

Домашнее задание к занятию 23

ДЗ на тему «Настройка безопасных VPN-соединений»:

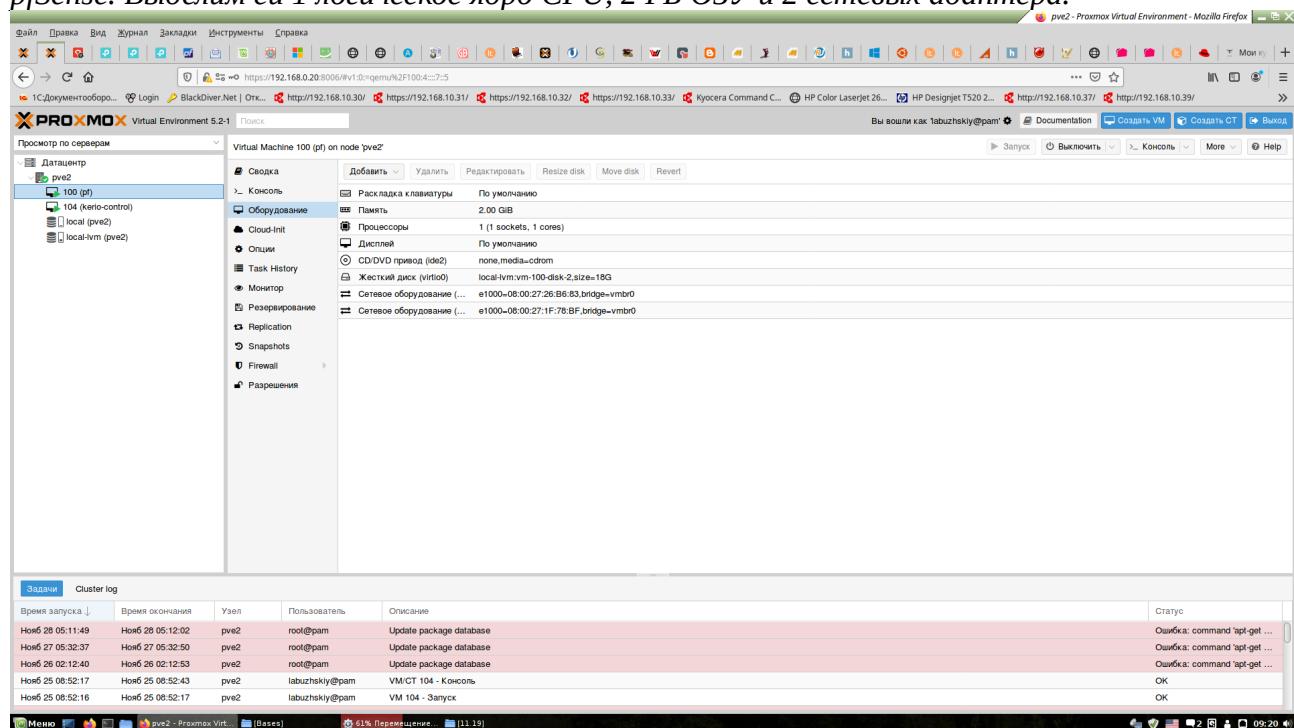
создать несколько VPN-соединений к другим компьютерам на базе Linux, находящихся в другом сегменте сети Интернет, настроить криптографические протоколы защищенного обмена

Цели занятия

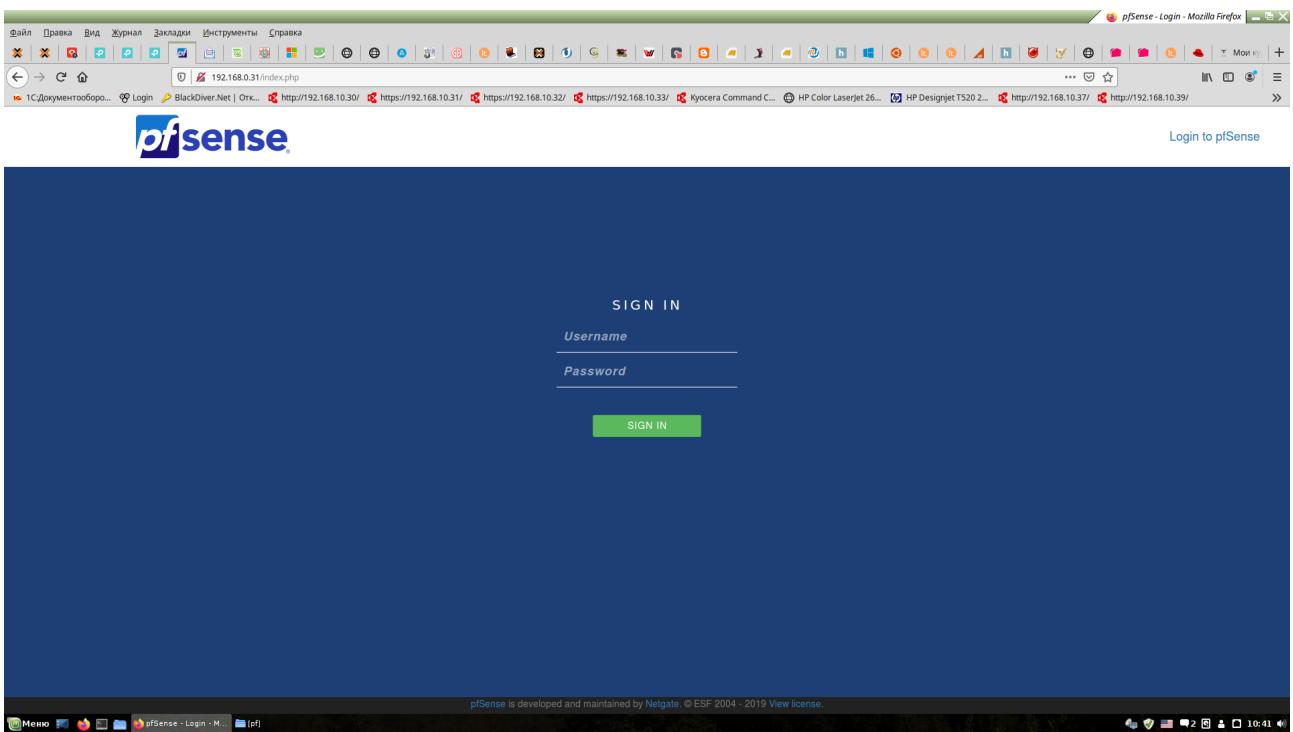
научиться практическим аспектам управления защищенными соединениями (SSH, VPN, VLAN, DMZ-сегментация)

На мой взгляд, реализация выполнения данного домашнего задания выглядела бы интереснее на базе ОС **pfSense**; разворачивать тестовый стенд предлагаю в **ProxmoxVE**.

1. Подготовительный этап: создание шаблона VM, в котором произведём развёртывание pfSense. Выделим ей 1 логическое ядро CPU, 2 ГБ ОЗУ и 2 сетевых адаптера.



