How to setup L2TP/IPsec with RADIUS Server (Windows 2008)



Introduction: The situation in my topology is when the VPN client try to build the tunnel with the DFL, the DFL will authenticate the client by RADIUS server which is located in it's LAN.

Step:

1. Setup L2TP's server, pool, and RADIUS server in DFL's Address Book.

😪 marine 📲 Configuration - 📲 Tool	is 🔹 💰 Status	+ Hantenance +			🗳 Liigeid	2 metp
CPL-660E	Addre	ss Book se Book contains symbolic name	s fur various types of addresses, indu	Sing IP networks and Ethemet NAC	alikesses.	
Oate and Time OBS OBS OBS OBS OBS OBS	2 ANI +	Name	Address -	Dear Auth Groups -	Commonts -	
DHCP Servers	2 2 4 5	SIFnets L2TP-Server L2TP-Pool Radius-Server	0.0.0.0/0 10.0.0.1 10.0.0.10-10.0.0.20 192.168.10.200		All possible network	ta .
Hardware Montoring Hardware Montoring Setting Wintelef Advanced Settings CP Settings CP Settings Cons. Timeout Settings Cons. State Settings Cons. Settings Constant Setti				(Right-	dict on a rowfor additional op	bons.

2. Setup IPsec's pre-shared key in Authentication Object.

PSK (Pre-Share	d Key) authentication is	based on a shared secret that is known only by the parties involved.	
General			
🔊 General			
Name: IPsec-I	key		
Shared Secr	et		
o Passphrase			38
Shared Secret		Note! Existing secret will always be shown with 8 characters to hide the actual length.	
Confirm Secret			

3. Setup IPsec interface, with following information. NOTE: Local Network: wan1_ip

	S Pace
LDAP ILDAP IKE Config Mode Pool	General Authentication XAuth Routing IKE Settings Keep-alive Advanced
HE Algorithms Place Algorithms HTTP Bannet Files Rules B 19 Roses B 19 Roses H 10 Roses C 40 Cocess	Nama: IPpec Local Namedit: wanijap M Rempte Notwerk: all-mete v Remate Endpoint: (None) v Encapsutation modal Transport v
Interfaces I	Migorithms RE Rigerithms NE Litismic 28800
PPTPL_2TP Servers PPTPL_2TP Clients Satch Management Uniterbace Groups PARP Parters	Prec Agorffreie: Maduum Sacods Prec Lifetime: 3600 Seconds Prec Lifetime: 0 Hadytus
H OP/PS	Comments
User Authentication Geocal User Databases Adminusers Qeocal (27P-db	Commerte
Accounting Servers	OK Cancel

An and the second	Psec An Pace Lumes term is used to define Pase endpoint and will appear as a logical interface in the sector
- UDAP	General Automatication Vieth Busines WEStellings Viets Size Advanced
IKE Config Mode Pool	selectar methodation what methodate methodate weathered
- D LBB	Authentication
KE Algorithms	Call 2.20th Parallelina
Psec Algorithms	0
HTTP Banner Files	Roof Certificate(#)
E 🙀 Russ	Wallable Selected
El- 🚦 IP Rules	
an_to_wan1	
GLACCESS	
TUPOLAN	
10 iDise	
AN ORF	
-CR PPPaE	Gateway cartificate: (Norm)
PPTP/LZTP Servers	Identification list (Nerver)
PPTPA,2TP Cients	
Switch Management	Pite-strand Key
Thinterface Groups	Providence data Internet land
ARP +	and a set of the set o
iti Ga Routing	O Local D
E SP/1P9	
E duser Authentication	Local ID Type Auto M Selects the type of Local ID to use
🖯 🕜 Local User Databases	Local D Value Specify the local identity of the turnel ID
Adminüsers	
121P-dD	
Citemal User Databases	OK Cancel
Mocconning general +	
C C C C C C C C C C C C C C C C C C C	IPSec
DAP	and the second second second a second s
Contract Contract Node Mox	General Authentication XAuth Routing IKE Settings Keep-alve Advanced
INCE Algorithms	C) Poulling
IDser Algorithms	2 roung
HTTP Banner Files	Addy CHCP, ONE shall don't single-nost classes
El-18 Rules	Dimartically add route to the remote network when a furnel is established
😑 🛢 IP Rules	
tan to want	Packet Sizes
Access	Specify the size at which is fragment plainted packets (rather than fragmenting (Pave).
El al Interfaces	Flainbert MTU 1420
Ethernet	
- EBVLAR	IP Addresses
A DOF	Automatically pick the address of a local interface that corresponds to the local net
- M PPPoF	 Specify address manually
PPTP/L2TP Servers	(Paddress (mone)
PPTPA_2TP Clients	
- Setuh Management	
	OK Cantal
#ARP #	
E us Routing	
H GIDP / IPS	
E Guser Authentication	
es 😰 Local User Databases	
Adminusers	
Colored Deer Databases	
Accounting Servers	



