Автор:
19.09.14 10:26 - Последнее обновление 19.09.14 11:09

PfSense + DSR

Необходимость написания этой статьи была продиктована реальной задачей объединить несколько распределенных филиалов с центральным офисом в одну VPN сеть. В качестве типа VPN соединения был выбран OpenVPN . Во многом такой выбор был сделан в силу того, что в центральном офисе в качестве роутера в свое время был установлен pfSense на базе FreeBSD. Идеальным вариантом было бы установить в удаленных филиалах также pfSense, однако для сетевого оборудования в филиалах отведено очень мало места и надо было найти оптимальный вариант машрутизатора, который мог справится со следующими задачами: быть достаточно компактным, поддерживать OpenVPN, а также, что немаловажно при местных не очень качественных операторах связи, иметь как минимум 2 канала для подключения к внешней сети интернет. В итоге был выбран D-link DSR-500. Дальнейшее рассуждение также справедливо и для DSR-250(N) и для DSR-1000(N). На pfSense настроен по методу OpenVPN PKI: Site-to-Site. Для начала необходимо создать сертификаты. Для этого воспользуемся статьей с сайта 3cx.com.ua
немного измененной под наши нужды.

Содержание

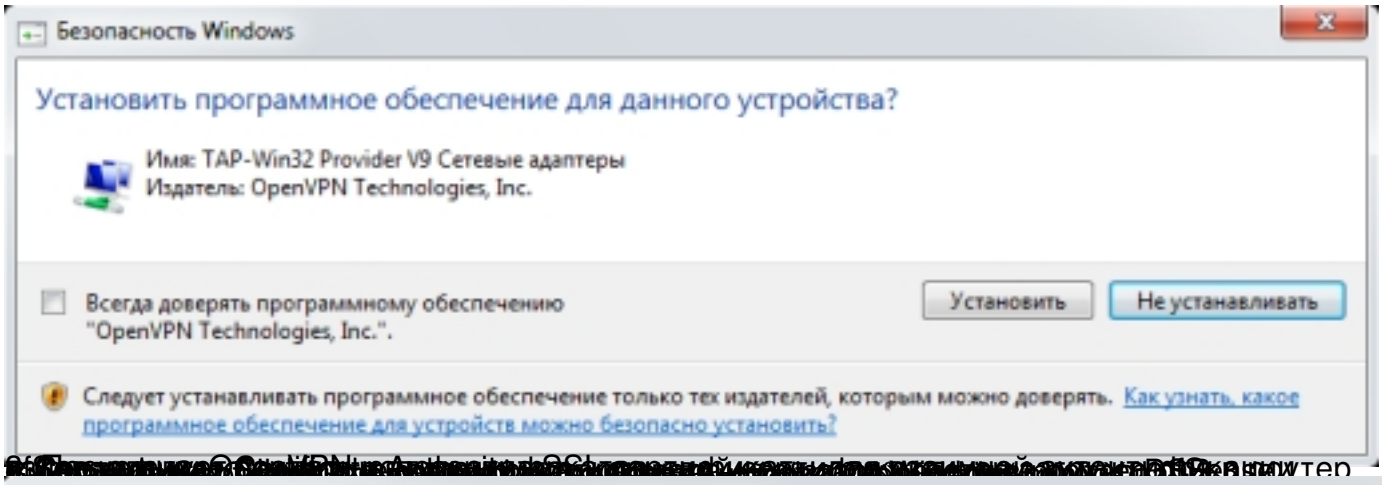
- 1 Создание сертификатов
- 2 Настройка сервера pfSense
- 3 Настройка клиента D-Link DSR500
- 4 Соединение, дополнительные настройки

