

Iàñòðîéêà VPN Ñåðâåðà-øëþçà íà OpenSuse 11.2.

Đàçääë : Nèñòåìà. Àäìèíèñòðèðîâàìèå

Íþóáéèëâàïí [DrStrip](#) [24/06/2010]

Íèñàë ñòàòùþ iðî óñòàíîâéó ðàçëè÷íûõ ÔÂ-òþíåðîâ, íî òóò ñâàéèëàñü ñðî-íàÿ ðàáîòà, â ïäííé íåâàéëøíé êíñíàíèé íøæíî áúëî íðîââñòè ÈÓ-àóäèò, è íàñòðîèòü äíñòóï óääàéåíûõ iëèùàäâî â áíóòðåííþþ ñâðöü êíñíàíèé. Òàè âíåñòî, "iðî òþíåðû" iíøó-èëàñü ñòàòöý "iðî VPN".

Íà øëþç, ñ äâóïÿ ñâðâåûìè êàðòî-êàìè, áúë óñòàíîâéáí OpenSuse 11.2, áåç X-Windows. Ñ íðîâàéåäåðíí áúëî íàñòðîâíí ñíâæëíàíèå PPPoE, ÷åðâç ïæí èç èíøåðôåéñîâ, ñ iíñíùþþ YAST. Èíðåðîâò íà øëþçå iíÿâèñÿ. Òàïåðü íøæíî, ðàçääàðü èíðåðíåò â áíóòðåííþþ ñâðöü è íàñòðîèòü iíäéëþ-âíèå íí VPN áíåðíèö iíñíùàäâî ñ M\$ Windows, ÷åñòü èç êíøåðûõ èñíñíëüçóþò Yota.

Íþðåðâà ÷òî ý óñòàíîâéë ýòî áúë mc (Íñòàëüâèÿ ií Norton Commander)

sudo zypper install mc

Â èà-âñòåâ ñâðâåðà VPN, ý ðåøèë èñíñíëüçîâàðü pptpd, ðîòÿ iíæíî áúëî èñíñíëüçîâàðü è openvpn.

Óñòàíâåéèëâàì pptpd

sudo zypper install pptpd

Íàñòðàéâåàì ôàéë êíñíðåéóðàöè /etc/pptpd.conf

ß iñòàéë åäí ií-òè, áåç èçìåíâéé çà èñéëþ-âíèàì äâóô ñòðîâ

localip 192.168.110.1

Ýòî IP êíòîðûé èñíñíëüçóåò ñàì ñâðâåð VPN iðè ñíâæëíàíèë ñ êéèåíòî.

remoteip 192.168.110.100-110

Ýòî àéàéàçíí IP áûäàåðòñÿ êéèåíòà iðè iíäéëþ-âíèë.

Íñæíî áûäàåâàðü àäðåñà è èç áíóòðåíâé êíèàéüíé ñâðöè (è èñíñíëüçîâàðü iàðàìåð proxyarp), íî ý ýòî íå áâéëå ñíâöèàëüíí, òàê èâé åñòóï íøæáí áúë ê êííéðåòííó ñâðâåðó, à íå ê áñåé áíóòðåíâé êíèàéüíé ñâðöè.

â ôàéëå /etc/pptpd.conf åñòü áùå ïæí iàðàìåð.

option /etc/ppp/options.ppp0

Ýòî iàðàìåð ÿðàéçûâååò íà ôàéë, êíñíðåéóðàöèè PPP. Iðè-âàì ií óñíè-àíèþ, iðè óñòàíîâéå iàéåòà, íí íå ñíçäååðòñÿ è çàïóñé åâííà iðèåâåååò ê ïðèåéå.

Â ýòî ôàéëå áîñíàùå íáíííà iàðàìåðâíà è íèì åñòü êíñíàíòàöèè. Cíçääåì ôàéë /etc/ppp/options.ppp0, ý íå ñòàë, çàïðà-âéâàòüñÿ è iðîñòî ñêíñíèðîâé, óæå ñóùåñòâóþùèé /etc/ppp/options.pptp (òàê èâé ó iàíÿ ñòîýé óæå PPTP Client) iíä èíåíâí /etc/ppp/options.ppp0 è iòðåäàéòèðîâé åâí.

Lock the port

lock

auth

Âéëþ-âåì àâòoðèçàöèþ

name pptpd

Èìÿ ñâðâåðà VPN

refuse-pap

refuse-mschap

refuse-eap

#Îòéëþ-âåì âñå íðîòîéíëû êðîâà chap

nobsdcomp

```

nodeflate
mtu 1400
mru 1400
#Âûñòàâëÿì MTU
lcp-echo-failure 5
lcp-echo-interval 30
Îòêðûâàâàì ôàéé /etc/ppp/chap-secrets è ïðïïèñûâàâì ëíâèíû è íàðîëè íàïðèìåð
vasya pptpd pA$$word "*"
# login password IP

```

Âìâñòî "*" , ïïðíïèñàòü äëÿ êàæäíàì êëèåíòà IP èç íóëà àäðåñâà ïðïïèñàííàì â /etc/pptpd.conf. Íî áóäüöà ïñóïðîæíû, åñèè åû äïñõòèì ïðïïèñàëè àäðåñ 192.168.110.100 äëÿ vasya, à ýóïò àäðåñ áûë áûäàí óæå äëÿ äðóäíàì êíííâèòà, òî ïðè ïäéëþ÷åíè vasya, ïðåäûäóùåé ïïëüçîâàòåëü áóäåò ïòéëþ÷åí.