После установки, его можно настраивать в веб-браузере, он имеет приветливый дружественный интерфейс:



Консоль управления выглядит примерно так:

```

QEMU (рђ - noVNC - Mozilla Firefox
Message from syslogd@p1 at Nov 28 00:38:36 ...
php-fpm: /index.php: Successful login for user 'admin' from: 100.100.10.10 (L
Welcome to pfSense 2.4.4-RELEASE-p3 (amdkd4) on pf ***
em0 (wan)      -> em0      -> v4: 192.168.0.30/8
em1 (lan)      -> em1      -> v4: 192.168.0.31/8
0) Logout (SSH only)
1) Assign Interfaces
2) Set Interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Firewall Rules
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell pfSense tools
13) Firewall Rules
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option: [1]

```

Время запуска	Время окончания	Узел	Пользователь	Описание	Статус
Нояб 28 09:20:19		pve2	labuzhskiy@pam	VM/CT 100 - Консоль	
Нояб 28 05:11:49	Нояб 28 05:12:02	pve2	root@pam	Update package database	Ошибка: command 'apt-get ...
Нояб 27 05:32:37	Нояб 27 05:32:50	pve2	root@pam	Update package database	Ошибка: command 'apt-get ...
Нояб 26 02:12:40	Нояб 26 02:12:53	pve2	root@pam	Update package database	Ошибка: command 'apt-get ...
Нояб 25 08:52:17	Нояб 25 08:52:43	pve2	labuzhskiy@pam	VM/CT 104 - Консоль	OK

После процедуры аутентификации, попадаем на её главную страницу, которая выглядит так:

The screenshot shows the pfSense dashboard interface. At the top, there's a header bar with various links and a search bar. Below it is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has several sections:

- System Information**: Shows details about the pf.localdomain device, including Name (pf.localdomain), User (admin@192.168.10.10 (Local Database)), System (pfSense Netgate Device ID: 46851000000000000000), BIOS (Vendor: Seabios Version: rel-1.1.0-0-g63451fca13-prebuilt.qemu-project.org Release Date: Tue Apr 1 2014), and Version (2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2019 FreeBSD 11.2-RELEASE-p10). It also displays CPU Type (Common KVM processor AES-NI CPU Crypto: No), Kernel PTI (Enabled), Uptime (12 Days 15 Hours 55 Minutes 03 Seconds), Current date/time (Thu Nov 28 8:47:11 +05 2019), DNS server(s) (127.0.0.1, 192.168.1.254), Last config change (Fri Aug 16 14:14:55 +05 2019), State table size (0% (79/199000) Show states), MBUF Usage (1% (1016/124688)), Load average (0.30, 0.36, 0.38), and CPU usage (2%).
- Netgate Services And Support**: A section for retrieving support information.
- Interfaces**: Displays two interfaces: WAN (1000baseT <full-duplex> 192.168.1.30) and LAN (1000baseT <full-duplex> 192.168.1.31).

At the bottom, there's a footer with the pfSense logo and a note about the license, along with a taskbar showing the current window and system status.

Пробежимся по настройкам нашего сервера:

В менеджере сертификатов выполним генерацию нового сертификата сервера

Create / Edit CA

Descriptive name: Tehnoprrom

Method: Import an existing Certificate Authority

Existing Certificate Authority

```
-----BEGIN CERTIFICATE-----
MIIEyDCAQ6gAwIBAgIBADANBgkqhkiG9w0BAQUFADCBiTELMAkGA
1UEBMMCUUx
HQAABgNVBAtE09yZ51eXJnc2tpe5ByZWdpb24xETAPBgNVAcTC
E9yZ51dJn
MRkwFwYDQOKFBPT09c11R1aG5vcvCHJvbVw1MRBwH0YJKoZIhvcNA
Paste a certificate in X.509 PEM format here.
```

Certificate Private Key (optional)

```
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSIAgEAAoIBAQD0a
bDAWY12A6Yb
RE6WIK0uaFUxtjf/r64ajrm5zvr3WCZ8uoU2153c3RE0e8aj
/5NBj0011G4-YGTF
FHfH1zJyaHicTAXMfcok/tG6oS1v7lax4XYW+5FYNFAnrc6BFk
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).
```

Serial for next certificate: 21

Enter a decimal number to be used as the serial number for the next certificate to be created using this CA.

Save

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
Tehnoprrom	✓	self-signed	8	emailAddress=labuzhskiy@ya.ru, ST=Orenburgskiy region, OU=factory, O=000 "Tehnoprrom", L=Orenburg, CN=ca, C=RU Valid From: Mon, 23 Jul 2018 09:38:54 +0500 Valid Until: Thu, 20 Jul 2028 09:38:54 +0500	OpenVPN Server LDAP Server	Edit Delete

В параметрах сетевых интерфейсов зададим настройки сетевым адаптерам по WAN и LAN

При этом в настройках интерфейса WAN зададим использование шлюза, для доступа в сеть интернет, а в настройках LAN нет. (LAN будем в дальнейшем использовать исключительно для настройки сервера, для доступа в веб-интерфейс через ЛВС, а WAN для взаимодействия с удалёнными клиентами приёма и передачи трафика оффтоп рабочих станций). При настройке WAN и LAN выделим из диапазона 2 рядом стоящих ip-адреса.

pf.localdomain - Interfaces: Interface Assignments - Mozilla Firefox

File Edit View Journal Bookmarks Tools Help

192.168.0.31/interfaces_assign.php

1C Документооборот Login BlackDiver.Net | On... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ Kyocera Command C... HP Color LaserJet 26... HP Designjet T520 2... http://192.168.10.37/ http://192.168.10.39/

pfSense System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIGs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:26:b6:83)
LAN	em1 (08:00:27:1f:78:bf) Delete
Available network ports:	ovpn2 () Add

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

pf.localdomain - Interfaces: WAN (em0) - Mozilla Firefox

File Edit View Journal Bookmarks Tools Help

192.168.0.31/interfaces.php?if=wlan

1C Документооборот Login BlackDiver.Net | On... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ Kyocera Command C... HP Color LaserJet 26... HP Designjet T520 2... http://192.168.10.37/ http://192.168.10.39/

Interfaces / WAN (em0)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxxxx
MTU	<input type="text"/>
MSS	<input type="text"/>
Speed and Duplex	Default (no preference, typically autoselect)

This field can be used to modify ('spoof') the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx or leave blank.

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.0.30
IPv4 Upstream gateway	GW_WAN - 192.168.0.1 + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>
---	--------------------------

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a

192.168.0.31/interfaces.php?if=lan

Interfaces / LAN (em1)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN
Enter a description (name) for the interface here.	
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	00:0C:29:00:00:00
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxxxx or leave blank.	
MTU	1500
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.	
MSS	1460
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.	
Speed and Duplex	Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.	

Static IPv4 Configuration

IPv4 Address	192.168.0.31	/ 8
IPv4 Upstream gateway	None	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10.0/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a network.	

Далее выполним настройку файервола для внешнего порта, который назначим на приём запросов из вне.

192.168.0.31/firewall_rules.php

pfSense COMMUNITY EDITION

Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 994.66 MB	IPv4 UDP	*	*	WAN address	443	*	none		OpenVPN wizard	

pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN

Address Family: IPv4

Protocol: UDP

Source

Source: Invert match. any Source Address /

Destination

Destination: Invert match. WAN address Destination Address /

Destination Port Range: (other) From Custom To Custom
Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port.