4. Setup L2TP's interface. NOTE: Outer interface filter: IPsec interface

WIRE O LBB		erver interface bermin	ates PPF (Point to Po	int Protocol) Summels set	up over existing IP networks	
Pres Agonthem HTTP Banner Files	General PPP Parameters Add Route					
🕀 🛊 P Ruies	Name	1219-4				
Can_to_want	HouriP Addiss:	12TP-Server	~			
E interfaces	Tunnel Protocol	L21P	¥.			
Ethemet	Outer Interface Filter	IPsec	Y			
- Carlos Pisec	Server IP:	wan1_p	~			
- R GRE) Comments		_			
Sadch Management	Comments				10	
Routing						OK Carcel

350 Rf2 (U L1818		
IKE Algorithms	APT (Tap) Tap) and the second se	
Psec Algorithms	General PPP Parameters Add Route	
- / HTTP Banner Files		
E S Rules		
HI S IP Rules	Specify FUser Authentication Rules and to be used, and the encryption strengths allowed. Also specify the P address assignment an information to based activity compared clarity.	Id the DNS/WINS server
tan_to_want	my Use User Authentication Rules	
Ca Accesa	No. of the second se	
El-unimentaces		
Ethernet	AT Microsoft Point-to-Point Encryption (MPPE)	
- WLAN	10 Nore	
- 🔅 Psec	(J) RC+40.54	
-RO GRE	IN RCASENE	
PPPoE		
PPTP/L2TP Servers	RE HC+ 120 bit	
PPTP%_2TP Cients	Stateful UPPE Seas secure, use only for compatibility)	
Switch Management		
	P Pool	
ARP		
🗄 🙀 Routing	PPost L2TP-Post	
E DP / IPS		
E 🛃 User Authentication	Primary Secondary	
E Local User Databases 👘	DNE (None) V (None)	
Adminüsers	Americana Disease)	
LITP-db	Handahana (Hanua) 🔤 (Anua)	
External User Databases		
Accounting Servers		
- Se User Authentication Rules		OK Carcel
A Authoritecture Commun		
UP INE ILU LISIS	L2TP-#	
- 2 KE Agonthma	APPTICATION SHOP CONTRACTOR AND A CONTRACT AND A CO	
Psec Algorithms	General PPP Parameters Add Route	
HTTP Banner Flere	A) Filter	
E Bules	Restricts asterny. Destroyments and asternet at the added	
ten to want	Allowed filehours all-costs	
Access		
12 wierlaces	Proxy ARP	
Ethernel	Interface to ASP publicit the added round on.	
- LIII VLAN	Proxy ARP Interfaces	
- 20, 1005	Austicide Delected	
- CR PUPPO	L2TP-tan	
PPTP/L2TP Servers	wanii	
THE PERTINE THE CLEARE	wanz >>	
Switch Management	56	
Alls		
In the rest of the second	Aware benefit ALL Wenfaces, including new ones.	
- CALIber Admentication		
El Cocal User Databases		The second se
Administers		Cincel

5. Group the interfaces, L2TP and Ian, for ip rule.

O INC & LORS	L2TP-lan Use an interface your to common enveron attentaces for a simplified security parkey
Plans Agginttims HTTP Barner Flass Foldes S P Rules S P Rules S Inc. to want	Ceneral Ceneral Same L279-Ian Securit/Torrupot Equivalent
Control Control Control Control Contro Control Control Control	Nationale Available
Addremitisers	Comments
External User Databases	OK Cancel