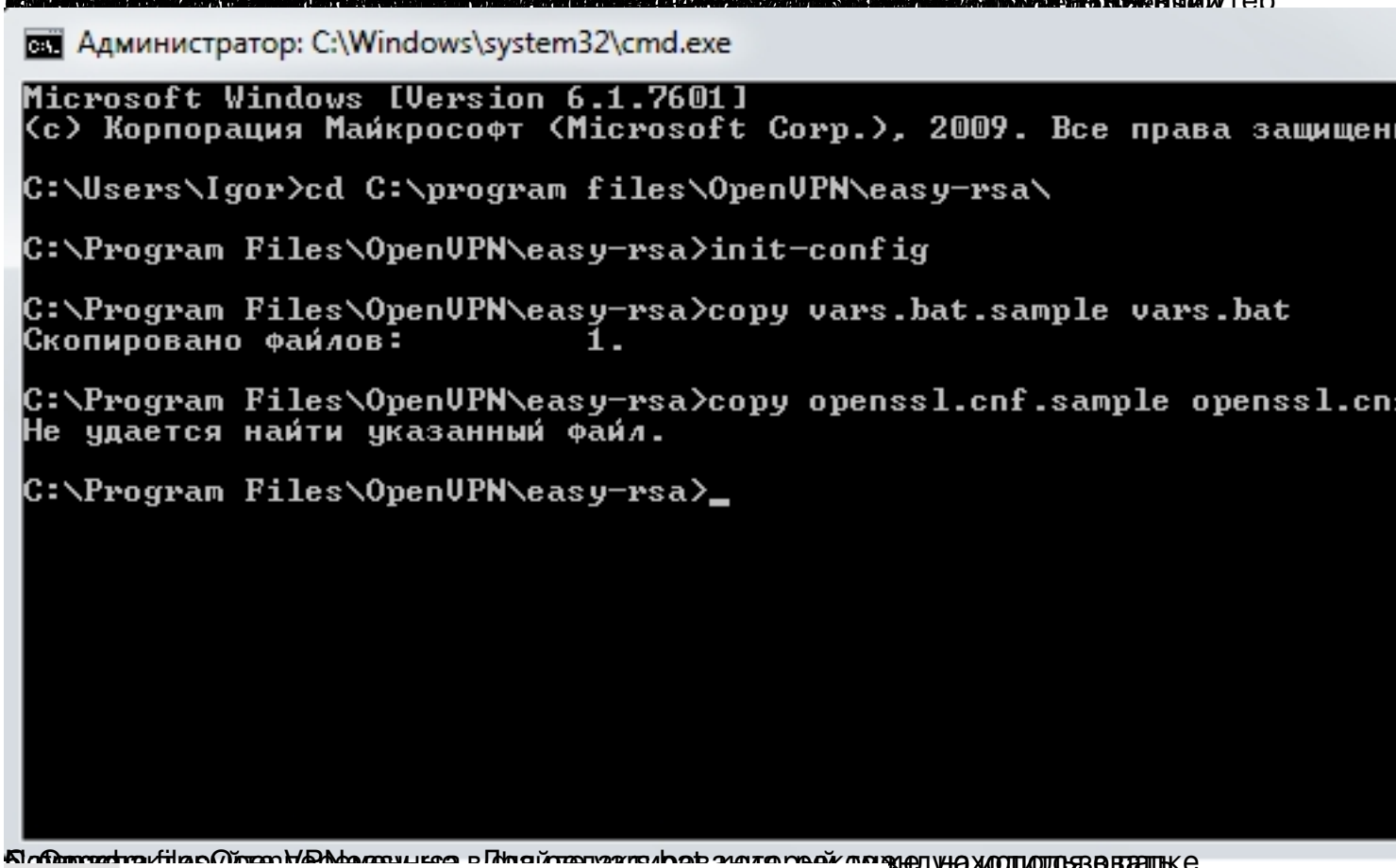
Создание сертификатов

1. Загрузите OpenVPN сервер отсюда. Я использовал файл Windows Installer.

2. Установите приложение. Все опции установки оставьте по умолчанию. На этапе установки появится запрос установки TAP адаптера. Соглашайтесь.

Автор:
19.09.14 10:26 - Последнее обновление 19.09.14 11:09



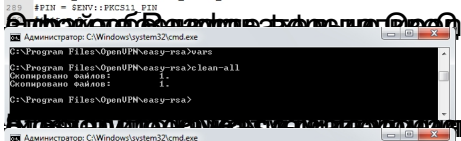


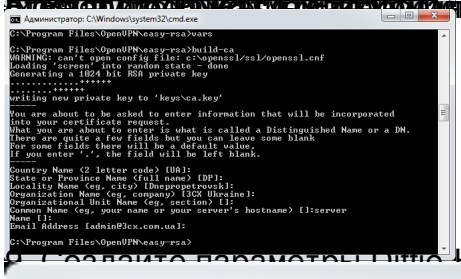

```
31  set KEY_COUNTRY=UA
32  set KEY_PROVINCE=DP
33  set KEY_CITY=Dnepropetrovsk
34  set KEY_ORG=3CX Ukraine
35  set KEY_EMAIL=admin@3cx.com.ua
```

и сертификатами PKCS#11.