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Rule Information

Tracking ID: 152644015
Created: 7/23/18 15:34:11 by admin@192.168.0.156
Updated: 8/3/18 12:19:29 by admin@192.168.0.156

Save

Не забываем сохраняться, внизу присутствует синяя кнопка «Save»

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN

Address Family: IPv4

Protocol: UDP

Source

Source: Invert match. any Source Address /

Destination

Destination: Invert match. WAN address Destination Address /

Destination Port Range: (other) From Custom To Custom
Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port.

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: OpenVPN wizard
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Rule Information

Tracking ID: 152644015
Created: 7/23/18 15:34:11 by admin@192.168.0.156
Updated: 8/3/18 12:19:29 by admin@192.168.0.156

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2019 View license.

Файл Драва Вид Журнал Закладки Инструменты Справка

192.168.0.31/firewall_rules_edit.php?id=3

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: OpenVPN

Address Family: IPv4

Protocol: Any

Source: Source: Invert match. any Source Address /

Destination: Destination: Invert match. any Destination Address /

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: OpenVPN wizard

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

0% Перемещение...

Меню Firefox (Bases) 20% Перемещение... 08:50

Файл Драва Вид Журнал Закладки Инструменты Справка

192.168.0.31/firewall_rules_edit.php?id=3

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: OpenVPN

Address Family: IPv4

Protocol: Any

Source: Source: Invert match. any Source Address /

Destination: Destination: Invert match. any Destination Address /

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: OpenVPN wizard

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

Rule Information

Tracking ID: 1602449997

Created: 7/24/18 13:01:27 by OpenVPN Wizard

Save

Меню Firefox (Bases) 20% Перемещение... 08:50

The screenshot shows the 'Edit Firewall Rule' page. The 'Action' dropdown is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Interface' dropdown is set to 'LAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'Any'. Under 'Source', the 'Source' dropdown is set to 'Invert match.' and 'LAN net'. Under 'Destination', the 'Destination' dropdown is set to 'any'. In the 'Extra Options' section, the 'Log' checkbox is unchecked. The 'Description' field contains 'Default allow LAN to any rule'. At the bottom, there are 'Advanced Options' and a 'Display Advanced' link.

По желанию можно настроить белый список защиты логина.

The screenshot shows the 'Login Protection' section. The 'Threshold' is set to 30, 'Blocktime' to 120, and 'Detection time' to 1800. A 'Whitelist' section is highlighted with a red oval, containing an 'Address' input field with '128' and the note 'Addresses added to the whitelist will bypass login protection.' Below it are 'Add address' and '+ Add address' buttons. The 'Serial Communications' section includes 'Serial Terminal' (unchecked), 'Serial Speed' (set to 115200), and 'Primary Console' (set to 'Serial Console'). The 'Console Options' section includes 'Console menu' (unchecked) and a 'Save' button. The status bar at the bottom indicates 'pfSense is developed and maintained by Netgate. © ESF 2004-2019 View license.'

Так же по желанию можно выполнять блокировку трафика по протоколу ipv6, при этом, блокируя трафик по протоколу, сам протокол по прежнему остаётся включенным.

IPv6 Options

Allow IPv6 All IPv6 traffic will be blocked by the firewall unless this box is checked. NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

IPv6 over IPv4 Tunneling These options create an RFC 2893 compatible mechanism for IPv4 NAT encapsulation of IPv6 packets, that can be used to tunnel IPv6 packets over IPv4 routing infrastructures. IPv6 firewall rules are also required, to control and pass encapsulated traffic.

Prefer IPv4 over IPv6 Refer to use IPv4 even if IPv6 is available. By default, if IPv6 is configured and a hostname resolves IPv6 and IPv4 addresses, IPv6 will be used. If this option is selected, IPv4 will be preferred over IPv6.

IPv6 DNS entry Do not generate local IPv6 DNS entries for LAN interfaces. If a LAN interface's IPv6 configuration is set to Track, and the tracked interface loses connectivity, it can cause connections to this firewall that were established via hostname to fail. This can happen unintentionally when accessing the firewall by hostname, since by default both IPv4 and IPv6 entries are added to the system's DNS. Enabling this option prevents those IPv6 records from being created.

DHCP6 DUID Raw DUID: As stored in DUID file or seen in firewall logs

By default, the firewall automatically creates a dynamic DUID-LLT which is not saved in the firewall configuration. To ensure that the same DUID is retained by the firewall at all times, enter a DUID in this section. The new DUID will take effect after a reboot or when the WAN interface(s) are reconfigured by the firewall.

If the firewall is configured to use a RAM disk for /var, the best practice is to store a DUID here; otherwise, the DUID will change on each reboot.

Raw DUID

Далее настраиваем имя хоста, его домен и DNS:

System

Hostname pf Name of the firewall host, without domain part

Domain localdomain Do not use 'local' as the final part of the domain (TLD). The 'local' domain is widely used by mDNS (including Avahi and Apple OS X's Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the router uses 'local'. Alternatives such as 'local.lan' or '.mylocal' are safe.

DNS Server Settings

DNS Servers	192.168.1.54	DNS Hostname	none
Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.			
Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).			
Gateway Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.			

Add DNS Server

DNS Server Override Allow DNS server list to be overridden by DHCP/PPP on WAN If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

Disable DNS Forwarder Do not use the DNS Forwarder/DNS Resolver as a DNS server for the firewall By default localhost (127.0.0.1) will be used as the first DNS server where the DNS Forwarder or DNS Resolver is enabled and set to listen on localhost, so the system can use the local DNS service to perform lookups. Checking this box omits localhost from the list of DNS servers in resolv.conf.

Localization

Тип языка: Russian

Разрешаем проверку валидности сертификата:

The screenshot shows the pfSense web interface under the 'System / Advanced / Notifications' tab. The 'Notifications' sub-tab is selected. The configuration page includes fields for E-Mail settings, such as 'E-Mail server', 'SMTP Port of E-Mail server', 'Connection timeout to E-Mail server', and 'From e-mail address'. A section for 'Secure SMTP Connection' contains a checkbox for 'Validate SSL/TLS', which is highlighted with a red oval. Other fields include 'Notification E-Mail auth username (optional)' and 'Notification E-Mail auth password'.

File Edit Bookmarks закладки Инструменты Справка
192.168.0.31/system_advanced_notifications.php
1С:документооборот Login BlackDiver.Net | Orc... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ https://192.168.10.33/ Kyocera Command C... HP Color LaserJet 26... HP Designjet T520 2... http://192.168.10.37/ http://192.168.10.39/
pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help
System / Advanced / Notifications ?
Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications
E-Mail
Disable SMTP Disable SMTP Notifications
Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.
E-Mail server
This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.
SMTP Port of E-Mail server (25)
This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).
Connection timeout to E-Mail server (20)
This is how many seconds it will wait for the SMTP server to connect. Default is 20s.
Secure SMTP Connection Enable SMTP over SSL/TLS
 Validate the SSL/TLS certificate presented by the server
When disabled, the server certificate will not be validated. Encryption will still be used if available, but the identity of the server will not be confirmed.
From e-mail address
This is the e-mail address that will appear in the from field.
Notification E-Mail address
Enter the e-mail address to send email notifications to.
Notification E-Mail auth username (optional)
Enter the e-mail address username for SMTP authentication.
Notification E-Mail auth password Confirmation
Enter the e-mail account password for SMTP authentication.
Меню Bases 24% Переводчик... 08:53

Проверяем настройки системы:

pf.localdomain - System: General Setup - Mozilla Firefox

Файл Дравка Вид Журнал Закладки Инструменты Справка

1С:документооборот... Login BlackDiver.Net | On... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ https://192.168.10.33/ Kyocera Command C... HP Color LaserJet 26... HP Designjet T520 2... http://192.168.10.37/ https://192.168.10.39/

Localization

Timezone: Asia/Yekaterinburg
Select a geographic region name (Continent/Location) to determine the timezone for the firewall.
Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.

