

Настройка L2TP сервера на NetDefendOS

В Objects -> Address Book зададим адреса LAN и WAN сетей и их интерфейсов. У вас там будут какие-то свои значения. Также создадим два объекта типа IP4 Address с названиями: l2tp-serv_ip – в который пропишем ip адрес сервера L2TP и l2tp-ip_pool с пулом ip адресов, которые будут выдаваться подключающимся L2TP клиентам. Создадим еще один объект IP4 Address с названием dns-wins_serv – с ip адресом сервера во внутренней сети на котором работают DNS и WINS сервера.

Status

System

Objects

Network

Policies

▼ General

Address Book

Services

ALG

Key Ring

▼ Address Pool

IP Pools

NAT Pools

▼ VPN Objects

LDAP

IKE Config Mode Pool

IKE ID Lists

IKE Algorithms

IPsec Algorithms








InterfaceAddresses

An address folder can be used to group related address objects for better overview.

+ Add

Edit this object

Filter

# ▲	Name	Address	User Auth Groups	Comments
1	 wan1_ip	95.120.100.250		IPAddress of interface wan1
2	 wan1_net	95.120.100.0/30		The network on interface wan1
3	 lan1_ip	192.168.1.1		IPAddress of interface lan1
4	 lan1_net	192.168.1.0/24		The network on interface lan1
5	 l2tp-ip_pool	192.168.200.2-192.168.200.254		
6	 l2tp-serv_ip	192.168.200.1		
5	 dns-wins_serv	192.168.1.2		Server DNS & WINS

В Objects -> Key Ring создаем Pre-Shared Key (PSK) - ключ для проверки подлинности. В нем желательно использовать одни цифры – так при использовании других символов есть вероятность расхождения в кодировках.

Status

System

Objects

Network

Policies

▼ General

Address Book

Services

ALG

Key Ring

▼ Address Pool

IP Pools

NAT Pools

▼ VPN Objects

LDAP

IKE Config Mode Pool

IKE ID Lists

IKE Algorithms

IPsec Algorithms

l2tp-ipsec_key

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name:

Shared Secret

☒ Passphrase

Shared Secret: Note! Existing secret will always be shown with 8 characters to hide the actual length.

Confirm Secret:

i A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 v uses UTF-8.

☐ Hexadecimal key

Passphrase:

В Objects -> IKE Algorithms и IPsec Algorithms определяем необходимые алгоритмы шифрования.

StatusSystemObjectsNet

▼ General

Address Book

Services

ALG

Key Ring

▼ Address Pool

IP Pools

NAT Pools

▼ VPN Objects

LDAP

IKE Config Mode Pool

IKE ID Lists

IKE Algorithms

IPsec Algorithms

I2tp_3des

Configure algorithms which are used in the IKE phase o

Name:

I2tp_3des

Encryption Algorithms

	Preferred	Min	Max
<input type="checkbox"/> NULL			
<input type="checkbox"/> DES	56	56	56
<input checked="" type="checkbox"/> 3DES	192	192	192
<input type="checkbox"/> CAST128	128	128	128
<input type="checkbox"/> Blowfish	128	128	448
<input type="checkbox"/> Twofish	128	128	256
<input type="checkbox"/> AES (Rijndael)	128	128	256

Integrity Algorithms

☐ MD5

☒ SHA1

☐ SHA256

☐ SHA512

▼ General

Address Book

Services

ALG

Key Ring

▼ Address Pool

IP Pools

NAT Pools

▼ VPN Objects

LDAP

IKE Config Mode Pool

IKE ID Lists

IKE Algorithms

IPsec Algorithms

I2tp_3des

Configure algorithms which are used in the IPsec pha

Name:

I2tp_3des

Encryption Algorithms

	Preferred	Min	Max
<input type="checkbox"/> NULL			
<input type="checkbox"/> DES	56	56	56
<input checked="" type="checkbox"/> 3DES	192	192	192
<input type="checkbox"/> CAST128	128	128	128
<input type="checkbox"/> Blowfish	128	128	448
<input type="checkbox"/> Twofish	128	128	256
<input type="checkbox"/> AES (Rijndael)	128	128	256

Integrity Algorithms

☐ MD5

☒ SHA1

☐ SHA256

☐ SHA512

В Network -> Interfaces and VPN -> IPsec создаем IPsec туннель для L2TP.