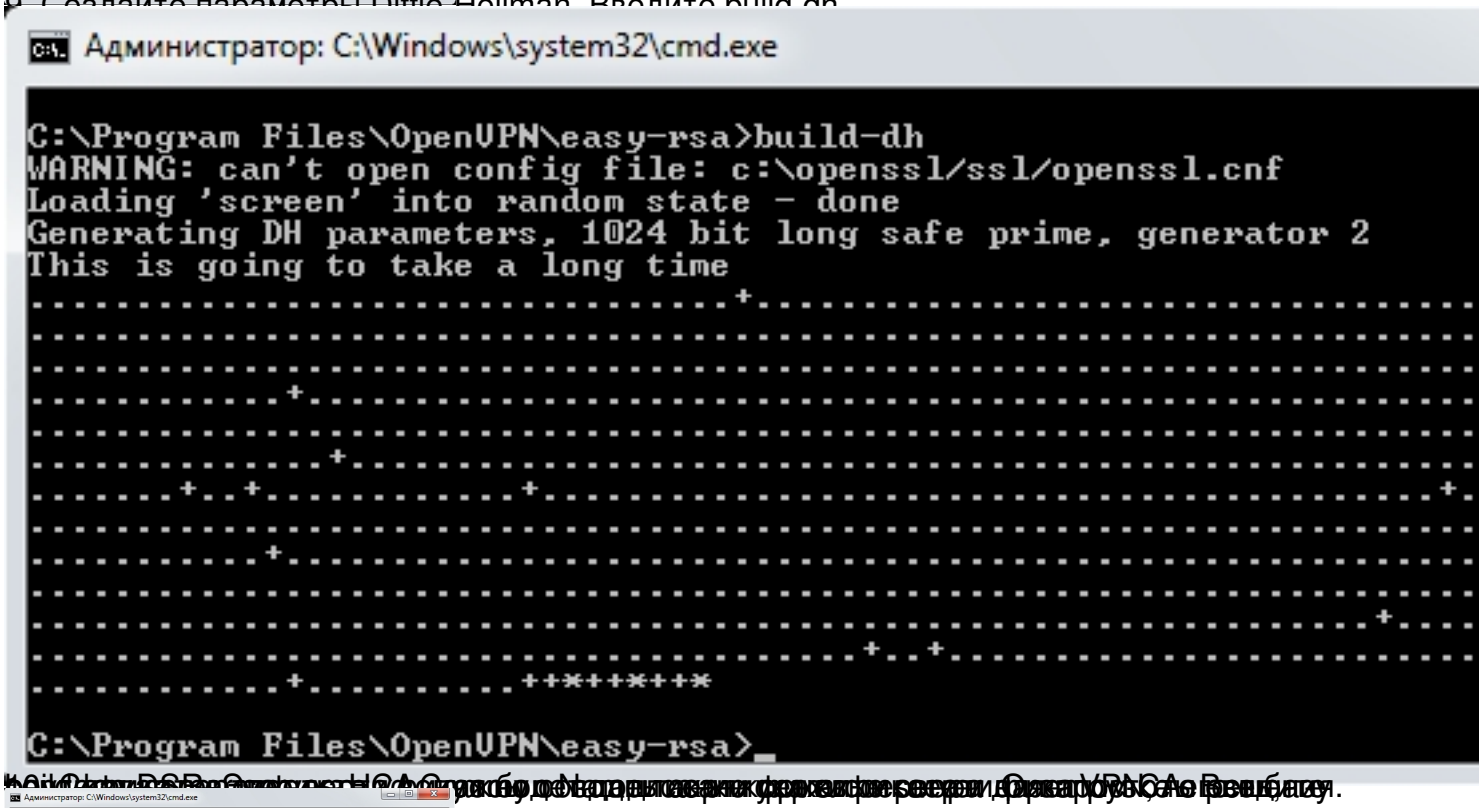
Автор:
19.09.14 10:26 - Последнее обновление 19.09.14 11:09

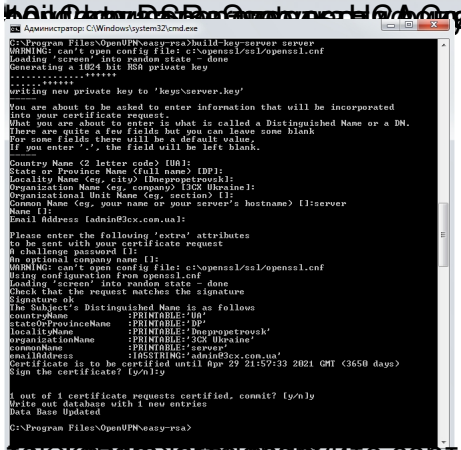
```
#
# If you are using PKCS#11
# Install engine_pkcs11 of opensc (www.opensc.org)
# And uncomment the following
# verify that dynamic_path points to the correct location
#
#pkcs11 = pkcs11_section

#[ pkcs11_section ]
#engine_id = pkcs11
#dynamic_path = /usr/lib/engines/engine_pkcs11.so
#MODULE_PATH = $ENV::PKCS11_MODULE_PATH
#PIN = $ENV::PKCS11_PIN
```