Timeservers: 0.pfsense.pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!

Language: English
Choose a language for the webConfigurator

webConfigurator

Theme: pfSense
Choose an alternative css file (if installed) to change the appearance of the webConfigurator. css files are located in /usr/local/www/css/

Top Navigation: Scrolls with page
The fixed option is intended for large screens only.

Hostname in Menu: Default (No hostname)
Replaces the Help menu title in the Navbar with the system hostname or FQDN.

Dashboard Columns: 2

Interfaces Sort: Sort Alphabetically
If selected, lists of interfaces will be sorted by description, otherwise they are listed wan,lan,optn...

Associated Panels Show/Hide

- Available Widgets Show the Available Widgets panel on the Dashboard.
- Log Filter Show the Log Filter panel in System Logs.
- Manage Log Show the Manage Log panel in System Logs.
- Monitoring Settings Show the Settings panel in Status Monitoring.

These options allow certain panels to be automatically hidden on page load. A control is provided in the title bar to un-hide the panel.

Require State Filter: Do not display state table without a filter
By default, the entire state table is displayed when entering Diagnostics > States. This option requires a filter to be entered before the states are displayed. Useful for systems with large state tables.

Left Column Labels: Active
If selected, clicking a label in the left column will select/toggle the first item of the group.

В менеджере пакетов можно рассмотреть перечень доступных (среди них, кстати, присутствует *stunnel*, способный маскировать и шифровать OpenVPN под *https*). Устанавливается банальным нажатием кнопки *Install*, но в текущий момент это не сама суть вопроса, поскольку нам потребуется другой пакет для экспорта настроек клиентов: нам нужен *OpenVPN-client-export*.

pf.localdomain - System: Package Manager: Available Packages - Mozilla Firefox

softflowd 1.2.3 Softflowd is flow-based network traffic analyzer capable of Cisco NetFlow data export. + Install

squid 0.4.44.9 High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. + Install

squidGuard 1.16.18.3 High performance web proxy URL filter. + Install

Status_Traffic_Totals 1.2.4 Traffic Totals page under the Status menu, which will give a total amount of traffic passed In/Out over the period of hours, days, and months. Uses vnStat for data collection. + Install

stunnel 5.50.2 SSL encryption wrapper between remote client and local or remote servers. + Install

sudo 0.3.2 sudo allows delegation of privileges to users in the sudoers file. Commands can be run as other users, such as root. + Install

suricata 4.1.5.2 High Performance Network IDS, IPS and Security Monitoring engine by OISF. + Install

syslog-ng 1.15.2 Syslog-NG syslog server. This service is not intended to replace the default pfSense syslog server but rather acts as an independent syslog server. + Install

Package Dependencies:

- softflowd-0.9.5_1
- squid-3.5.27_3
- c-icap-modules-0.5.3_1
- squidGuard-1.4.15
- vnstat-1.13_1
- stunnel-5.47_1
- sudo-1.8.28
- suricata-4.1.5
- barnyard2-1.13_1
- syslog-ng-3.14.1_1
- logrotate-3.13.0_1

pf.localdomain - System: Package Manager: Installed Packages - Mozilla Firefox

System / Package Manager / Installed Packages

Installed Packages Available Packages

Name	Category	Version	Description	Actions
openvpn-client-export	security	1.4.18_4	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	= Current Remove Information Reinstall Never version available

Package is configured but not (fully) installed or deprecated

pfSense is developed and maintained by Netgate. © ESF 2004–2019 View license.

Далее выставляем параметры AD, тип аутентификации LDAP, открываем на контролере домена tcp-порт 389, если закрыт, создаём группу пользователей pfSense, на которую делегируем полномочия администратора, нажимаем на кнопку Select a container, и выбираем наши DC и OU.

Не забываем внизу нажимать на кнопку «Save»

Создаём «сквозную» группу пользователей, с повышенными привилегиями, аналогичную той, на которую делегированы полномочия в AD.

The screenshot shows the pfSense User Manager Groups page. At the top, there is a navigation bar with links for 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. Below the navigation bar is a breadcrumb trail: 'System / User Manager / Groups'. A red oval highlights the 'Groups' tab, which is currently selected. The main content area displays a table titled 'Groups' with columns: 'Group name', 'Description', 'Member Count', and 'Actions'. The table contains four rows:

Group name	Description	Member Count	Actions
admins	System Administrators	0	
all	All Users	8	
pfSense	Domain Users	6	

At the bottom right of the table, there is a green button labeled '+ Add'.

И так мы добрались до управления пользователями. На сервере psSense это выглядит таким образом:

The screenshot shows the pfSense User Manager Users page. At the top, there is a navigation bar with links for 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. Below the navigation bar is a breadcrumb trail: 'System / User Manager / Users'. A red oval highlights the 'Users' tab, which is currently selected. The main content area displays a table titled 'Users' with columns: 'Username', 'Full name', 'Status', 'Groups', and 'Actions'. The table contains eight rows:

Username	Full name	Status	Groups	Actions
[REDACTED]	[REDACTED]	✓	pfSense	
[REDACTED]	[REDACTED]	✗		
[REDACTED]	[REDACTED]	✓	pfSense	
[REDACTED]	[REDACTED]	✓	pfSense	
[REDACTED]	[REDACTED]	✓	pfSense	
[REDACTED]	[REDACTED]	✗	pfSense	
admin	System Administrator	✓		
[REDACTED]	[REDACTED]	✓	pfSense, pfSense-admins	

At the bottom right of the table, there are three buttons: '+ Add', a green button, and a red button labeled 'Delete'.

Добавление новых пользователей pfSense выглядит примерно так:

The screenshot shows two consecutive screenshots of the pfSense User Manager interface, illustrating the process of creating a new user.

Screenshot 1 (Top): The "User Properties" section is displayed. The "Defined by" field is set to "USER". The "Disabled" checkbox is unchecked. The "Username" field contains "sth". The "Password" field contains "thg". The "Full name" field contains "thg". The "Expiration date" field is empty. The "Custom Settings" checkbox is unchecked. Under "Group membership", the "Not member of" list contains "admins" and "pfSense-admins", and the "Member of" list contains "pfSense". Buttons for "Move to 'Member of' list" and "Move to 'Not member of' list" are visible. A "Create Certificate for User" section is present with a "Descriptive name" field containing "thg".

