Инструкция по настройке VPN-соединения между модемом OnCell G3110 и маршрутизатором EDR-G903

Оборудование.

- 1. Маршрутизатор EDR-G903
- 2. Модем OnCellG3110
- 3. 2 компьютера

Топология сети





С одной стороны имеем модем OnCell G3110, имеющий выход в интернет через Floating IP, выделяемый провайдером. Модем является шлюзом для сети 192.168.127.Х и имеет в этой сети IP-адрес 192.168.127.254. С другой стороны – маршрутизатор, имеющий выход в интернет через статический IP-адрес, выделенный провайдером (в рассматриваемом примере – 87.245.206.198). Маршрутизатор является шлюзом для сети 192.168.126.Х и имеет в этой сети IP-адрес 192.168.126.254. Модем является VPN-клиентом, а коммутатор VPN-сервером. Обратите внимание, что при настройке тоннеля VPN по протоколу IPSec, необходимо, чтобы локальные сети с одной и с другой стороны не пересекались!

Настройка VPN-сервера.

- 1. С помощью браузера откройте WEB-интерфейс коммутатора EDR-G903.
- 2. В пункте меню Network/Interface/WAN1 укажите конфигурацию, выданную провайдером (статический IP-адрес, маску подсети, шлюз и DNS-сервер). Нажмите кнопку Activate.

	•WAN1 Configuration	
Main Menu		
- Overview	Connection	
Device Overview		
- Basic Setting	Connect Mode O Disable 💿 Enable	
- Network	Connect Type Static IP 👻	
Mode Configuration		
- Interface	Address Information	
WAN 1	IP Address 87.245.206.198	Gateway 87.245.206.193
WAN 2/DMZ	Subnet Mask 255.255.255.240	
LAN		
DHCP Server	PPTP Dialup	
DHCP List	PPTP Connection Enable	IP Address 0.0.0.0
Dynamic DNS		
802.1Q VLAN Setting	User Name	Password
- Communication Redundancy		
- Network Redundancy	DNS (Optional for dynamic IP or PPPol	E Type)
- Routing	Server 1 Se	erver 2 Server 3
- NAT	87.245.206.131 8.	8.8.8 0.0.0.0
- Firewall Policy		
- VPN		á ctivate
- IPSec		Attivate
	Рис. 2	

•

3. В пункте меню Network/Interface/LAN укажите конфигурацию порта LAN в локальной сети. Нажмите кнопку Activate.

	LAN Configuration
Main Menu	
- Overview	LAN IR Configuration
Device Overview	IR Address
- Basic Setting	
- Network	192.168.126.254 (ex. 192.168.1.1)
Mode Configuration	Subnet Mask
- Interface	255.255.255.0 (ex. 255.255.255.0)
WAN 1	
WAN 2/DMZ	
LAN	Activate
DHCP Server	
	Рис. 3

4. Настройте правило NAT в пункте меню NAT/NAT Setting, как показано на рисунке 4. В поле LAN IP Range укажите диапазон IP-адресов локальной сети, для которых будет действовать данное правило NAT. Нажмите кнопку New/Insert и Activate.

	^	• Ne	two	rk Ado	dress Tra	anslation				
Main Menu										
- Overview										
Device Overview		Enable		\checkmark		LANUE Dongo	1021691261	102 169 126 1	150	
- Basic Setting		NAT Mod	e	N-1	*	DAN IF IXalige	132.100.120.1	132.100.120.2	.52	
- Network		Interface		Auto	*	WAN IP	87.245.206.198			
Mode Configuration										
- Interface										
WAN 1	=									
WAN 2/DMZ		New/Ins	ert	Move	Delete	Modify				
LAN		NAT Lis	t (1	/128)						
DHCP Server		Enoble	Indox	15	Protocol		Course IP	Source	Dectination IP	Destination
DHCP List		Chaple	Index	11	FIOLOUUI		Source IP	Port	Desunation IP	Port
Dynamic DNS		~	1	Auto		192.168.1	26.1~192.168.126.252		87.245.206.198	
802.1Q VLAN Setting										
- Communication Redundancy										
- Network Redundancy										
- Routing										
- NAT										
NAT Setting										
- Firewall Policy										
- VPN		Activate								
						D 4				

- Рис. 4
- 5. Включите VPN-сервер в пункте меню VPN/IPSec/Global Settings. Там же включите функцию IPSec NAT-T Enable, нажмите кнопку Activate.