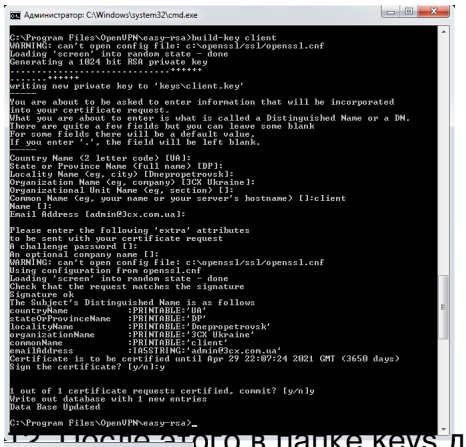


9. Создайте параметры Diffie-Hellman. Введите build-dh

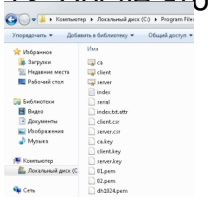




Также генерируем сертификат клиента. Введите build-key client. Common Name



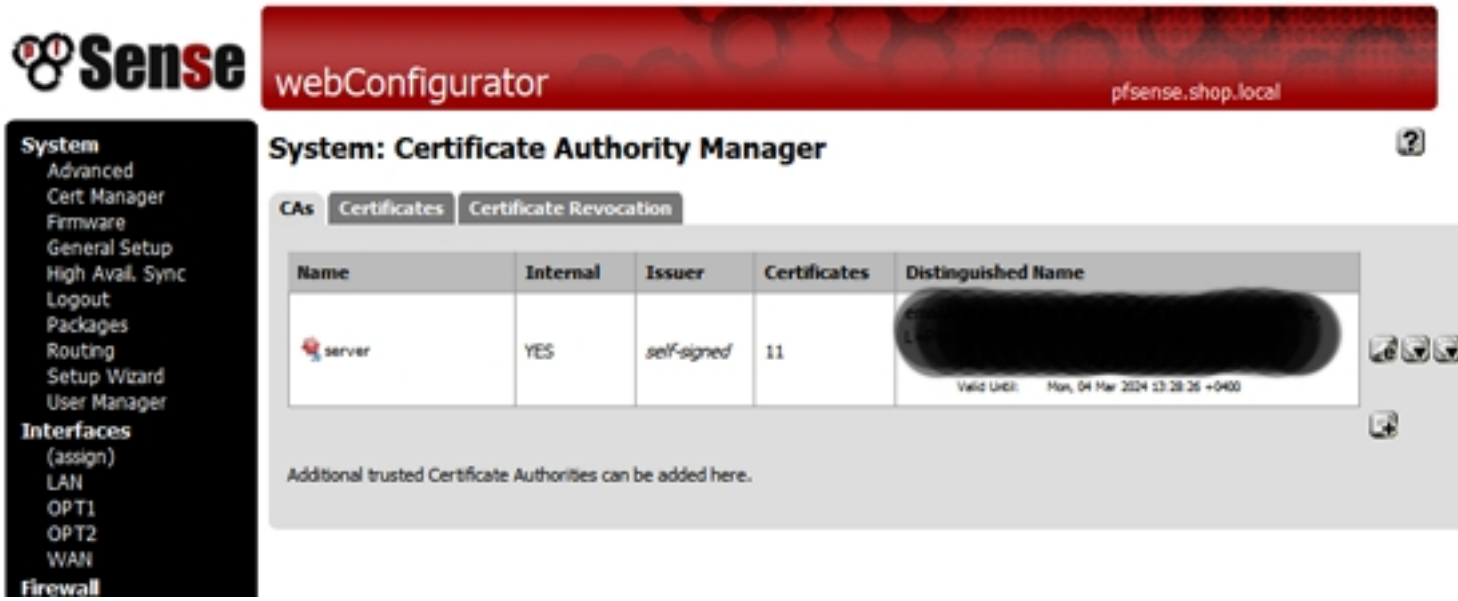
19. После этого в папке keys должны присутствовать все необходимые сертификаты.



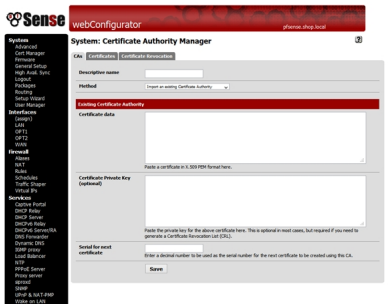
Настройка сервера pfSense

Также воспользуемся уже написанной статьей с форума [psSense](#) и также немного переработанной.

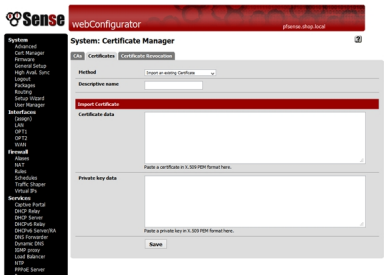
На сервере (pfSense) переходим в меню System -> Cert Manager на вкладку CAs



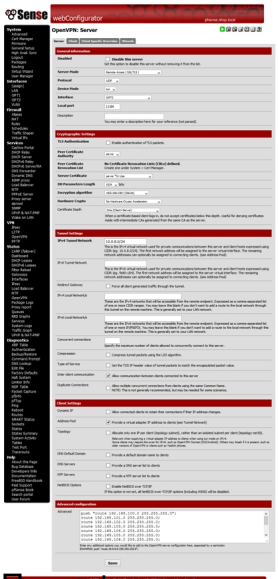
Импортируем и сохранеем сертификат нового центра сертификации