StatusSystemObjectsNetwork

Interfaces and VPNRoutingNetwork Services

▼ Link Layer

Ethernet

VLAN

PPPoE

ARP/Neighbor Discovery

▼ VPN and Tunnels

IPsec

SSL

PPTP/L2TP Servers

L2TPv3 Servers

PPTP/L2TP Clients

L2TPv3 Clients

GRE

▼ Miscellaneous

Interface Groups

I2tp-ipsec-tunnel

An IPsec tunnel item is used to define IPsec endpoint and will appear

General

Authentication

Virtual Routing

XAuth

Name:

I2tp-ipsec-tunnel

Local Network:

wan1_ip

Remote Network:

all-nets

Remote Endpoint:

(None)

Encapsulation mode:

Transport

Local Gateway:

(None)

(Optional) S

IKE Config Mode Pool:

(None)

(Optional)

Algorithms

IKE Algorithms:

I2tp_3des

IKE Lifetime:

28800

seconds

IPsec Algorithms:

I2tp_3des

IPsec Lifetime:

3600

seconds

IPsec Lifetime:

0

kilobytes

Comments:

I2tp-ipsec-tunnel

An IPsec tunnel item is used to define IPsec endpoint and will appear

General

Authentication

Virtual Routing

XAuth

☐ X.509 Certificate

Root Certificate(s)

Available

Selected

HTTPSAdminCert

+ Include

x Remove

Gateway certificate:

Identification list:

(None)

☒ Pre-shared Key

Pre-shared key:

I2tp-ipsec_key

Selects the Pre-s

Local ID

Local ID Type:

Auto

Selects the type

Local ID Value:

Specify the local

Status System Objects **Network**

Interfaces and VPN Routing Network Services

l2tp-ipsec-tunnel

An IPsec tunnel item is used to define IPsec endpoint and will appear as a link layer.

General
Authentication
Virtual Routing
XAuth

In Virtual Router scenarios, it is often useful to specify which routing table to use to accomplish the segmentation.

- ☒ Make interface a member of all routing tables.
Traffic arriving on this interface will be routed according to the default routing table.
- ☐ Make interface a member of a specific routing table.
The route for the interface IP will only be inserted into the selected routing table.

Routing table:

main

Specifies the PBR table to use for all routing lookups, unless overridden by the Virtual Router.

i The routing table specified here may be overridden by Virtual Router, not routing for the tunnel itself.

Status System Objects **Network**

Interfaces and VPN Routing Network Services

▼ Link Layer

Ethernet

VLAN

PPPoE

ARP/Neighbor Discovery

▼ VPN and Tunnels

IPsec

SSL

PPTP/L2TP Servers

L2TPv3 Servers

PPTP/L2TP Clients

L2TPv3 Clients

GRE

▼ Miscellaneous

Interface Groups

Status

System

Objects

Network

Policies

Interfaces and VPN

Routing

Network Services

I2tp-ipsec-tunnel

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Authentication

Virtual Routing

XAuth

Routing

IKE Settings

Keep-alive

Advanced

☐ Allow DHCP over IPsec from single-host clients

☒ Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU:

IP Addresses

☒ Automatically pick the address of a local interface that corresponds to the local interface

☐ Specify address manually:

IP Address:

HA IP Address:

Specifies private originator IP for the tunnel

OK

Cancel

Status

System

Objects

Network

Policies

Interfaces and VPN

Routing

Network Services

I2tp-ipsec-tunnel

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General

Authentication

Virtual Routing

Routing

IKE Settings

Keep-alive

Advanced

IKE

☒ Main Mode

DH Group

☐ Aggressive Mode

Perfect Forward Secrecy

PFS

DH Group

Security Association

☒ Per Net

☐ Per Host

☐ Per Port

NAT Traversal

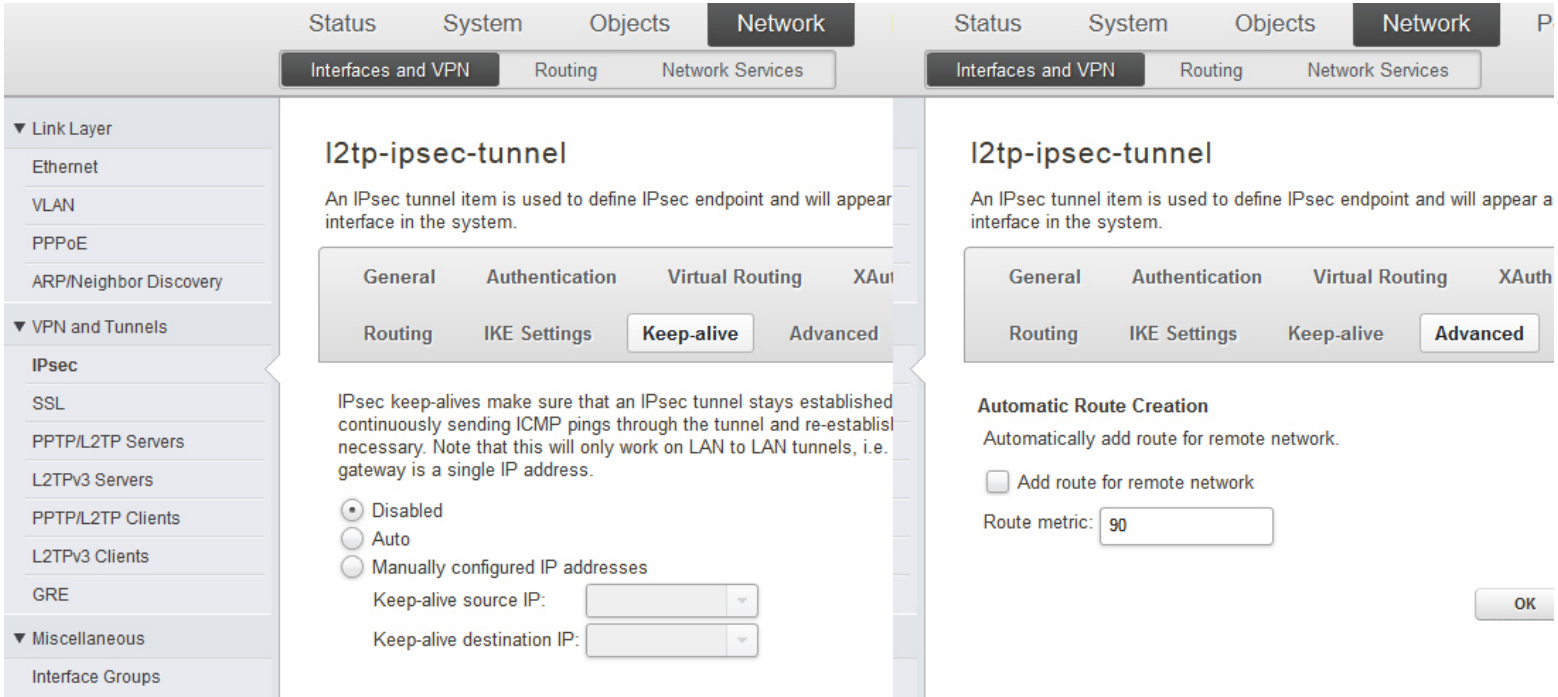
☐ Off

☒ On if supported and NATed

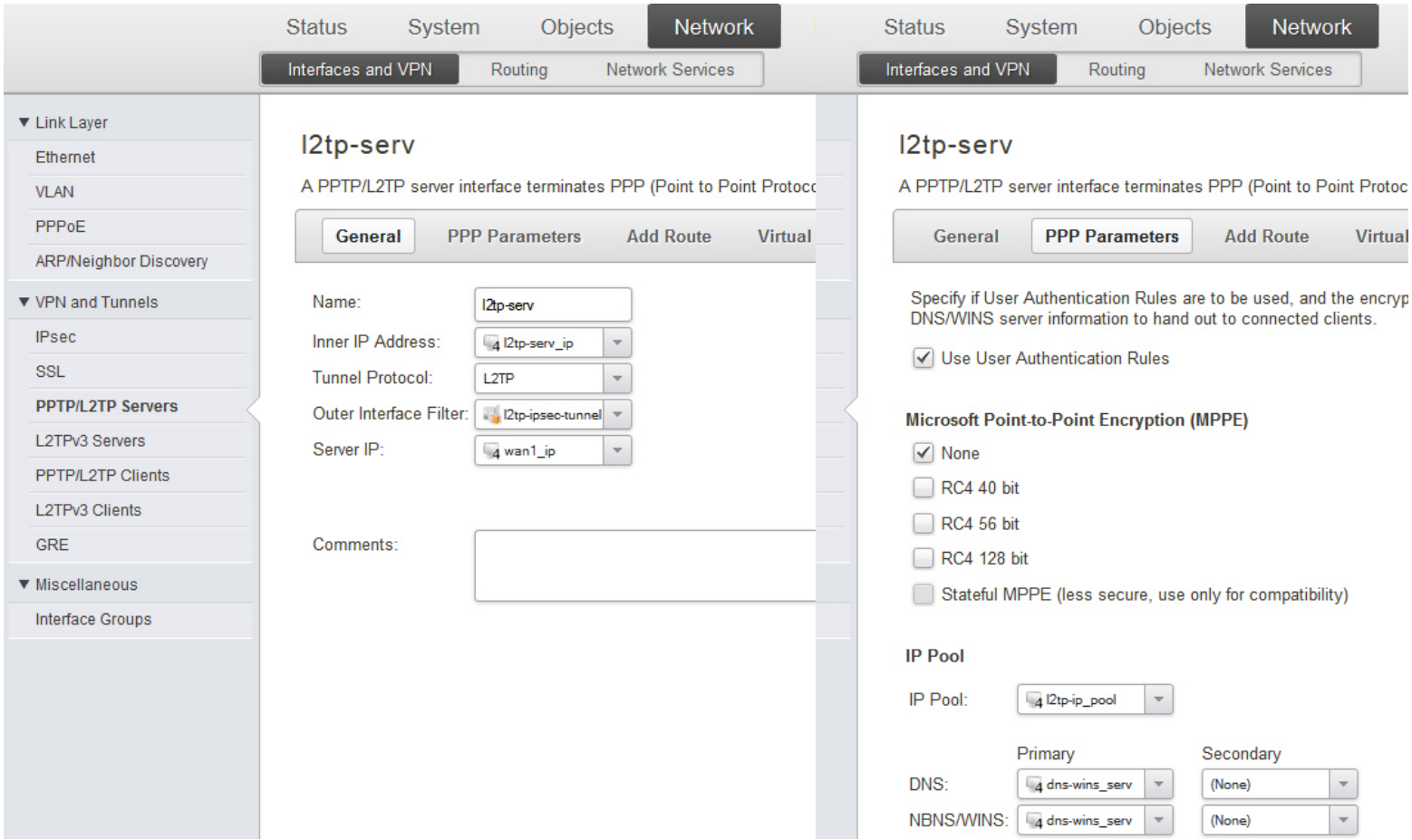
☐ On if supported

Dead Peer Detection

☒ Use Dead Peer Detection



В Networks -> Interfaces and VPN -> PPTP/L2TP Servers создаем L2TP сервер, к которому будет идти подключение. Если сервера WINS у вас нет – можно указать только DNS сервер. Если ни DNS ни WINS серверов во внутренней сети LAN у вас нет - можно в качестве dns-wins_serv использовать адрес бесплатного DNS сервера с адресом 8.8.8.8, но в этом случае имена компьютеров и сетевых устройств во внутренней сети будут видны только по ip, а не по именам, зато будет работать интернет. Сам L2TP не шифруем, так как ранее уже был зашифрован IPsec.



StatusSystemObjectsNetwork

Interfaces and VPNRoutingNetwork Services

▼ Link Layer

Ethernet

VLAN

PPPoE

ARP/Neighbor Discovery

▼ VPN and Tunnels

IPsec

SSL

PPTP/L2TP Servers

L2TPv3 Servers

PPTP/L2TP Clients

L2TPv3 Clients

GRE

▼ Miscellaneous

Interface Groups

I2tp-serv

A PPTP/L2TP server interface terminates PPP (Point to Point Prot

GeneralPPP ParametersAdd RouteVirtu

Filter

Restricts networks for which routes may automatically be added.

Allowed Networks:all-nets

Proxy ARP

Interface to ARP publish the added route on.

Proxy ARP interfaces

Available	Selected
dmz	lan1
lan2	
lan3	
wan1	
wan2	

+ Include

✕ Remove