6. Setup ip rule.

Add	-						
	1 L2TP-lan	Allow	Gro II 1-1-1 L2TP-lan	all-nets	Bust #	all-nets	all_tcpudpicmp
1	g lan_to_wan1	Allow	121 Ian	🤘 lannet	Core	🤘 lan_ip	ping-inbound

General	Log Settings	NAT	SAT MI	ultiplex SAT	SLB SAT	SLB Monit	ors		
👩 Genera	al								
Name:	L2TP-lan								
Action:	Allow	~							
Service:	all_tcpudpicmp	~							
Schedule:	(None)	~							
Addre:	ss Filter ce interface and source	ce network,	together with destina	ition interface a	nd destination r	etwork. All param	eters have t	to match for the	rule to match.
D Addre:	ss Filter ce Interface and source Interface	ce network,	together with destina	ition interface a	nd destination r	etwork. All param	eters have t	to match for the	rule to match.
Addre: Specify source	ss Filter ce Interface and source Interface L2TP-lan L2TP-lan	ce network,	together with destina Network all-nets all-nets	ition interface a	nd destination r	etwork. All param	eters have t	to match for the	rule to match.
Specify source: Source:	ss Filter ce Interface and source Interface L2TP-lan L2TP-lan	ce network,	together with destina Network all-nets all-nets	ition interface a	nd destination r	ietwork. All param	sters have t	to match for the	rule to match.
Addre: Specify source: Destination: Orm	ss Filter ce interface and source interface L2TP-lan L2TP-lan	ce network,	together with destina Network all-nets all-nets	ition interface a	nd destination r	etwork. All param	eters have t	to match for the	rule to match.
Addre Specify sour Source: Destination: Comments:	ss Filter ce Interface and source Interface L2TP-lan L2TP-lan	ce network,	together with destina Network all-nets all-nets	ation interface a	nd destination r	ietwork. All param	sters have t	lo match for the	rule to match.
Addre: Specify source: Source: Sestination: Comments:	ss Filter ce Interface and source Interface L2TP-lan L2TP-lan	ce network,	together with destina Network all-nets all-nets	ation interface a	nd destination r	ietwork. All param	eters have t	to match for the	rule to match.

7. Setting External Authentication for RADIUS

G Rules	General General	
Access Access Interfaces Contents Conte	Norme Radius P Address Radius-Server V Seconds Pett 1912 Refy Timeout 2 Shared Second Access Records Contem Second Access Records Contemnate Access Records Comments	with 0 charindans in hide the actual langue.
ABS Counting C	Comments	