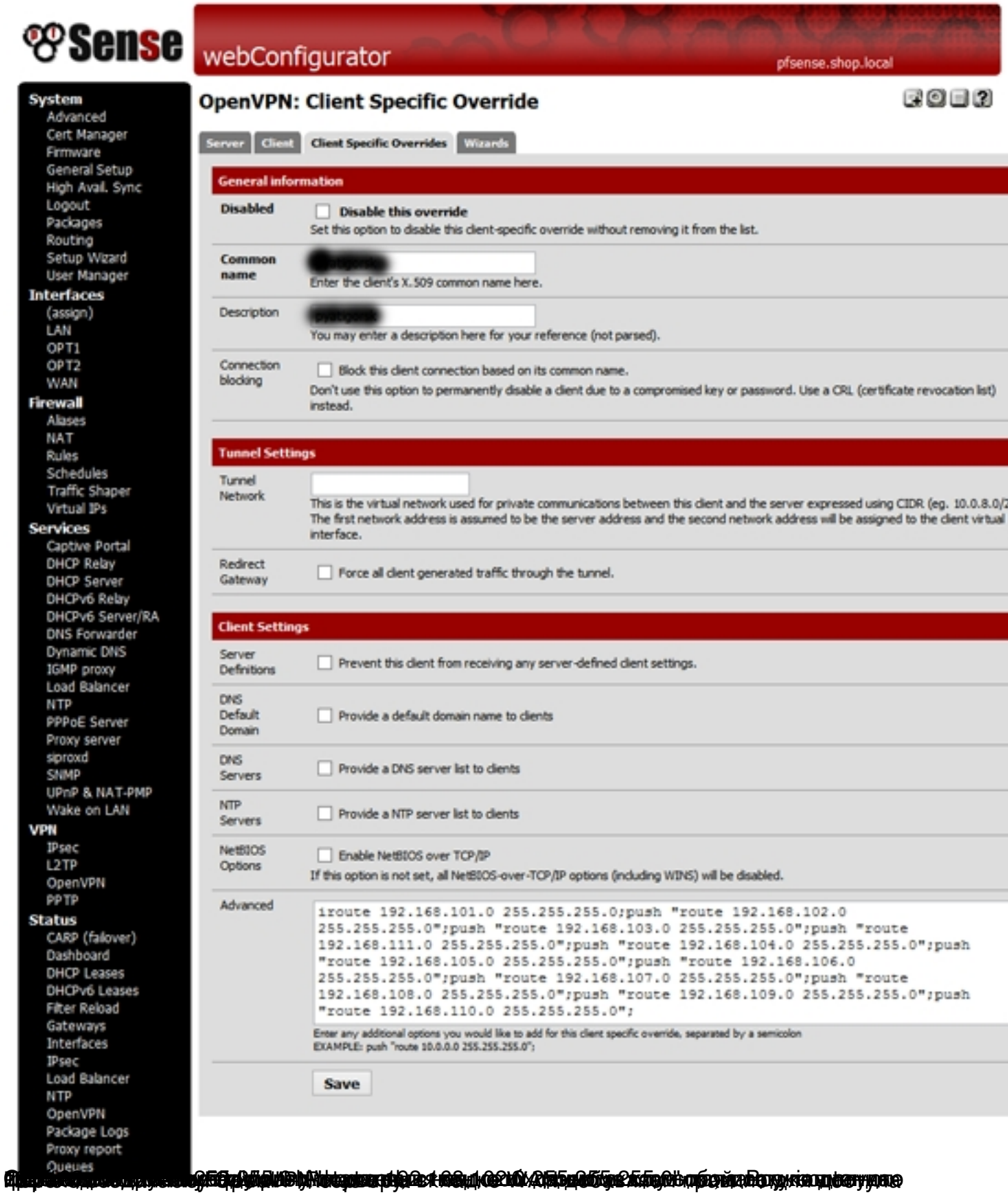
Переходим на вкладку Certificates и сохраняем сертификаты сервера и клиента/ов



Переходим в меню VPN -> OpenVPN на вкладку Server и добавляем новый сервер кнопкой “+”:



Переходим на вкладку Client Specific Overrides и кнопкой “+” добавляем настройки

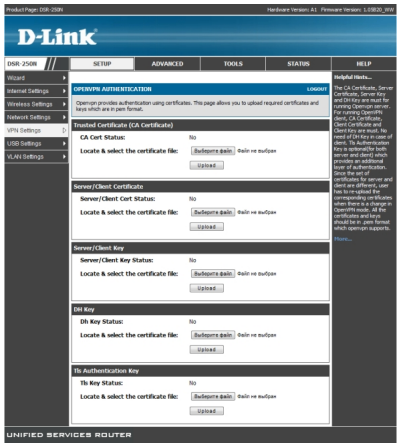

pfSense
webConfigurator
pfsense.shop.local
System
Advanced
Cert Manager
Firmware
General Setup
High Avail. Sync
Logout
Packages
Routing
Setup Wizard
User Manager
Interfaces
(assign)
LAN
OPT1
OPT2
WAN
Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs
Services
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server/RA
DNS Forwarder
Dynamic DNS
IGMP proxy
Load Balancer
NTP
PPPoE Server
Proxy server
siproxd
SNMP
UPnP & NAT-PMP
Wake on LAN
VPN
IPsec
L2TP
OpenVPN
PPTP
Status
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
Filter Reload
Gateways
Interfaces
IPsec
Load Balancer
NTP
OpenVPN
Package Logs
Proxy report
Queues
OpenVPN: Client Specific Override
Server
Client
Client Specific Overrides
Wizards
General information
Disabled
Disable this override
Set this option to disable this client-specific override without removing it from the list.
Common name
Enter the client's X.509 common name here.
Description
You may enter a description here for your reference (not parsed).
Connection blocking
Block this client connection based on its common name.
Don't use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.
Tunnel Settings
Tunnel Network
This is the virtual network used for private communications between this client and the server expressed using CIDR (eg. 10.0.8.0/24). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.
Redirect Gateway
Force all client generated traffic through the tunnel.
Client Settings
Server Definitions
Prevent this client from receiving any server-defined client settings.
DNS Default Domain
Provide a default domain name to clients
DNS Servers
Provide a DNS server list to clients
NTP Servers
Provide a NTP server list to clients
NetBIOS Options
Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
Advanced
iroute 192.168.101.0 255.255.255.0;push "route 192.168.102.0 255.255.255.0";push "route 192.168.103.0 255.255.255.0";push "route 192.168.111.0 255.255.255.0";push "route 192.168.104.0 255.255.255.0";push "route 192.168.105.0 255.255.255.0";push "route 192.168.106.0 255.255.255.0";push "route 192.168.107.0 255.255.255.0";push "route 192.168.108.0 255.255.255.0";push "route 192.168.109.0 255.255.255.0";push "route 192.168.110.0 255.255.255.0";
Enter any additional options you would like to add for this client specific override, separated by a semicolon
EXAMPLE: push "route 10.0.0.0 255.255.255.0";
Save