Âñâ íàñòðàèâàâì çàïóñêàâì äâàíí

/etc/init.d/pptpd start

Íàñòðàèâàâì VPN ñîâääíáíèå â M\$ Windows

Íà áééàäéå "Áåçïïàññòú" áûáèðàâì "Ãïïïèñòåëüíí" è óêàçûâàâì ñëåäóþùèå íàðàìåòðû:

Øôðôïâàíèå - "íåíáýçàòåëüíí"

Îòéëþ÷åíàì áñâ ïðïòîéëü è áééëþ÷åíàì CHAP ñîâääíÿâìñý è ïðïâåðÿâì êíííâèò, ñ êëèåíòà äíéæåí ïèíäíàòöñý 192.168.110.1..

Çääñü ý ñääëëàþ íàëåíüêà ïðèìå÷åíèå íà ñ÷åò Yota.

Ðåêîíåíâàííûé MTU äëÿ Mobile WiMAX=1386, ðåðíè÷åñêàÿ ïäéëåðæêà Yota ñêàçàëà, ÷òî íàäí óñòàííâèòü MTU=1372. Â íàùâàì áñèè, íñòàâèòü MTU ïî óïè÷åíèþ äëÿ PPTP â M\$ Windows, òî ñîâääíáíèå íàñòàáëëüíà, íaiðèìåð ïïñòòéà ïäéëþ÷åíèÿ ï RDP, ïðèâåðæäà è ðàçðûâó VPN. ß íå ñòàë áûñ÷èòûâàòü òî÷íà çíà÷åíèå MTU (áûë óæå áå÷åð ñóáàíòû) , à óñòàííâèë äëÿ ïðïòîéëà

MTU=1400, à äëÿ ñîâääíáíèë VPN MTU=1350. Âñâ çàðàáòàëî. Âñëè íå çíàåðå èàê ïïàíýòü MTU èääì ï [ññûëéå](#) ÷èòàâì è íáíÿâì.

Âñëè ó áàñ WIN7 (ñ ïðàâàìèå àäíèíà)

netsh interface ipv4 set subinterface "íàçâàíèå ïäéëþ÷åíèÿ" mtu=xxxx store=persistent

Íó áîò, òåïåðü íàðåñîäèì è íàñòðîéêå Firewall, íàïïèíàþ, ÷òî íóæíí ïáâñïå÷èòü ðàçäà÷ó èíòåðíåòà íà ïòéñ è íáâñïå÷èòü áññòóï ïäéëþ÷åííû ï VPN êëèåíòâà ê íàïíò èç ñåðâåðíà â êíèåëüíé ñåòè íòéñà.

Íàñòðîéêè õðàíÿòñý â óàééå /etc/sysconfig/SuSEfirewall2, ïðèâåäó è ïïèøó òå çíà÷åíèÿ èíòîðûâ íóæíû äëÿ íáâñïå÷åíèÿ ðàâîòû VPN è ðàçàä÷è èíòåðíåòà.

FW_DEV_EXT="any dsl0 eth0"
FW_DEV_INT="eth1"

#Íàçíà÷åí èíòåðôåñû
FW_ROUTE="yes"
FW_MASQUERADE="yes"

#Âéëþ÷åâì ðîóòèíà è íàñêàðàäèíà
FW_MASQ_NETS="0/0"
#Ãàâàì íåñðàíè÷åíûé áññòóï â èíòåðíåò èç áíóòðåíâé ñåòè
FW_SERVICES_EXT_TCP="1723"

```
#Îòêðûâàåì ïîðò äëÿ VPN  
FW_SERVICES_EXT_IP="47"  
#Îòêðûâàåì ïðîñêîë GRE=47  
FW_FORWARD="192.168.110.0/24,192.168.10.3 192.168.10.3,192.168.110.0/24"  
#Îòêðûâàåì äîñòóï íà ñâðâåð 192.168.10.3 èç íàøåé ñâòè VPN 192.168.110.0/24
```

Ío áîò è áñâ, VPN ðàáîòàâò, èíòåðíåò ðàçäàâòñÿ, à äàëüíâéøåì íà ñâðâåð áûë óñòàííâåí Squid2 â ðåæèìå "ïðîçðà÷íâî" ïðîñêè è lightsquid, íî ýòî òåìà óæå äëÿ äðóãîé ñòàòüè.

Âñåì óääà÷è!