	<u>^</u>	IPSec Globa	l Setting
Main Menu			
- Overview			
Device Overview		All IPSec Connection	Enable 🚩
- Basic Setting		IPSec NAT-T Enable	\checkmark
- Network		Activate	
Mode Configuration			
- Interface			
		Рис. 5	

6. Задайте настройки VPN-тоннеля. В пункте меню VPN/IPSec/IPSec Setting задайте настройки, как показано на рисунках 6 и 7. Адреса локальной и удалённой сети укажите свои (в примере - 192.168.126.0 и 192.168.127.0 соответственно).

	IPSec Settin	ng				
Main Menu						
- Overview	Setting		A 44444 4 0			
Device Overview	Setting	U QUICK Setting	Advanced S	eming		
- Basic Setting	Tunnel Setting					
- Network	Enable 🗹 Name	Test (Must	L2TP tunnel			
Mode Configuration		begin with an alphabet)				
- Interface	VPN Connection Type	Site to Site(Any) 🚩	Remote VPN Ga	iteway 0.0.0.0		
WAN 1	Connect Interface	WAN1 🔽	Startup Mode	Wait for connectir	ng 🗸	
WAN 2/DMZ						
LAN	Local Network	192.168.126.0	Netmask	255.255.255.0	ID	
DHCP Server	Remote Network	192.168.127.0	Netmask	255.255.255.0	ID	user1@moxa.com
DHCP List	Key Exchange (Phas	e 1)				
Dynamic DNS	IKE Mode	Aggressive V				
802.1Q VLAN Setting						
- Communication Redundancy	Authentication Mode	Pre-shared Key 🚩	12345678			
		Рис	6			

В поле Pre-Shared Key укажите секретный ключ, с помощью которого устройства будут получать доступ к VPN-серверу. Для безопасности ваших данных, выберете как можно более сложный ключ. В ключ примере – 12345678 – не является безопасным.

	• IPSec Settir	ng			
Main Menu					
- Overview	Develop Material	100 100 107 0	N-A	0.55.055.055.0	
Device Overview	Remote Network	192.168.127.0	Netmask	255.255.255.0	ID user1@moxa.com
- Basic Setting	Key Exchange (Phase	e 1)			
- Network	IKE Mode	Aggressive 🔽			
Mode Configuration	Authentication Mode	Pre-shared Kev 🔽	12345678		
- Interface					
WAN 1	Encryption Algorithm	3DES 🚩	Hash Algorithm	SHA1	×
WAN 2/DMZ	DH Group	DH 2 (modp1024) 🛛 👻			
LAN	Negotiation Times	0 (0:forever)	IKE Life Time	1	hour.
DHCP Server	Dokou Evniro Timo	0. min	Dokou Euro Domo	unt 100	~
DHCP List	Rekey Expire Time	9 mm.	Rekey ruzz reite	100	70
Dynamic DNS	Data Exchange (Phas	e 2)			
802.1Q VLAN Setting	Perfect Forward Secrecy	✓	SA Life Time	30	min.
- Communication Redundancy	Encryption Algorithm	3DES 🗸	Hash Algorithm	SHA1	*
- Network Redundancy 📃	Dead Peer Detection				
- Routing	Dead Feel Detection				
- NAT	Action Hold N	Delay	30 seconds	I Imeout 1	20 seconds
NAT Setting	Add Delete	Modify Activat	te		
- Firewall Policy					
VDN	IPSec Connection	(1/100)			
	Рис. /				

Далее нажмите кнопки Add и Activate. Настройка VPN-сервера закончена.

Настройка VPN-клиента.

- 1. С помощью браузера откройте WEB-интерфейс модема OnCell G3110.
- 2. В пункте меню Network Settings/Basic Network Settings укажите конфигурацию интерфейса LAN. Нажмите кнопку Submit.

🔁 Main Menu	Basic Network Settings				
🗀 Overview	Sasto Hottion oottings				
💼 Basic Settings	IP configuration	Static 💌			
🖻 🔂 Network Settings	IP address	192.168.127.254			
👘 💼 Basic Network Settings	Notwork				
DNS Settings	Neumask	255.255.255.0			
📄 💼 Advanced Network Set	Gateway				
📄 💼 Auto IP Report Setting:	WINS function	💿 Enable 🛛 Disable			
💼 GSM GPRS Settings	WINS server				
💼 GuaranLink Settings	LAN speed	Auto 💌			
🕴 🗎 🔲 OnCell Central Manage					
- VPN Settings	DHCP Server Configuration				
🗉 🧰 Serial Port Settings	DHCP server	🔘 Enable 💿 Disable			
🖣 🧰 System Management 👘					
🖻 🧰 System Monitoring	Submit				
💼 Save Configuration					
🗄 🧰 Restart					

Рис. 8

3. В пункте меню Network Settings/GSM GPRS Settings выберите тип соединения GPRS. Точку доступа APN уточните у оператора мобильной связи (в примере – internet). Нажмите кнопку Submit.