Screenshot 2 (Bottom): The "Keys" section is displayed. It includes fields for "Authorized SSH Keys" (with a placeholder "Enter authorized SSH keys for this user") and "IPsec Pre-Shared Key". A "Save" button is at the bottom.

При этом создание и хранение может вестись как в Локальной БД, так и в БД, из AD.
На изображении ниже в развертывающемся списке выбрана локальная БД пользователей.

The screenshot shows the pfSense User Manager Settings page. The 'Session timeout' field is set to 4 hours. The 'Authentication Server' is set to 'Local Database'. The 'Auth Refresh Time' is set to 30 seconds. There are 'Save' and 'Save & Test' buttons at the bottom.

По завершении создания нового пользователя в списке доступных сертификатов генерируется назначенный ему сертификат.

Примечание: после удаления пользователя не забывать вычищать из списка лишние сертификаты (они не всегда вычеваются в автоматическом режиме).

The screenshot shows the pfSense Certificate Manager Certificates page. It lists several certificates:

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5b55983b183cc)	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-5b55983b183cc, C=US		Details, Edit, Delete
CA: No Server: Yes		Valid From: Mon, 23 Jul 2018 13:56:27 +0500 Valid Until: Sat, 13 Jan 2024 13:56:27 +0500		
OVPN Server Certificate	[REDACTED]	emailAddress=labuzhskiy@ya.ru, ST=Orenburgskiy region, OU=faktory, O=OOO Tehnopr, L=Orenburg, CN=labuzhskiy, C=RU	OpenVPN Server	Details, Edit, Delete
CA: No Server: Yes		Valid From: Mon, 23 Jul 2018 12:22:25 +0500 Valid Until: Thu, 20 Jul 2028 12:22:25 +0500		
[REDACTED] User Certificate	[REDACTED]	emailAddress=labuzhskiy@ya.ru, ST=Orenburgskiy region, O=OOO Tehnopr, L=Orenburg, CN=labuzhskiy, C=RU	User Cert	Details, Edit, Delete
CA: No Server: Yes		Valid From: Wed, 01 Aug 2018 12:23:42 +0500 Valid Until: Sat, 29 Jul 2028 12:23:42 +0500		
[REDACTED] User Certificate	[REDACTED]	emailAddress=labuzhskiy@ya.ru, ST=Orenburgskiy region, O=OOO Tehnopr, L=Orenburg, CN=Aleksenko M, C=RU	User Cert	Details, Edit, Delete
CA: No Server: No		Valid From: Fri, 24 Aug 2018 10:11:26 +0500 Valid Until: Mon, 21 Aug 2028 10:11:26 +0500		
Dobrynin A User Certificate	Tehnopr	emailAddress=labuzhskiy@ya.ru, ST=Orenburgskiy region, O=OOO Tehnopr, L=Orenburg, CN=Dobrynin A, C=RU	User Cert	Details, Edit, Delete
CA: No Server: No		Valid From: Thu, 20 Sep 2018 10:37:30 +0500 Valid Until: Sun, 17 Sep 2028 10:37:30 +0500		
Zhidkov N User Certificate	Tehnopr	emailAddress=labuzhskiy@ya.ru, ST=Orenburgskiy region, O=OOO Tehnopr, L=Orenburg, CN=Zhidkov N, C=RU	User Cert	Details, Edit, Delete
CA: No Server: No		Valid From: Tue, 09 Oct 2018 09:11:20 +0500 Valid Until: Fri, 06 Oct 2028 09:11:20 +0500		

Внесём изменения в настройки сервера:

The screenshot shows the pfSense OpenVPN Servers list page. The URL is 192.168.0.31/vpn_openvpn_server.php. The page title is "pf.localdomain - VPN: OpenVPN: Servers - Mozilla Firefox". The pfSense logo is at the top left. The main content area has tabs: Servers (selected), Clients, Client Specific Overrides, Wizards, Client Export, Shared Key Export. A table lists one server entry:

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP /	10.8.10.0/24	Crypto: AES-256-CBC/SHAS12 D-H Params: 4096 bits	(tun)	

The screenshot shows the pfSense OpenVPN Servers edit page. The URL is 192.168.0.31/vpn_openvpn_server.php?action=edit&id=0. The page title is "pf.localdomain - VPN: OpenVPN: Servers: Edit - Mozilla Firefox". The pfSense logo is at the top left. The main content area has tabs: Servers (selected), Clients, Client Specific Overrides, Wizards, Client Export, Shared Key Export. A form titled "General Information" contains fields:

- Disabled: Disable this server
- Server mode: Remote Access (SSL/TLS + User Auth)
- Backend for authentication: tehnoprom\labuzhsky (Local Database selected)
- Protocol: UDP IPv4 and IPv6 on all interfaces (multihomed)
- Device mode: tun - Layer 3 Tunnel Mode
- Interface: WAN
- Local port:
- Description: A description may be entered here for administrative reference (not parsed).

The screenshot shows the pfSense OpenVPN Servers edit page. The URL is 192.168.0.31/vpn_openvpn_server.php?action=edit&id=0. The page title is "pf.localdomain - VPN: OpenVPN: Servers: Edit - Mozilla Firefox". The pfSense logo is at the top left. The main content area has tabs: Servers (selected), Clients, Client Specific Overrides, Wizards, Client Export, Shared Key Export. A form titled "General Information" contains fields:

- Disabled: Disable this server
- Server mode: Remote Access (SSL/TLS + User Auth)
- Backend for authentication: tehnoprom\labuzhsky (Local Database selected)
- Protocol: UDP IPv4 and IPv6 on all interfaces (multihomed)
- Device mode: tun - Layer 3 Tunnel Mode
- Interface: WAN
- Local port:
- Description: A description may be entered here for administrative reference (not parsed).

A "Cryptographic Settings" section is present with a "TLS Configuration" subsection:

- Use a TLS Key

A note states: "A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or eavesdropping."

File Edit View Bookmarks Tools Help

1СДокументооборот Login BlackDiver.Net | Orx... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ https://192.168.10.33/ Kyocera Command C... HP Color LaserJet 26... HP Designjet T520 2... http://192.168.10.37/ http://192.168.10.39/

Cryptographic Settings

TLS Configuration	<input checked="" type="checkbox"/> Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
TLS Key	<pre># # 2048 bit OpenVPN static key #-----BEGIN OPENVPN Static Key V1----- c5f25bdb4123c441e7b64cae7e587c439 e27cd3baa923a1aa1a14fc878a4227ee7 -----END OPENVPN Static Key V1-----</pre> <p>Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.</p>
TLS Key Usage Mode	TLS Encryption and Authentication In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
Peer Certificate Authority	Tehnoprrom
Peer Certificate Revocation List	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
Server certificate	OVPN (Server: Yes, CA: Tehnoprrom, In Use)
DH Parameter Length	4096 bit
ECDH Curve	Use Default
Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block)
Enable NCP	<input checked="" type="checkbox"/> Enable Negotiable Cryptographic Parameters Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.

pf.localdomain - VPN: OpenVPN Servers: Edit - Mozilla Firefox

Enable NCP Enable Negotiable Cryptographic Parameters
Check this option to allow OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic Encryption Algorithms from those selected in the NCP Algorithms list below.