☐ Always select ALL interfaces, including new ones.

StatusSystemObjectsNetwork

Interfaces and VPNRoutingNetwork Services

▼ Link Layer

Ethernet

VLAN

PPPoE

ARP/Neighbor Discovery

▼ VPN and Tunnels

IPsec

SSL

PPTP/L2TP Servers

L2TPv3 Servers

PPTP/L2TP Clients

L2TPv3 Clients

GRE

▼ Miscellaneous

Interface Groups

I2tp-serv

A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) t

GeneralPPP ParametersAdd RouteVirtual Ro

In Virtual Router scenarios, it is often useful to specify which routing tab

Routing Rules to accomplish the segmentation.

☒ Make interface a member of all routing tables.

Traffic arriving on this interface will be routed according to the main i

all routing tables.

☐ Make interface a member of a specific routing table.

The route for the interface IP will only be inserted into the selected r

Routing table:main

Specifies the PBR table to i

routing table will be used for

❗

The routing table specified here may be overridden by Virtual Routing

arriving through the tunnel, not routing for the tunnel itself.

В System -> Device -> Local User Databases добавим новую базу пользователей, которые будут подключаться по L2TP - назовем её I2tp-users. Зайдем в эту базу, добавим пользователя (у меня это – user) и определим пароль для него.

StatusSystemStatusSystemStatusSystemStatusSystem

DeviceAdvanced SettingsDeviceAdvanced SettingsDeviceAdvanced SettingsDeviceAdvanced Settings

▼ Device

Date and Time

DNS

Remote Management

Log and Event Receivers

High Availability

▼ Monitoring

Hardware Monitoring

Link Monitors

▼ Users

Local User Databases

Local User Data

Manage the local user data

+ Add

#	Name
1	AdminUsers
2	I2tp-users

I2tp-users

A local user databa

General

+ Add

Name

user

user

User credentials may be used in User A

GeneralSSH Public Key

Name:user

Password:.....

Confirm Password:.....