Переходим на вкладку OpenVPN и добавляем правило:

Настройка клиента D-Link DSR500

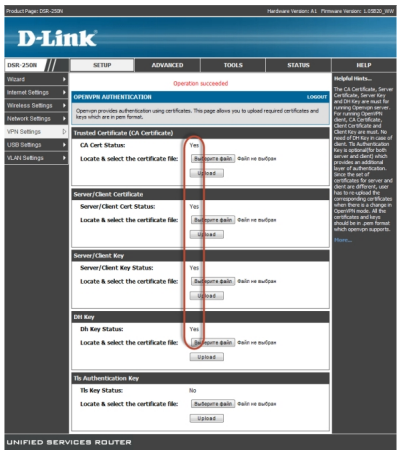
В первую очередь особо хочу отметить, что OpenVPN реализован только на WW прошивках. На прошивках RU этого функционала нет. WW прошивка ничем кроме расширенного функционала не отличается. В любом случае интерфейс будет на английском языке.

1. Откройте web интерфейс роутера. У меня испытательный роутер имеет IP адрес 192.168.101.10. Перейдите в раздел Setup – VPN Settings – OpenVPN – OpenVPN Authentication.



2. Загрузите в роутер созданные файлы сертификатов в соответствии с таблицей. Trusted Certificate (CA Certificate) ca.crt Server/Client Certificate client.crt Server/Client Key client.key DH Key dh1024.pem

Убедитесь, что файлы загружены успешно.



3. Перейдите в раздел Setup – VPN Settings – OpenVPN – OpenVPN Configuration.

Установите галочку Enable Openvpn.

Выберите режим Client. Server IP – это адрес вашего VPN сервера.

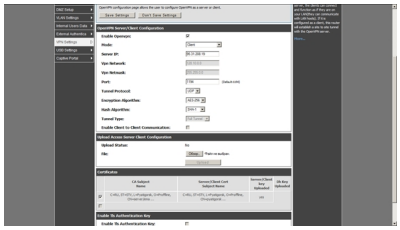
Port рекомендуется оставить по умолчанию.

Encryption Algorithm — в данном примере я установил AES-256 (как на сервере).

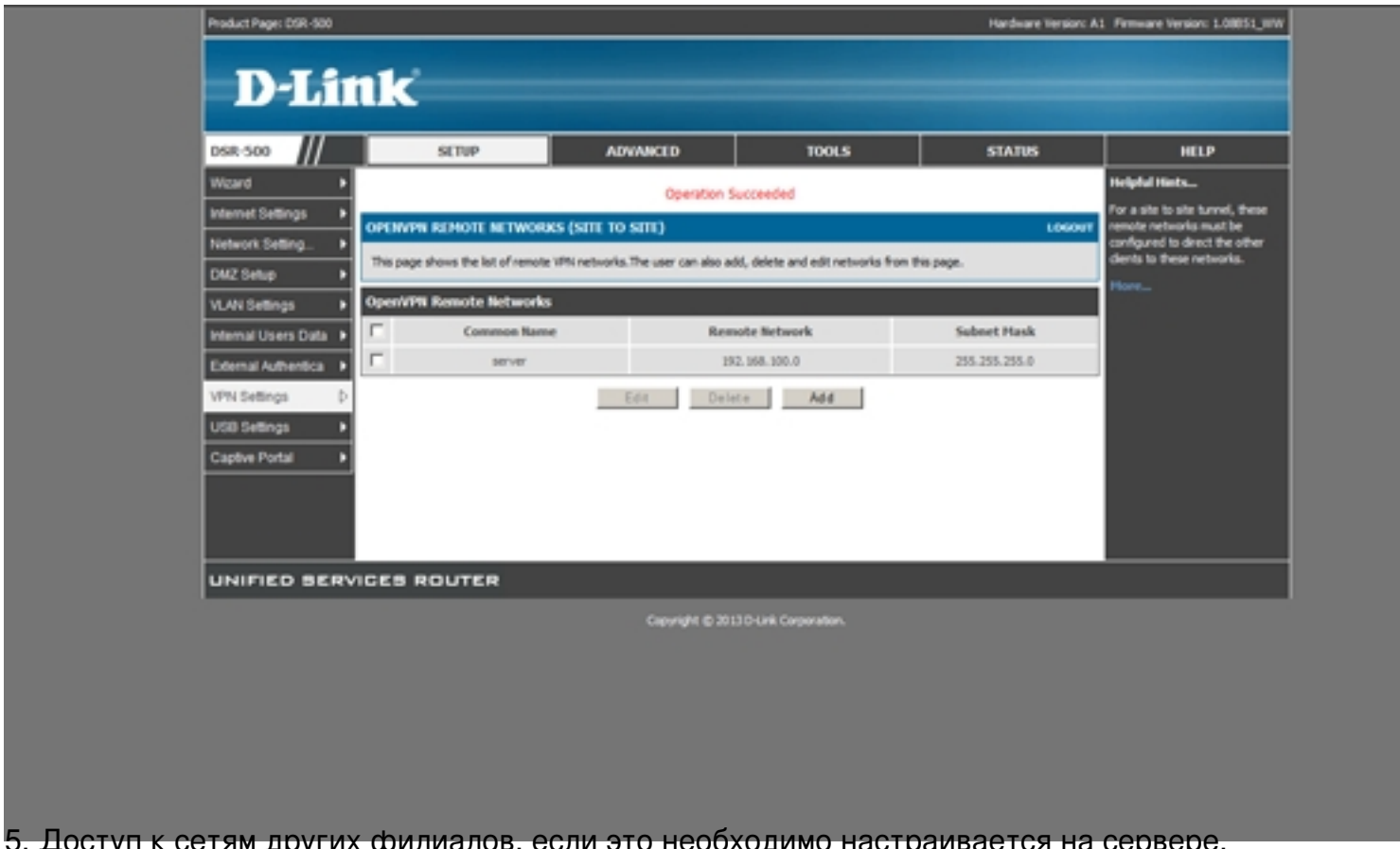
Hash Algorithm – SHA-1, по умолчанию.