NCP Algorithms

AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-GCM (192 bit key, 128 bit block)
AES-192-OFB (192 bit key, 128 bit block)
AES-256-CBC (256 bit key, 128 bit block)
AES-256-CFB (256 bit key, 128 bit block)
AES-256-GCM (256 bit key, 128 bit block)
AES-256-OFB (256 bit key, 128 bit block)

Available NCP Encryption Algorithms
Click to add or remove an algorithm from the list

Allowed NCP Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected NCP Encryption Algorithms is respected by OpenVPN.

Auth digest algorithm SHA512 (512-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto No Hardware Crypto Acceleration

Certificate Depth Two (Client+Intermediate+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching Enforce match
When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

Tunnel Settings

IPv4 Tunnel Network 10.8.10.0/24
This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24).
The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network fe80::/64
This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64).
The -1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

The screenshot shows the 'Tunnel Settings' section of the OpenVPN configuration interface. Key settings include:

- IPv4 Tunnel Network:** 10.8.10.0/24
- IPv6 Tunnel Network:** (empty)
- Redirect IPv4 Gateway:** Force all client-generated IPv4 traffic through the tunnel.
- Redirect IPv6 Gateway:** Force all client-generated IPv6 traffic through the tunnel.
- IPv6 Local network(s):** (empty)
- Concurrent connections:** (empty)
- Compression:** Adaptive LZO Compression [Legacy style, comp-lzo adaptive]
- Push Compression:** Push the selected Compression setting to connecting clients.
- Type-of-Service:** Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
- Inter-client communication:** Allow communication between clients connected to this server
- Duplicate Connection:** Allow multiple concurrent connections from clients using the same Common Name. (This is not generally recommended, but may be needed for some scenarios.)

Теперь внесём изменения в настройки клиентов, оптимизации CPU, и параметры ip-адреса, для внешних клиентских подключений.

The screenshot shows the 'Client Settings' section of the OpenVPN configuration interface. Key settings include:

- Dynamic IP:** Allow connected clients to retain their connections if their IP address changes.
- Topology:** Subnet – One IP address per client in a common subnet
- Advanced Client Settings:**
 - DNS Default Domain:** Provide a default domain name to clients
 - DNS Default Domain:** AD [REDACTED]
 - DNS Server enable:** Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
 - DNS Server 1:** 192.168.1.54
 - DNS Server 2:** (empty)
 - DNS Server 3:** (empty)
 - DNS Server 4:** (empty)
- Block Outside DNS:** Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
- Force DNS cache update:** Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
- NTP Server enable:** Provide an NTP server list to clients
- NetBIOS enable:** Enable NetBIOS over TCP/IP

Файл Правка Вид Журнал Закладки Инструменты Справка

192.168.0.31/vpn_openvpn_server.php?action=edit&id=0

1СДокументооборот Login BlackDiver.Net | On... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ https://192.168.10.33/ Kyocera Command C... HP Color Laserjet 26... HP Designjet T520 2... http://192.168.10.37/ http://192.168.10.39/

If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE:push route10.0.0.1 255.255.255.0

UDP Fast I/O Use fast I/O operations with UDP writes to tun/tap. Experimental.
Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.

Send/Receive Buffer Default
Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KB and test higher and lower values.

Gateway creation Both IPv4 only IPv6 only
If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level 3 (recommended)
Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

More: Only fatal errors
Default through 4: Normal usage range.
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Save

pfSense is developed and maintained by Netgate. © ESF 2004–2019 View license.

Меню Помощь Базы 40% Перемещение... [11.19] 09:05

Файл Правка Вид Журнал Закладки Инструменты Справка

192.168.0.31/vpn_openvpn_export.php

1СДокументооборот Login BlackDiver.Net | On... http://192.168.10.30/ https://192.168.10.31/ https://192.168.10.32/ https://192.168.10.33/ Kyocera Command C... HP Color Laserjet 26... HP Designjet T520 2... http://192.168.10.37/ http://192.168.10.39/

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Server

Remote Access Server Server UDP 443

Client Connection Behavior

Host Name Resolution Other

Host Name 92.***.35
Enter the hostname or IP address the client will use to connect to this server.

Verify Server CN Automatic - Use verify-x509-name (OpenVPN 2.3+)
Where possible
Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.

Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version.

With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.

Block Outside DNS Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client Do not include OpenVPN 2.4 settings in the client configuration.
When using an older client (OpenVPN 2.3.x or earlier), check this option to prevent the exporter from placing known-incompatible settings such as Negotiable Cryptographic Parameters (NCP) into the client configuration.

Use Random Local Port Use a random local source port (lport) for traffic from the client. Without this set, two clients may run concurrently.

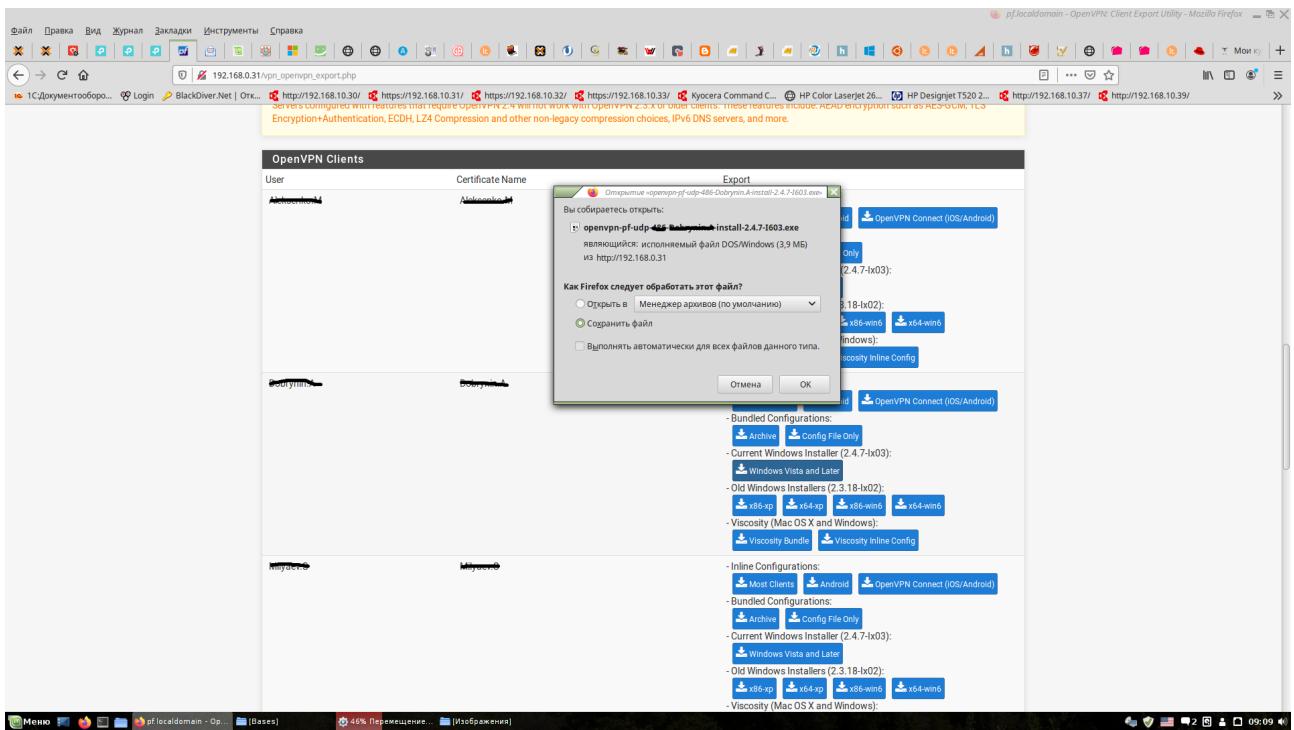
Certificate Export Options

Меню Помощь Базы 41% Перемещение... [11.19] 09:06

ARP-таблица по клиентам:

Так будет выглядеть экспорт клиентов через установленный нами ранее пакет:

Для Microsoft Windows скачивается готовый инсталляционный SFX-архив, включающий в себя все необходимые настройки.