Groups:

❗

Comma separated list of group

Users that are members of the 'ad

Users that are members of the 'au

Add administrators

Add a

Per-user IP Configuration (for PPTP,

Static Client IP Address:(None)

Networks behind user:(None)

Metric for networks:

user

User credentials may be used in User

GeneralSSH Public Key

Select the SSH public keys to assoc

SSH Keys

Available	Sele
-----------	------

+ Include

✕

В Policies -> User Authentication -> Authentication Rules добавим новое правило с названием l2tp-auth_rule. В настройках включим только протокол MS-CHAP v2, так как MS-CHAP криптографически уязвим.

Firewalling

User Authentication

Firewalling

User Authentication

Intrusion Prevention

Firewalling

User Authentication

Intrusion Prevention

Rules

Authentication Rules

Authentication Agents

User Directories

LDAP

RADIUS

Accounting

RADIUS

Settings

Authentication Settings

I2tp-auth_rule

The User Authentication Ruleset specifies from which system, and how.

General

Log Settings

Accounting

Agent Options

Select one or more accounting servers for the authenticated user that should be used.

Accounting servers

Available

Selected

+ Include

x

User Statistics

☒ Bytes Sent

☒ Bytes Received

☒ Packets Sent

☒ Packets Received

☒ Enable reporting of the number of sessions the session lasted.

☐ Support Interim Accounting

I2tp-auth_rule

The User Authentication Ruleset specifies from which system, and how.

General

Log Settings

Authentication

Agent Options

Restrictions

PPP Agent Options

☐ Allow no authentication.

☐ Use PAP authentication protocol. User name:

☐ Use CHAP authentication protocol.

☐ Use MS-CHAP authentication protocol.

☒ Use MS-CHAP v2 authentication protocol.

HTTP(s) Agent Options

Login Type:

HTML form

HTTP Banners:

Default

Realm String: (Optional)

MAC Authentication

☐ Allow Clients behind router to connect

MAC Auth Secret: Password must be the same as the one used for the user.

Confirm Secret: Not checked

HTTPS Certificates

Host Certificate:

Root Certificates

Available

Selected

HTTPSAdminCert

I2tp-auth_rule

The User Authentication Ruleset specifies from which system, and how.

General

Log Settings

Authentication

Agent Options

Restrictions

Timeouts

Idle Timeout:

1800

 seconds

Session Timeout: seconds

☐ Use timeouts received from the authenticating server.

Note that if no timeouts are received, OR if the user is idle for more than the session timeout, the user will be logged out.

Multiple Username Logins

☒ Allow multiple logins per username

☐ Allow one login per username, disallow the user from logging in again.

☐ Allow one login per username, Replace existing user if idle for more than

10

 seconds

В Policies -> Firewalling -> Main IP Rules создаем 3 правила. Первое правило (слева) разрешает подключившимся по L2TP пользователям работу в сети Internet через NAT. Два других правила разрешают прохождение пакетов из сети L2TP во внутреннюю сеть LAN и наоборот.

Firewalling

User Authentication

Intrusion Prevention

Rules

Main IP Rules

Application Rule Sets

Profiles

Schedules

Anti-virus

Web Content Filtering

URL Filter

File Control

I2tp-any_nat

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Log Settings

NAT

Multiplex SAT

SLB SAT

SLB M

Application Control

Name: I2tp-any_nat

Action: NAT ! NAT, are not u

Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, target interface and destination network. All parameters have to be specified.

Interface

Network

Source: I2tp-serv

Destination: wan1

I2tp-ip_pool

all-nets

Firewalling

User Authentication

Intrusion Prevention

Ian-I2tp_allow

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Log Settings

NAT

Multiplex SAT

SLB SAT

SLB M

Application Control

Name: Ian-I2tp_allow

Action: Allow ! NAT, are not u

Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, target interface and destination network. All parameters have to be specified.

Interface

Network

Source: lan1

Destination: I2tp-serv

I2tp-ip_pool

I2tp-ip_pool

Firewalling

User Authentication

Intrusion Prevention

I2tp-Ian_allow

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Log Settings

NAT

Multiplex SAT

SLB SAT

SLB M

Application Control

Name: I2tp-Ian_allow

Action: Allow ! NAT, are not u

Service: all_services

Schedule: (None)

Address Filter

Specify source interface and source network, target interface and destination network. All parameters have to be specified.

Interface

Network

Source: I2tp-serv

Destination: lan1

I2tp-ip_pool

I2tp-ip_pool

B Network -> Interfaces and VPN -> IPsec -> Advanced Settings проверим что галка IPsec Before Rules установлена. Также проверим остальные настройки IPsec туннеля.