8. Setting Authentication Rule. (Finish the DFL's setting)

- @ Psec Agorithms	Radius-auth The Star Activentication Releast appealing from where users are abuved to authenticate to the system, shull have	
HTTP Banner Files	General Log Settings Authentication Options Accounting Agent Options Restrictions	
Runch	and the second	
A. MORD	A General	
ian_to_wan1		
Access	Patho	
niertaces	Auftentication agent ppp	
Ethernet	Adhertsater Source RADIUS	
LEVLAN		
S Pher.	Trankx (277-4 M	
NI OAE	Chigh stor P ⁴ all-viet x 🕑 💽 Por XAuth and PPPP the is the further originator IP	
PPPOE	Terminate @ wani_in @	
PPTP/LITP Servers		
PPTP/L2TP Clambs	* Comments	
- Switch Management		
meetace croups	Commenta	
MRP 1		
gnituus		
P/IPS		
ser Authentication	04	Eano
Local User Databases		
Automication Releases		
User Autoenteation Rules	Redus-auth The User Anthermation Multised spontose from where oversize attained to anti-indicate to the system, and have Description of Sections Authority and October Accounting Account	
Base Automitation Balan	Redius-auth The User Authentication fluence and then where users are alween to authenticate is the watern, and how General Log Settings Authentication Options Accounting Agent Options Restrictions	
Ober Aufsentigsen föllinge	Redius-auth The Over Anthermution Pointeel spoultes from where over an attenditive authoriticate is the system, and have General Conserver Log Settings (Authentication Options) Accounting Agent Options (Restrictume +) General	
Clear Automication Rules Actionic atom (Strongs Actionic Automication (Strongs Action Contents) Action Contents Action Conten	Rectius-auth The Older Authoritization Prototics Than where users are attracted to the system, and then General General	
Roac Agentication Balan Action Story Action Story Action Story Action Story S	Redius-auth The User Authentication fluinsed apolities from where users are allowed to adheridicate is the wattern and how General Defect and to more suffernitication centers. Web select the authentication riskfood, which is used for emcopiling the user password. Defect and to more suffernitication servers. Web select the authentication riskfood, which is used for emcopiling the user password.	
IPaer Automication Rules Actioning providences IPaer Agginthms HTTP Banner Files tetes Proces Join to want Access Incluses	Redius-auth The User Anti-interaction Hubble Internation oners are attracted to the system, and new General	
Unar Autoentication Rules Actionatic atom technique Insec Algorithms HTTP Banner Files HTTP Banner Files Secs	Redius-auth The Over Authoritization Provides from where users are atteacted and an endoced to the system, and how Centeral Centeral Select one or insert authentication servers. Also asted the authentication mathod, which is used for encrypting the user parameters Redius anywar Audio	
Road Autoentication Rules Activation Strongs Road Autoentication Strongs Road Autoentication Strongs Road Autoentication Road	Redus-auth The User Authentication Humanian ones an always to adhered by the water, and hum General Log Settings Authentication Options Accounting Agent Options Reduction Ceneral Delicit are to more suffernication servers. Hiso saled the authentication riskford, which is used for emorphing the user passweed. Reduct server Authentication Reduct	
Clear Automication Rules Automic Converting Automatic atom restroys ATTP Banner Flags ATTP Banner Flags Attris Process Process Converting Access Process Process Proces P	Redius-auth The Older Anthematics management of autoentic autoentication in the system, and have General General Second Autoentication autoentication Options Accounting Agent Options Redinctions Redinct autoentication servers. Also saled the authentication method, which is used for encoping the user parameter. Redinct autoentication	
	Redius-auth The Clean Authority at an intervention of plants and an ensemble authority authority and the motion, and them Connerval Conn	
	Redus-auth The User Authoritization Humanian positive from where one is an adverted to adheridicate is the wattern and hum General Log Sentral Deficit and to more suffernitization centrers. We sailed the authoritization interfood, which is used for emcoping the user passwerd. Redus server maintee findum	
Clear Automication Rules Automic Convertigence ITTP Banner Flags ITTP Banner Flags ItTs Proces Proc	Reclius-auth The Ouer Authomation mained spectrum where uses an animatic authomatic out in the system, and have Converse	
Hoar Automication Rules Activation to the testing Articular Automication Sciences Article Automication Files Article Automication Files Article Automication Article Automicatio Article Automication Article Automication Article Aut	Redius-auth The User Authentication Rules of spatializes from where users are element to adfracticate to the woten, and hum Conserve Log Settings (Authentication Option) Accounting Agent Options Restrictions Conserve Log Settings Conserve Log Settings Defected	
Clear Activities and the second seco	Redus-auth The User Authoritization Humanian mension are at advantation and the option, and hum Connersal Log Settings Authoritization Options Accounting Agent Options Reductions Reduction Reductions R	
Clear Autoentication Rules Autoentication (Schorgs Autoentication (Schorgs Autoentication (Schorgs Autoentication) F Proces F Proces F Proc	Reclus-auth The User Authomatics in the where users are attended to advected bit the wystem, aid them Converse Log Settings Authomatics and where a set of the advected attended which is used for encrypting the user parameters Actival servers Actival	
Liner Aufwentextum Rules Annother provingeneration Annother Press Annoth		
	Control Authomatication managements are assessed and activation of the system, and them Conversit Log Settings Authomatication matrices users are assessed to activation of the system, and them Conversit Log Settings Authomatication matrices users are assessed to activation of the system, and them Conversit Log Settings Authomatication matrices, and the system and th	
	Reduse auth The User Authority also influence specifies many where users are elseworthy authority and setting and the worten, authority Concernant Log Settings Undiversification Ceptions Accounting Agent Opmons Restrictuum Concernant Log Settings Undiversification method, which is use Sfore emorphing the user parameters Concernant Settings Meanume, Honor, dween, Settings	
	Recluse auth The Clear Authonic action instances appointed in positive internation operations and movement to authonic clear in and move Clear Authonic action operations Accounting Agent Clear Data Clear Authonic action operations Accounting Agent Clear Data Clear Authonic action operations Accounting Agent Clear Data Clear Authonic action operations Accounting Agent Clear Data Clear Authonic action clear Data Accounting Agent Clear Data Clear Authonic action clear Data Accounting Agent Clear Data Decisional Accounting Agent Clear Data Decisional Accounting Agent Clear Data Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accounting Accountin	
	Concernant Automatication many views users are attended to advected to the system, aid time Concernant Log Settings Automatication advected and advected and the system, aid time Concernant Concernant Agent Options Restructuure Concernant Concernant Agent Options Restructuure Concernant Concernant Concernant Agent Options Restructuure Concernant Concernant Concernant Concernant Restructuure Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant Concernant	
	Sectors Authority can be added to particular them where were any advanced to advance out and advance out adv	
	Recluse auth The Close Authentication resides represented and well on our and answer close on an answer close on the system, and these Concerning Log Sentings Authentication contexts Accounting Agent Close on an answer close anternation of the system and the syst	