Далее я отметил галочкой используемые сертификаты.

Enable TLS Authentication Key включается, если предполагается шифрование сертификатов, иначе сертификаты будут передаваться в открытом виде. В IP телефонах Yealink режим шифрования сертификатов не поддерживается.



4. Перейдите в раздел Setup – VPN Settings – OpenVPN – OpenVPN Remote Networks (Split Tunneling). Здесь следует добавить удаленную сеть сервера, к которой OpenVPN клиент будет иметь доступ. Я добавил свою локальную сеть 192.168.100.0.



5. Доступ к сетям других филиалов, если это необходимо настраивается на сервере.

Соединение, дополнительные настройки

Через несколько секунд в меню Status – OpenVPN видим успешно подключившийся клиент:

Таблица маршрутов сервера (pfSense1 головного офиса):

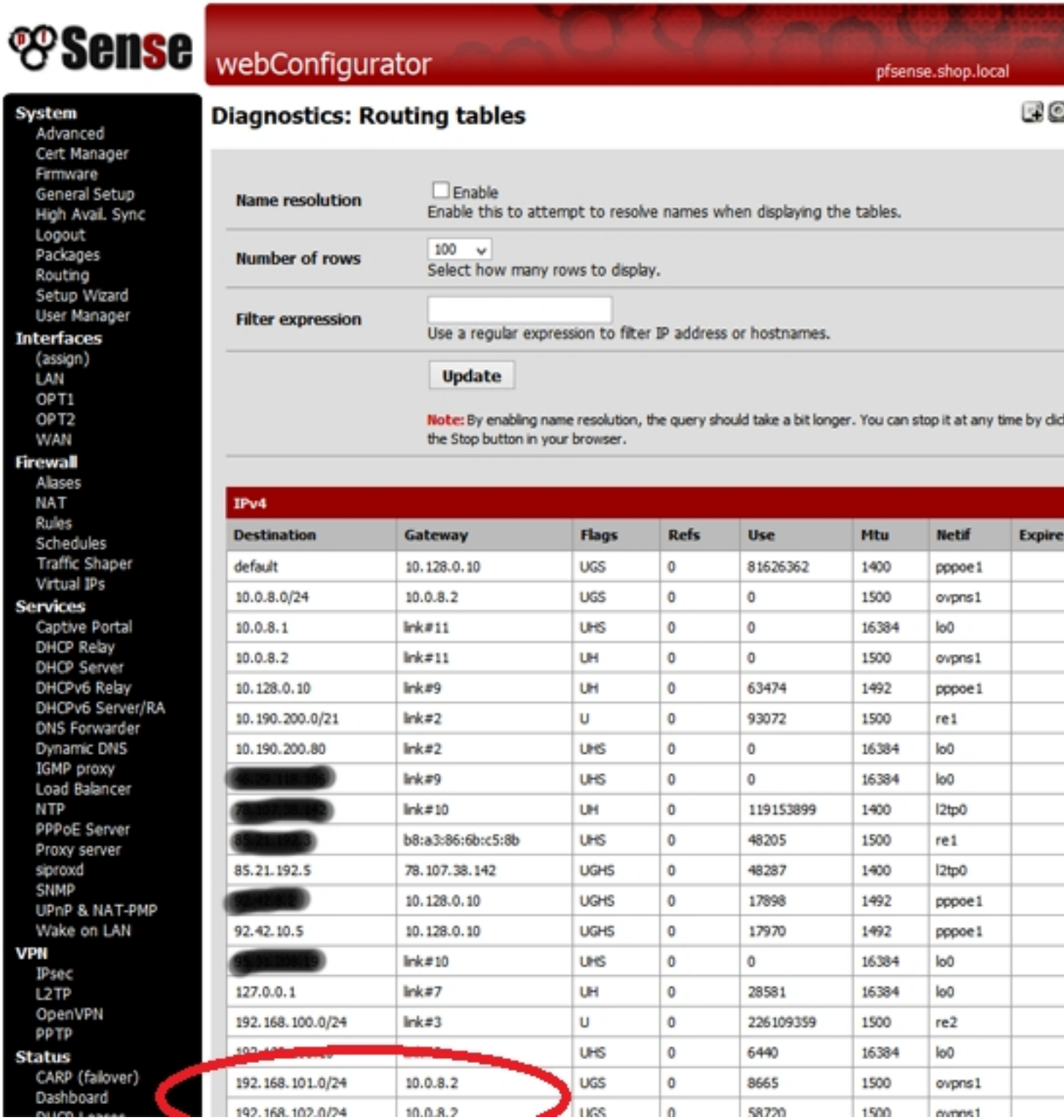
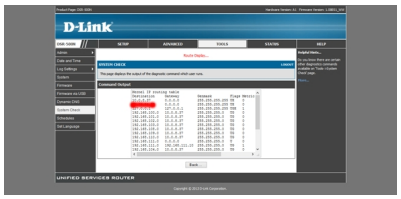