Status System Objects **Network** Policies

Interfaces and VPN Routing Network Services

▼ Link Layer

Ethernet

VLAN

PPPoE

ARP/Neighbor Discovery

▼ VPN and Tunnels

IPsec

SSL

PPTP/L2TP Servers

L2TPv3 Servers

PPTP/L2TP Clients

L2TPv3 Clients

GRE

▼ Miscellaneous

Interface Groups

IPsec Tunnel Settings

Settings for the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

General		
IPsec Max Rules:	<input type="text" value="0"/>	Amount of IPsec rules allowed (0 = automatic)
IPsec Max Tunnels:	<input type="text" value="0"/>	Amount of IPsec tunnels allowed (0 = automatic)
IKE Send Initial Contact:	<input checked="" type="checkbox"/>	Send 'initial contact' messages.
IKE Send CRLs:	<input checked="" type="checkbox"/>	Send CRLs in the IKE exchange.
IPsec Before Rules:	<input checked="" type="checkbox"/>	Pass IKE & IPsec (ESP/AH) traffic sent to the security gateway directly to the IPsec engine without consulting the ruleset.
IKE CRL Validity Time:	<input type="text" value="86400"/>	Maximum number of seconds a CRL is considered valid (0=obey the 'next update' field in the CRL)
IKE Max CA Path:	<input type="text" value="15"/>	Maximum number of CA certificates in a certificate path.
IPsec Certificate Cache Max Certs:	<input type="text" value="1024"/>	Maximum number of entries in the certificate cache.
IPsec Gateway Name Cache Time:	<input type="text" value="14400"/>	Amount of time to keep an IPsec tunnel open when the remote DNS name fails to resolve
 Dead Peer Detection		
DPD Metric:	<input type="text" value="3"/>	Metric 10s of seconds with no traffic or other evidence of life in tunnel before SA is removed
Flow Metric:	<input type="text" value="15"/>	Minimum number of seconds without data traffic in a flow to activate IKE DPD liveness corresponding IKE SA.
DPD no wait:	<input type="checkbox"/>	Do not wait for 10 times the value of DPD Metric after the value of Flow Metric has expired before activating IKE DPD.
DPD Keep Time:	<input type="text" value="2"/>	Number 10s of seconds a SA will remain in dead cache after a delete. DPD will not trigger if SA is cached as dead.
DPD Expire Time:	<input type="text" value="15"/>	Number of seconds that DPD-R-U-THERE messages will be sent.

B Network -> Interfaces and VPN -> PPTP/L2TP Servers -> Advanced Settings проверим установленные галочки в настройках PPTP/L2TP серверов.

StatusSystemObjectsNetworkPolicies

Interfaces and VPNRoutingNetwork Services

▼ Link Layer

Ethernet

VLAN

PPPoE

ARP/Neighbor Discovery

▼ VPN and Tunnels

IPsec

SSL

PPTP/L2TP Servers

L2TP Server Settings

PPTP/L2TP server settings.

General

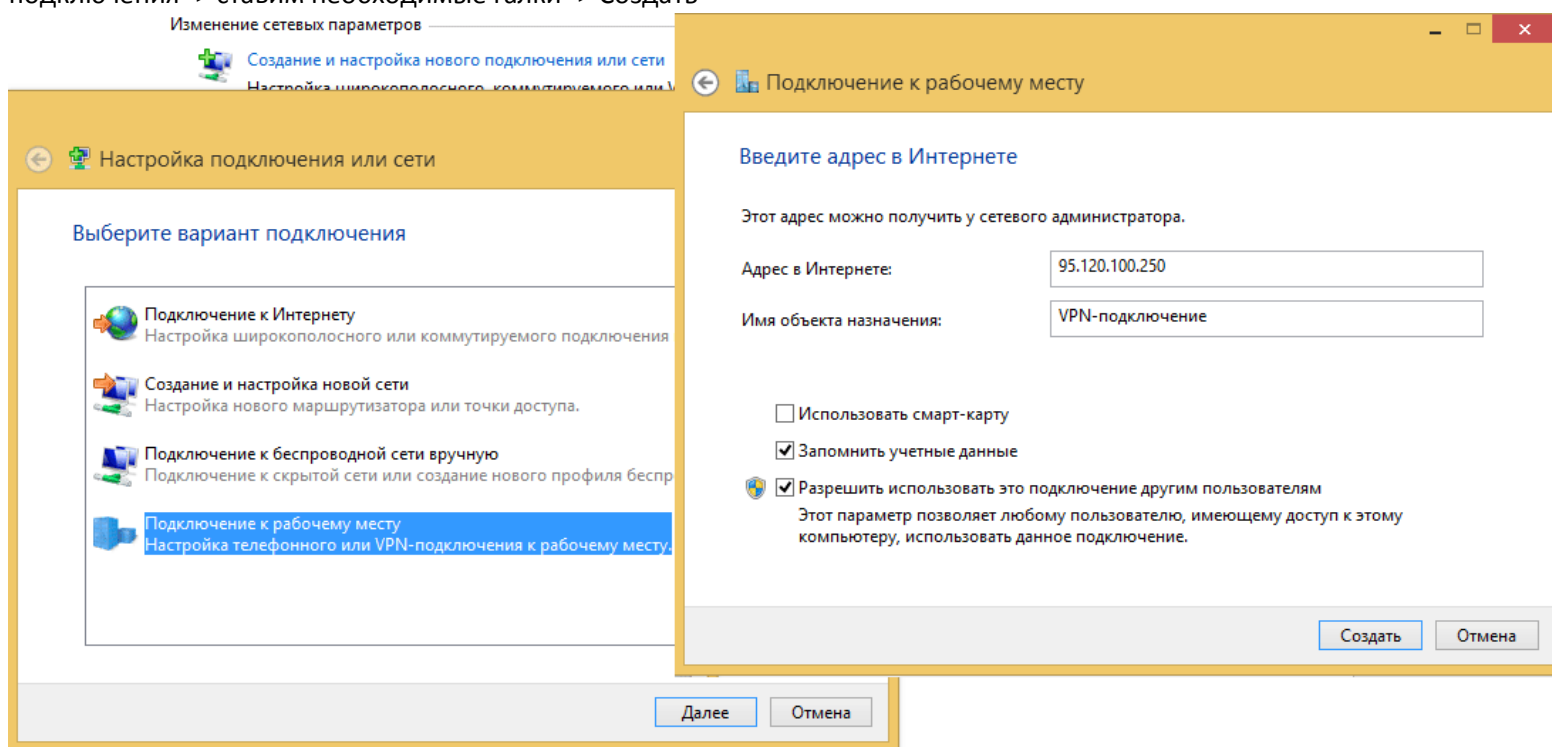
L2TP Before Rules: ☒ Pass L2TP connections sent to the security gateway directly to the L2TP engine without consulting the ruleset.