	Radius-auth The User Archentication Roleant specifies from where users are adveed to authenticate to the system, and from
HTTP Banner Files	General Log Settings Authentication Options Accounting Agent Options Restrictions
E d Rules	General
	Search one or more accounting servers. Also select the statistics for the authenticated user that should be sent to the accounting server. Accounting servers
Chemiel Chemiel Constant Co	Available Bailable Ba
at a rep / upp	(V) Bytes Sent (V) Bytes Received
ET-ut User Authentication	(ii) Packets trent (iii) Packets Received
Count User Catabases Count User Catabases Count User Catabases Counting Service Counting Service Counting Service Counting Service	Enable reporting of the number of seconds the session lasted

9. Create a account for RADIUS in windows 2008.



10. Check the RADIUS port in NPS, first.

Network Policy Server			
File Action View Help			
Image: Second Servers Image: Second Servers	General Policy Server	(Local) Properties	×
Remote RADIUS Server G Policies Network Access Protection	Authentication:	1812,1645	
Accounting		Authentication default ports 1812,1645	
	Accounting:	1813,1646	
	Accounting default ports 1813,1646 If you do not use the RADIUS default port numbers, you must configure exceptions on the firewall for the local computer to allow RADIUS traffic on the new ports. Learn more. You can configure NPS to monitor IPv4 RADIUS traffic, IPv6 RADIUS traffic, or both on specific network adapters. Learn more.		
	5	OK Cancel Apply	

11. Setup the NPS Client.

Network Policy Server	L2TP-Radius Properties	Lov
File Action View Help Image: Stress of the s	Settings Image: Carlos Properties Settings Image: Carlos Properties L2TP-Radius Carlos Ca	J r network.
<u>× </u>	OK Cancel Apply	

12. Setup RADIUS policy.

S. Network Policy Server	LATE-policy properties	-	
File Action View Help	Overview Conditions Constraints Settings		
🧆 🔿 🛛 🖾 📖	Policy name: L2TP-policy		
RADIUS Clients and Servers RADIUS Clients RADIUS Clients RADIUS Clients RADIUS Server G Policies Policies	Policy State If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.		
Network Policies	Access Permission If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access, <u>What is access permission?</u>		
	Grant access. Grant access if the connection request matches this policy.		
	C Deny access. Deny access if the connection request matches this policy.		
	Ignore user account dial-in properties. If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts		
	Network connection method Select the type of network access server that sends the connection request to NP5. You can select either the network access server type or Vendor specific. Type of network access server: Unspecified		
	Vendor specific:		
	UK Cancel Appy	21	



End of Document.