Для Linux платформы скачивается архив в *.zip формате, содержащий все необходимые для настройки файлы.

Во время активных подключений консоль pfSense отображает состояние подключений:

Время запуска	Время окончания	Узел	Пользователь	Описание	Статус
Нояб 26 09:20:19		pve2	labuzhskiy@pam	VM/CT 100 - Консоль	
Нояб 26 05:11:49	Нояб 26 05:12:02	pve2	root@pam	Update package database	Ошибка: command 'apt-get ...'
Нояб 27 05:32:37	Нояб 27 05:32:50	pve2	root@pam	Update package database	Ошибка: command 'apt-get ...'
Нояб 26 02:12:40	Нояб 26 02:12:53	pve2	root@pam	Update package database	Ошибка: command 'apt-get ...'
Нояб 25 06:52:17	Нояб 25 06:52:43	pve2	labuzhskiy@pam	VM/CT 104 - Консоль	OK

На этом наш подготовительный этап завершён, переходим к выполнению поставленной задачи.

1-й сегмент сети:

Картина до подключения:

Здравствуйте, гость. Войти Зарегистрироваться Что дает регистрация? * Напомнить пароль

2 IP

32 Тесты new! 15 VPN Сервисы 5 Софт 48 Провайдеры 6 Забавы 37 Статьи

Ваш IP адрес: 92.***.15.35

Имя вашего компьютера: 92.***.15.35
Операционная система: Microsoft Windows 7
Ваш браузер: Firefox 70.0
Откуда вы: Россия, Оренбург
Ваш провайдер: Радиосвязь
Прокси: Не используется, уточнить?
Защита данных: Отсутствует, исправить?

Сменить IP-адрес

Тесты Сервисы Забавы ПРОКСИ СЕРВИС Krot VPN

Скорость интернет соединения	Проверка анонимности	Время загрузки файла	Объем загружаемого файла
Информация об IP адресе или домене	IP интернет ресурса	Время реакции вашего компьютера	Система управления сайтом (CMS)
Хостинг сайта	Расстояние до сайта	Информация о сайте	Сайты на одном IP
Все домены одного владельца	Доступность сайта	Посещаемость сайта	Наличие IP в СПАМ базах

Ожидание ответа от top-fwz1.mail.ru...

Проверка порта Проверка файла на

картина после подключения:

Здравствуйте, гость. Войти Зарегистрироваться Что дает регистрация? * Напомнить пароль

2 IP

32 Тесты new! 15 VPN Сервисы 5 Софт 48 Провайдеры 6 Забавы 37 Статьи

Ваш IP адрес: 91.***.142.142

Имя вашего компьютера: 91.***.142.142
Операционная система: Microsoft Windows 7
Ваш браузер: Firefox 70.0
Откуда вы: Россия, Оренбург
Ваш провайдер: Дом.ru
Прокси: Не используется, уточнить?
Защита данных: Отсутствует, исправить?

История Сменить IP-адрес

Тесты Сервисы Забавы ПРОКСИ СЕРВИС Krot VPN

Скорость интернет соединения	Проверка анонимности	Время загрузки файла	Объем загружаемого файла
Информация об IP адресе или домене	IP интернет ресурса	Время реакции вашего компьютера	Система управления сайтом (CMS)
Хостинг сайта	Расстояние до сайта	Информация о сайте	Сайты на одном IP
Все домены одного владельца	Доступность сайта	Посещаемость сайта	Наличие IP в СПАМ базах

Передача данных с pagead2.googlesyndication.com...

Проверка порта Проверка файла на

The screenshot shows the Wildberries homepage. At the top, there's a navigation bar with links for 'Здравствуйте, гость.', 'Войти', 'Зарегистрироваться', 'Что такое регистрация?', and 'Напоминать паролю'. Below the navigation is a large purple banner with the Wildberries logo. The main content area displays the text 'Ваш IP адрес: 91.144.139.142' and various system information: 'Имя вашего компьютера: 91.144.139.142', 'Операционная система: Microsoft Windows 7', 'Ваш браузер: Firefox 70.0', 'Откуда вы: Россия, Оренбург', 'Ваш провайдер: Дом.ru', 'Прокси: Не используется, уточнить?', and 'Защита данных: Отсутствует, исправить?'. On the right side, there's a detailed log of network activity from a proxy server, listing numerous entries such as '2019 openVPN 2.4.4 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11]' and '2019 TCP/UDP: Preserving recently used remote address: [AF_INET]'. The log continues with various system messages and connection details.

Как видно из скриншотов выше была выполнена подмена ip-адреса, находясь в другом сегменте сети Internet, на интерфейс *tun0* в момент подключения был назначен новый ip-адрес.

Пример 2:

Картина перед подключением:

A screenshot of a Mozilla Firefox browser window. The title bar reads "Узнать IP адрес - Mozilla Firefox". The toolbar includes standard icons for File, Edit, View, Journal, Bookmarks, Tools, and Help. The address bar shows the URL "https://2ip.ru". A message at the top of the main content area says, "Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее и также рекламу более интересной и подходящей для вас." Below this is a large image of a man working on a laptop by a window. To the right of the image is the text "Нужна Помощь от Бога?" and a quote: "Бог Ответит Тебе. Начни Отношения С Ним Прямо Сейчас." A circular button with a right-pointing arrow is next to the quote. Below the image is the website address "MirStudentov.com". The main navigation bar has links for "Здравствуйте, гость.", "Войти", "Зарегистрироваться", "Что дает регистрация?", "Напомнить пароль", and a "2" badge. Below the navigation bar are links for "IP", "Тесты", "VPN", "Сервисы", "Софтвер", "Провайдеры", "Забавы", and "Статьи". The main content area displays information about the user's IP address: "Ваш IP адрес: 145.255.24.17", "Имя вашего компьютера: 145.255.17.dynamic.o56.ru", "Операционная система: Linux", "Ваш браузер: Firefox 70.0", "Откуда вы: Россия_Орск", "Ваш провайдер: Уфанет", "Прокси: Не используется, уточнить?", and "Защита данных: Отсутствует, исправить?". On the left, there's a sidebar with tabs for "Тесты", "Сервисы", "Забавы", "ПРОКСИ СЕРВИС", and "Krot VPN". Under "Сервисы", there are links for "Скорость интернет соединения", "Проверка анонимности", "Время загрузки файла", "Объем загружаемого файла", "Информация об IP адресе или домене", "IP интернет ресурса", "Время реакции вашего компьютера", "Система управления сайтом (CMS)", "Хостинг сайта", "Расстояние до сайта", "Информация о сайте", "Сайты на одном IP", "Все домены одного", "Доступность сайта", "Посещаемость сайта", and "Наличие IP в СПАМ базах". At the bottom, there's a "Мемо" section and a footer with the text "Узнать IP адрес - Mozilla..." and "30 251 участник". On the right side of the main content area, there's an advertisement for HUAWEI with the text "СКИДКИ до 17 000 ₽" and "ЧЕРНАЯ ПЯТНИЦА", featuring images of a smartphone and a laptop.