PPTP Before Rules: ☒ Pass PPTP connections sent to the security gateway directly to the PPTP engine without consulting the ruleset.

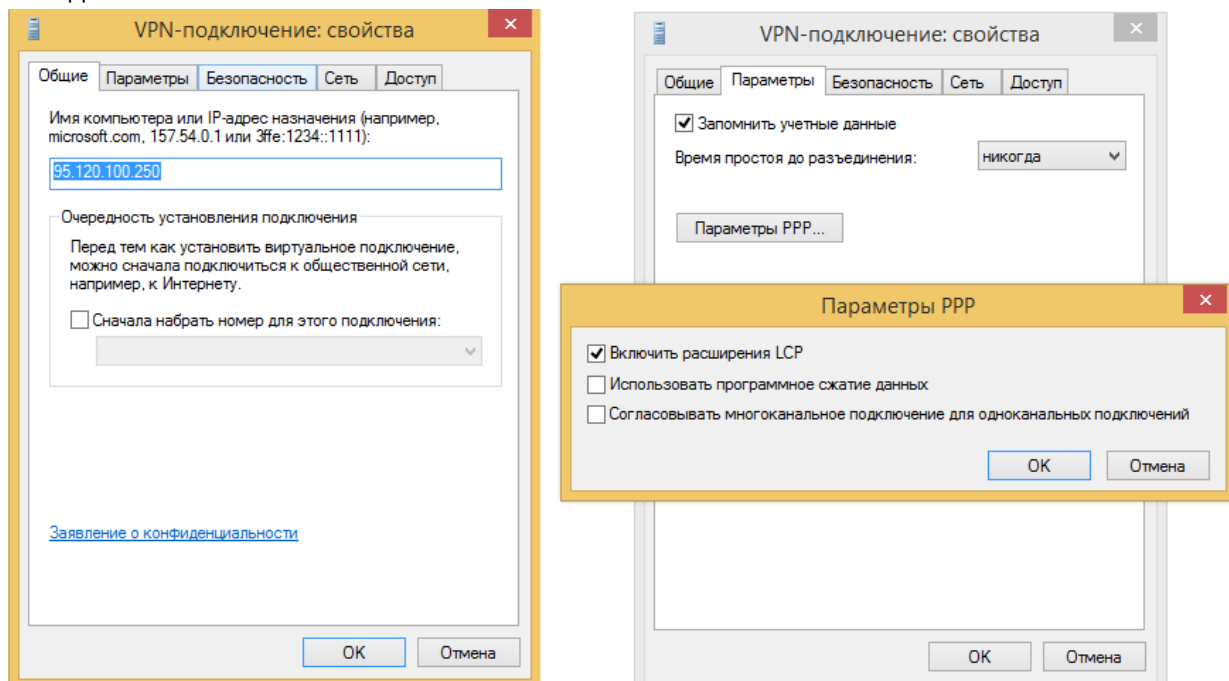
Save

Настройка Windows 7 / 8 для подключения к L2TP серверу

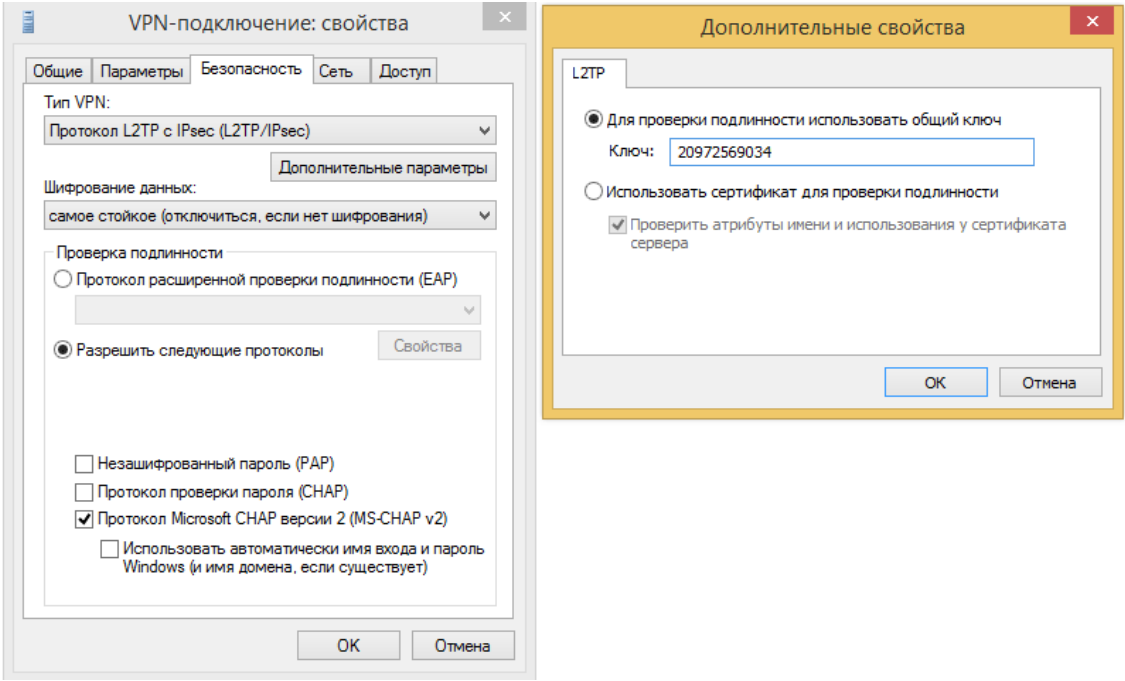
Открываем Центр управления сетями и общим доступом -> Создание и настройка нового подключения или сети -> Подключение к рабочему месту Настройка телефонного или VPN-подключения к рабочему месту -> Использовать мое подключение к Интернету (VPN) -> вводим адрес сервера L2TP (нашем случае это ip адрес wan1_ip) и название подключения -> ставим необходимые галки -> Создать