pfSense
webConfigurator
pfsense.shop.local
System
Advanced
Cert Manager
Firmware
General Setup
High Avail. Sync
Logout
Packages
Routing
Setup Wizard
User Manager
Interfaces
(assign)
LAN
OPT1
OPT2
WAN
Firewall
Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs
Services
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server/RA
DNS Forwarder
Dynamic DNS
IGMP proxy
Load Balancer
NTP
PPPoE Server
Proxy server
siproxd
SNMP
UPnP & NAT-PMP
Wake on LAN
VPN
IPsec
L2TP
OpenVPN
PPTP
Status
CARP (failover)
Dashboard
Diagnostics: Routing tables
Name resolution
Enable
Enable this to attempt to resolve names when displaying the tables.
Number of rows
100
Select how many rows to display.
Filter expression
Use a regular expression to filter IP address or hostnames.
Update
Note: By enabling name resolution, the query should take a bit longer. You can stop it at any time by clic
the Stop button in your browser.
IPv4
Destination
Gateway
Flags
Refs
Use
Mtu
Netif
Expire
default
10.128.0.10
UGS
0
81626362
1400
pppoe1
10.0.8.0/24
10.0.8.2
UGS
0
0
1500
ovpns1
10.0.8.1
link#11
UHS
0
0
16384
lo0
10.0.8.2
link#11
UH
0
0
1500
ovpns1
10.128.0.10
link#9
UH
0
63474
1492
pppoe1
10.190.200.0/21
link#2
U
0
93072
1500
re1
10.190.200.80
link#2
UHS
0
0
16384
lo0
link#9
UHS
0
0
16384
lo0
link#10
UH
0
119153899
1400
l2tp0
b8:a3:86:6b:c5:8b
UHS
0
48205
1500
re1
85.21.192.5
78.107.38.142
UGHS
0
48287
1400
l2tp0
10.128.0.10
UGHS
0
17898
1492
pppoe1
92.42.10.5
10.128.0.10
UGHS
0
17970
1492
pppoe1
link#10
UHS
0
0
16384
lo0
127.0.0.1
link#7
UH
0
28581
16384
lo0
192.168.100.0/24
link#3
U
0
226109359
1500
re2
UHS
0
6440
16384
lo0
192.168.101.0/24
10.0.8.2
UGS
0
8665
1500
ovpns1
192.168.102.0/24
10.0.8.2
UGS
0
58720
1500
ovpns1

Таблица маршрутов клиента



Сети головного офиса и филиала доступны друг другу через созданный туннель.

Как видите, какие либо настройки маршрутизации на OpenVPN клиенте полностью отсутствуют. Заполнив поле Remote Network на клиенте, мы передали маршрут в сеть головного офиса клиенту. Напомню, это действие абсолютно аналогично тому, что на сервере в поле Advanced мы написали бы: push “route 192.168.10.0 255.255.255.0” или тому, что на клиенте в Remote Network написали: 192.168.10.0/24, или на клиенте в поле Advanced: route 192.168.10.0 255.255.255.0. Но и это не все. Мы могли бы написать: push “route 192.168.10.0 255.255.255.0” в Client Specific Overrides для ovpnc на сервере и это привело бы к тому же результату. OpenVPN в режиме PKI позволяет централизованно и гибко управлять клиентами. Все можно сделать на сервере, не прописывая route или Remote Network на каждом клиенте. Все можно настроить индивидуально в Client Specific Overrides. Для сравнения, push “route 192.168.10.0 255.255.255.0” в поле Advanced сервера действует глобально на всех клиентов.

источник: http://it-pedia.com/index.php?title=PfSense_%2B_DSR

{jcomments on}