></pre>	
<pre>noot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com cn: alumno1 gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: posixAccount objectClass: top sn: 1 uid: alumno1 uidNumber: 1002</dc=asir,dc=com></pre>	
<pre>dot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com cn: alumno1 gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: posixAccount objectClass: top sn: 1 uid: alumno1 uidNumber: 1002 # search result</dc=asir,dc=com></pre>	
<pre>loot@alvaroniko:/home/alvaroniko# [dapsearch -x -b 'dc=asir,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com cn: alumno1 gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: organizationalPerson objectClass: top sn: 1 uid: alumno1 uidNumber: 1002 # search result search result search: 2 result: 0 Surcess</dc=asir,dc=com></pre>	
<pre>dot@alvaroniko:/home/alvaroniko# ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumno1)' # extended LDIF # # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com cn: alumno1 gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: person objectClass: posixAccount objectClass: top sn: 1 uid: alumno1 uidNumber: 1002 # search result search: 2 result: 0 Success</dc=asir,dc=com></pre>	
<pre>loot@alvaroniko:/home/alvaroniko# Ldapsearch -x -b 'dc=asir,dc=com' '(cn=alumno1)' # extended LDIF # LDAPv3 # base <dc=asir,dc=com> with scope subtree # filter: (cn=alumno1) # requesting: ALL # # alumno1, usuarios, asir.com dn: cn=alumno1,ou=usuarios,dc=asir,dc=com cn: alumno1 gidNumber: 1002 homeDirectory: /home/alumno1 objectClass: inetOrgPerson objectClass: organizationalPerson objectClass: person objectClass: top sn: 1 uid: alumno1 uidNumber: 1002 # search result search: 2 result: 0 Success # numResponses: 2 # numResponses: 2</dc=asir,dc=com></pre>	

2.- Instalación de un cliente LDAP bajo Windows o GNU/Linux para autenticarse.

NO HE DOCUMENTADO ESTA PARTE PORQUE DE MOMENTO NO HE CONSEGUIDO QUE EXISTA CONECTIVIDAD ENTRE LOS CLIENTES LDAP Y EL SERVIDOR LDAP

3.- Busca información sobre LDAP y su implementación en productos comerciales.

Descripción

LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas. **Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica.** El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos y/o organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras,

documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Un directorio LDAP lo componen:

- Un directorio es un árbol ordenado de entradas
- > Una entrada consta de un conjunto de atributos.

- Un atributo tiene un nombre (un tipo de atributo o descripción de atributo) y
- uno o más valores.
- Los atributos son definidos por un esquema
- Cada entrada tiene un identificador único: su Nombre distintivo
- > (Distinguished Name, DN).

Usos empresariales

Dadas las características de LDAP sus usos más comunes son:

- **Directorios de información**. Por ejemplo bases de datos de empleados organizados por departamentos (siguiendo la estructura organizativa de la empresa) ó cualquier tipo de páginas amarillas.

- **Sistemas de autenticación/autorización centralizada**. Grandes sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Por ejemplo:

o **Active Directory Server de Microsoft,** para gestionar todas las cuentas de acceso a una red corporativa y mantener centralizada la gestión del acceso a los recursos.

o **Sistemas de autenticación para páginas Web**, algunos de los gestores de contenidos más conocidos disponen de sistemas de autenticación a través de LDAP.

o Sistemas de control de entradas a edificios, oficinas....

- **Sistemas de correo electrónico.** Grandes sistemas formados por más de un servidor que accedan a un repositorio de datos común.

- Sistemas de alojamiento de páginas web y FTP, con el repositorio de datos de usuario compartido.

- Grandes sistemas de autenticación basados en RADIUS, para el control de accesos de los usuarios a una red de conexión o ISP.

- Servidores de certificados públicos y llaves de seguridad

- Autenticación única ó "single sign-on" para la personalización de aplicaciones.

- Perfiles de usuarios centralizados, para permitir itinerancia ó "roaming"

- Libretas de direcciones compartidas.

Ejemplos de uso de LDAP

Sistema de correo electrónico

Cada usuario se identifica por su dirección de correo electrónico, los atributos que se guardan de cada usuario son su contraseña, su límite de almacenamiento (quota), la ruta del disco duro donde se almacenan los mensajes (buzón) y posiblemente atributos adicionales para activar sistemas anti-spam o anti-virus.

Como se puede ver este sistema LDAP recibirá cientos de consultas cada día (una por cada email recibido y una cada vez que el usuario se conecta mediante POP3 o webmail). No obstante el número de modificaciones diarias

es muy bajo, ya que solo se puede cambiar la contraseña o dar de baja al usuario, operaciones ambas que no se realizan de forma frecuente.

Sistema de autenticación a una red

Cada usuario se identifica por un nombre de usuario y los atributos asignados son la contraseña, los permisos de acceso, los grupos de trabajo a los que pertenece, la fecha de caducidad de la contraseña...

Este sistema recibirá una consulta cada vez que el usuario acceda a la red y una más cada vez que acceda a los recursos del grupo de trabajo (directorios compartidos, impresoras...) para comprobar los permisos del usuario. Frente a estos cientos de consultas solo unas pocas veces se cambia la contraseña de un usuario o se le incluye en un nuevo grupo de trabajo.