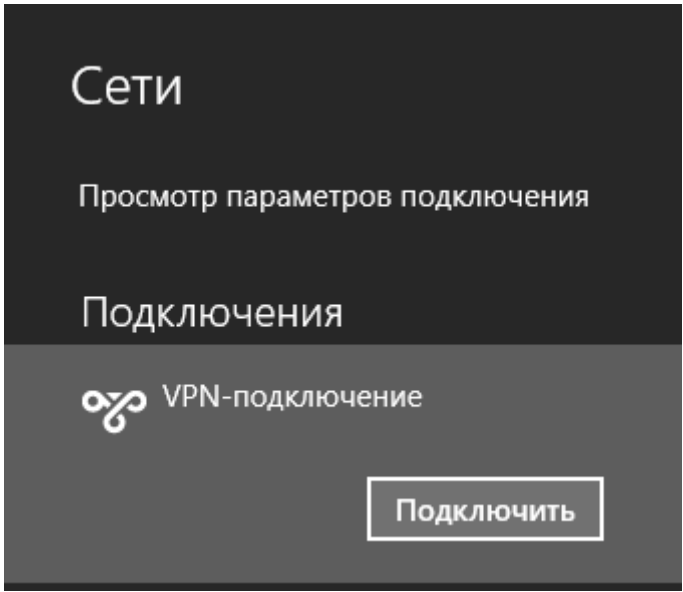
Снова заходим в Центр управления сетями и общим доступом -> Изменение параметров адаптера -> правой кнопкой мышки на VPN-подключение -> Свойства



Выставим правильные параметры подключения для L2TP и в Дополнительных параметрах введем ключ Pre-Shared Key (PSK), заданный ранее в Objects -> Key Ring.



В подключениях выбираем наше ранее созданное VPN-подключение и жмем Подключить. Вводим имя пользователя и пароль, которые мы задали ранее в System -> Device -> Local User Databases. Подключаемся 😊



Любые перепечатки и распространения без моего уведомления запрещены.
e-mail для связи со мной: info@it-st.ru
Создано Sub-Zero © 2014