Main Menu	GSM GPRS Settings	
Basic Settings	Туре	⊙ gsm ⊙ gprs ○ sms ○ virtual MODEM
🖣 🔁 Network Settings	SIM PIN	••••
Basic Network Settings	Band	Auto
DNS Settings		
🗀 Advanced Network Set	GPRS	
🗀 Auto IP Report Setting:	TCP/IP Compression	🛇 Enable 💿 Disable
💼 GSM GPRS Settings	Inactivity time	0 (0 - 65535 ms)
GuaranLink Settings	Link quality report	O Enable O Disable
🖳 🖻 🧰 OnCell Central Manage	PPP Config	O Enable O Disable
- VPN Settings	ATD	*99***1# (Default: *99***1#)
🗎 🧰 Serial Port Settings		
🖲 🔲 System Management	PPP Authentication	Auto
🖲 🔲 System Monitoring	Username	
Save Configuration	Password	
⊡ Restart	APN	internet
	Connection control	Always On/None
	Connection interval	5 (5 - 65535 min)
	Ping remote host	Ping Test
	Submit	

Рис. 9

4. Проверьте соединение с сетью Internet с помощью команды Ping. Например, проверьте доступность маршрутизатора по его внешнему IP-адресу. В рассматриваемом примере – 87.245.206.198.

C:\WINDOWS\system32\cmd.exe	- 🗆 ×	
Microsoft Windows XP [Версия 5.1.2600] (С) Корпорация Майкрософт, 1985—2001.	^]
C:\Documents and Settings\a.soluyanov>ping 87.245.206.198		1
Обмен пакетами с 87.245.206.198 по 32 баи́т:		
Ответ от 87.245.206.198: число байт=32 время=531мс TTL=47 Ответ от 87.245.206.198: число байт=32 время=587мс TTL=47 Ответ от 87.245.206.198: число байт=32 время=570мс TTL=47 Ответ от 87.245.206.198: число байт=32 время=529мс TTL=47		
Статистика Ping для 87.245.206.198: Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь), Приблизительное время приема-передачи в мс: Минимальное = 529мсек, Максимальное = 587 мсек, Среднее = 554 мсек		
C:\Documents and Settings\a.soluyanov>_		
	-	1
D 10		_

- Рис. 10
- 5. В пункте меню Network Settings/VPN Settings укажите настройки VPN-клиента, как показано на рисунках 11 и 12.

Main Menu	VPN Settings				
Basic Settings	Configuration				
🖻 🔁 Network Settings	VPN tunnel	● Enable ○ Disable			
Basic Network Settings	VPN tunnel mode	ISAKMP/PSK			
DNS Settings	Remote Network				
Auto IP Report Setting:	Remote endpoint IP or hostname	87.245.206.198			
GSM GPRS Settings	Remote subnet IP	192.168.126.0			
📹 GuaranLink Settings	Remote subnet netmask	255.255.255.0			
OnCell Central Manage	Local Network				
VPN Settings Serial Port Settings	Local subnet IP	192.168.127.0			
System Management	Local subnet netmask	255.255.255.0			
🖲 📄 System Monitoring	ISAKMP (Key Management)				
Save Configuration	Pre-shared key (PSK)	12345678			
En Restart	Perfect forward secrecy (PFS)	⊙ Enable ○ Disable			
	Local Identity				
	Identity option	User FQDN 💌			
	IP/FQDN/User_FQDN	user1@moxa.com			
	ISAKMP Phase 1				
	Operation mode	Aggressive 💌			
	NAT traversal (NAT-T)	⊙ Enable			
	Encryption mode	3DES 💌			
Рис. 11					

В полях Remote subnet IP и Local subnet IP укажите адреса ваших удалённой и локальной сетей соответственно. Значения полей Pre-shared key (PSK) и IP/FQDN/User_FQDN должны совпадать с теми значениями, которые были указаны в настройках VPN-сервера.

