VPN L2TP

IP Pool

Выделим всех клиентов, подключаемых по VPN в отдельный пул адресов. Так проще будет настроить маршрутизацию и правила межсетевого экрана, при необходимости.



РРР профиль настройки

Перейдём на вкладку Profiles и добавим новый профиль. Зададим имя для удобства. Не мудрствуя лукаво, я просто оставил L2TP. А также указал локальный и удалённый адреса из нашего пула (по счастливой случайности он так же называется L2TP).

-			
👯 Bridge			
The second secon			
T <mark>o Mes</mark> h			
IP N			
MPLS N			
Routing			
🔯 System 🗈 🗈		New PPP Profile	
👰 Queues			
Files		General Protocols Limits Queue Scripts	OK
Log		Name: L2TP	Cancel
RADIUS		Local Address: L2TP 🛛 🐺 🔺	Apply
🔀 Tools 💦 🕅	Interface PPPoE Servers Secrets Profiles Active Connections L2TP S	Remote Address: L2TP	
New Terminal	• - 6 7		Comment
Dot1X	Name / Local Address Remote Address Bridge Rate Limit	Bridge:	Сору
🖲 Dude 🗈 🏌	efault	Bridge Port Priority:	Remove
Make Supout.rif	default-encr	Bridge Path Cost:	Tioniovo
Manual		Bridge Horizon:	
New WinBox			
Kit Exit		Incoming Filter:	
		Outgoing Filter:	
		Address List:	
		Interface List:	
		DNS Senior	
		WINS Server:	
		- Change TCP MSS	
1	2 iteme	C no 🔶 yes C default	
1	2 10110	- Use UPnP	
		C no C yes 🧿 default	

Я также отметил возможность изменять максимальный размер сегмента TCP (опция Change TCP MSS). Есть подозрение, что это поможет избежать фрагментацию сегментов.

Секреты

Под секретом в данном случае понимаются учётки VPN-юзеров. Заходим также в раздел PPP, на вкладку Secrets и под каждого пользователя создаём свой секрет. В качестве сервиса выбираем **l2tp**, а в качестве профиля — созданный на шаге № 2 профиль PPP.

and blidge								
The second secon								
°T <mark>°</mark> Mesh								
5 IP 🗈 🗅								
MPLS N								
对 Routing								
🔯 System 🗈 🗈								
🙅 Queues								
📔 Files								
Log	ppp							
2 RADIUS						1		
🔀 Tools 🛛 🕅	Interface PPPoE Servers	s Secrets	Profiles Activ	ve Connections	L2TP Secrets			
🗖 New Terminal	+ * * -	T PPP	⁹ Authentication	&Accounting				
🔅 Dot1X	Name / Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged	Out
🕲 Dude 🛛 🗅	🔞 user1_p *****	pptp		default	192.168.1.23	1 10.10.88.111	Apr/03/2	021 20:07:43
Make Supout.rif				N	ew PPP Secret			
Manual						4.15		
🕥 New WinBox					Name:	user (_IZtp		ок
🚮 Exit					Password:	•	^	Cancel
					Service:	l2tp	Ŧ	Apply
					Caller ID:		•	
					Profile:	L2TP	Ŧ	Disable
				1				Comment
					Local Address:			Сору
				F	Remote Address:		•	Copy
				-	Routes:		•	Remove
	1 item				Lan David			
	Invent				Limit Bytes In:			
					Limit Bytes Out:		•	
				L	ast Logged Out:			

Сервер L2TP

Здесь просто убедимся, что у нас запущены соответствующие сервисы. Заходим в L2TP Server и убеждаемся в наличии соответствующих настроек:



Нужно указать ключ в поле IPsec Secret.

Файрволл

На сетевом экране *IP – Firewall* необходимо открыть следующие порты (цепочка input – *входящий*): протокол udp, порты 500, 4500, 1701.

	Firewa														
UVireless	Filter	Rules	NAT	Mangle	Raw Servi	ce Ports	Connectio	ons Addres	s Lists	Laver7	Protocols				
Bridge					→										
			 × 		r CO Reset	Counters	CO Res	et All Counter	S						
Mesh	#	Act	ion	Chain	Src. Addres	s Dst. Ad	ddress Pro	oto Src. Po	rt D	st. Port	In. Inter	Out. Inf	In. Inter	. Out. Int	t \$
9 P	0	pptp	acc	input			6.6	tcn)	1	723					
MPLS N	1	-	acc	input			47	(g							
Routing	2 >	X 🛷	acc	forward			Firewall Ru	le <500.1701	.4500>						
System 🗅	37	X 🛷	acc	torward	Real Providence		Gammel		= .			I I			1
Queues			000	mper			General	Advanced	Extra	Action	Statistics	3	ОК		
Files								Chain	input			Ŧ	Cance	el	
Log	PF							Src. Address				- Ī	Apply	,	
RADIUS	1							Dst Address				↓ ↓ ↓	. ++-3		
🗙 Tools 🛛 🗅									0			_ [Disabl	e	
New Terminal								Protocol	6	(tcp)	Ŧ	▲ [Comme	ent	
Dot1X								Src. Port				▼ ¹	C		
🕲 Dude 🛛 🗅								Dst. Port	5	00,1701,4	4500		Сору		
Make Supout.rif	_							Any Port				. I	Remov	/e	
Manual	5 item	is (1 sel	ected)					1 1					Reset Cou	Inters	
🕥 New WinBox								In. Interface	-			Ĭ	Ponet All Co	untorn	
Kit Exit							C)ut. Interface				• L	neset Air Ct	Juniters	2
							ln.	Interface List				-			
							Out.	Interface List				-			
							-	Packet Mark				•			
							Con	nection Mark				-			
							F	Routing Mark	_			_			
							R	louting Table				-			
	2 items	1 ite	m (1 sel	lected)			Conr	nection Type				-			
		1					Corre	nection State				-			
							Conr	iection state							
							Connectio	n NAT State				•			

Groups

```
Добавим свою групу в IP - IPSec - Groups:
```

Log	DDD	IPeac									
P RADIUS		II Sec									
K Tools	Interface	Policies	Proposals	Groups	Peers	Identities	Profiles	Active Peers	Mode Configs	Installed SAs	Keys
New Terminal	+ -	+ -	7								
Dot1X	Name	Name		1							
🕽 Dude 🛛 🗅	🔒 user1	* default							IR-second	12-1	ſ
Make Supout.rif	😝 user1	l2tp							Psec Group	i <i∠ip></i∠ip>	<u>1</u>
Manual									Name: 12tp		OK
New WinBox											Cancel
🚰 Exit											Applu
											Сору
											Remove