GSM GPRS Settings	Local Identity		
GuaranLink Settings	Identity option	User FQDN 💌	
🖲 🧰 OnCell Central Manage	IP/FQDN/User_FQDN	user1@moxa.com	
VPN Settings	ISAKMP Phase 1		
Serial Port Settings System Management	Operation mode	Aggressive 💌	
Tanagement	NAT traversal (NAT-T)	⊙ Enable ○ Disable	
Save Configuration	Encryption mode	3DES 💌	
🗉 🧰 Restart	Authentication mode	SHA-1 💌	
	Diffie-Hellman group	Group 2-1024bits 💌	
	SA lifetime	3600 (600 - 864000 secs) 🗇 🗍 7-90	
	ISAKMP Phase 2		
	Encryption mode	3DES 💌	
	Authentication mode	SHA-1 💌	
	Diffie-Hellman group	Group 2-1024bits 💌	
	SA lifetime	1800 (600 - 864000 secs) ~ 30 MUH	
	Advanced Settings		
	Anti-replay	◯ Enable 💿 Disable	
	Dead peer detection (DPD)	💿 Enable 🛛 Disable	
	Submit		
javascript:clickOnFolder(48)	1 Submet		

Рис. 12

Обратите внимание на то, что значения параметров SA lifetime Phase 1 и SA lifetime Phase 2 указываются в секундах. В настройках VPN-сервера параметр SA lifetime Phase 1 соответствует параметру IKE Lifetime и указывается в часах (в примере – 1 час), см рис 7; параметр SA lifetime Phase 2 имеет то же название, но указывается в минутах (в примере – 30 минут), см. рис. 7. Значения соответствующих параметров должны совпадать, не забудьте произвести пересчёт величин!!!

Нажмите кнопку Submit. Настройка VPN-клиента завершена.

Результат.

Для проверки правильности настройки перейдите в пункт меню System Monitoring/System Status/System Log. В поле System Log при корректной настройке

всех параметров должно появиться сообщение о том, что фазы 1 и 2 создания тоннеля VPN завершены.

		Super menion	
		Auto TP Report Setti	
	- 🗀	GSM GPRS Settings	System Log
	🗀	GuaranLink Settings	
		OnCell Central Mana	System Log
		Oncell Central Marie	2000/01/08 00:42:22 [Network] VBN phase2 renew key
	····	VPN Settings	2000/01/08 00:42:22 [Network] VPN phase2 renew key success
E	9 🚞 S	erial Port Settings	2000/01/08 01:04:55 [Network] VPN phase2 renew key
Ē	- -	vstem Management	2000/01/08 U1:04:56 [Network] VPN phase2 renew key success
			2000/01/08 01:20:21 [Network] VPN start phase1 aggr. mode connect
	E. 🗖	MISC. Network Settir	2000/01/08 01:20:22 [Network] VPN start end yption
	֥	Auto Warning Settin	2000/01/08 01:20:23 [Network] VPN phase2 pass
		Maintenance	2000/01/08 01:42:54 [Network] VPN phase2 renew key
			2000/01/08 01:42:56 [Network] VPN phase2 renew key success
		Console Settings	2000/01/08 02:05:27 [Network] VPN phase2 renew key
		🗎 Pina 🚽	2000/01/08 02:05:29 [Network] VPN phase2 renew key success
			2000/01/08 02:20:54 [Network] VPN start phase1 aggr. mode connect
		🔲 Manuai SMS	2000/01/08 02:20:55 [Network] VPN share encryption
		🔲 Firmware Upgradi	2000/01/08 02:20:35 [Network] VPN phase1 pass
		Configuration Imr	2000/01/08 02:22:3/ [Network] VM priast Link Down
		Configuration Inf	2000/01/08 02:43:28 [Network] VPN nhase2 renew key
		Configuration Exp	2000/01/08 02:43:30 [Network] VPN phase2 renew key success
		🗎 Load Factory Defa	
		📄 Change Password	
		📄 Remote SMS Cont	Select all Clear log Refresh
	÷.	Certificate	

Аналогично в WEB-интерфейсе маршрутизатора EDR-G903 можно увидеть статус VPN-тоннеля. Выберите пункт меню VPN/IPSec/IPSec Status. При корректной настройке все параметров IPSec Connection List будет выглядеть следующим образом:



Для проверки доступности сетей на противоположный концах VPN-тоннеля используйте команду Ping.