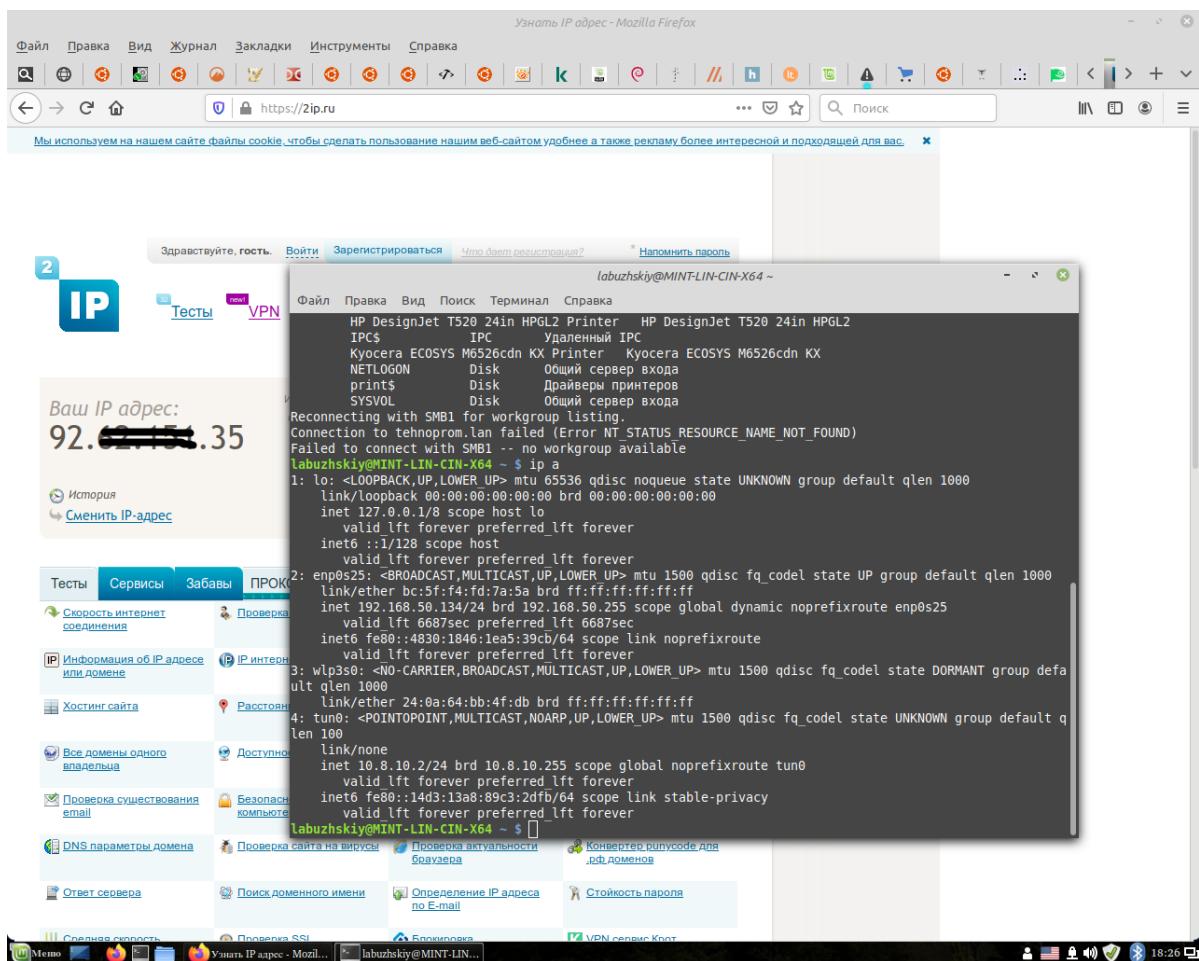
Картина после подключения:

The screenshot shows a Firefox browser window with the URL <https://2ip.ru>. The page displays the IP address 92.***.35 and various system information. Below this, there is a large grid of test options under the 'ПРОКСИ СЕРВИС' tab. The status bar at the bottom indicates 'Прочитано googleads.g.doubleclick.net'.

Файл Правка Вид Журнал Закладки Инструменты Справка
https://2ip.ru Поиск
Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее а также рекламу более интересной и подходящей для вас.
Здравствуйте, гость. Войти Зарегистрироваться Что дает регистрация? Напомнить пароль
IP Тесты VPN Сервисы Софт Провайдеры Забавы Статьи
Ваш IP адрес: 92.***.35
Имя вашего компьютера: 92.***.35
Операционная система: Linux
Ваш браузер: Firefox 70.0
Откуда вы: Россия_Оренбург
Ваш провайдер: Радисвязь
Прокси: Не используется, уточнить? Захотелось, исправить?
История Сменить IP-адрес
Тесты Сервисы Забавы ПРОКСИ СЕРВИС Krot VPN
Скорость интернет соединения Проверка анонимности Время загрузки файла Объем загружаемого файла
Информация об IP адресе или домене IP интернет ресурса Время реакции вашего компьютера Система управления сайтом (CMS)
Хостинг сайта Расстояние до сайта Информация о сайте Сайты на одном IP
Все домены одного владельца Доступность сайта Посещаемость сайта Наличие IP в СПАМ базах
Проверка существования email Безопасность вашего компьютера Проверка порта Проверка файла на вирусы
DNS параметры домена Проверка сайта на вирусы Проверка актуальности браузера Конвертер ip2unicode для .оф доменов
Ответ сервера Поиск доменного имени Определение IP адреса по E-mail Стойкость пароля
Прочитано googleads.g.doubleclick.net Блокировка VPN сервисы Krot
Меню Узнать IP адрес - Mozilla Firefox 18:21

The screenshot shows a Firefox browser window with the URL <https://2ip.ru>. A terminal window is open in the foreground, displaying a password prompt and a listing of shared resources on the network. The status bar at the bottom indicates 'Средняя скорость' and 'labuzhskiy@MINT-LIN-CIN-X64 ~ \$'.

Файл Правка Вид Журнал Закладки Инструменты Справка
https://2ip.ru Поиск
Мы используем на нашем сайте файлы cookie, чтобы сделать пользование нашим веб-сайтом удобнее а также рекламу более интересной и подходящей для вас.
Здравствуйте, гость. Войти Зарегистрироваться Что дает регистрация? Напомнить пароль
IP Тесты VPN Сервисы Забавы ПРОКСИ СЕРВИС Krot VPN
Ваш IP адрес: 92.***.35
История Сменить IP-адрес
Тесты Сервисы Забавы ПРОКСИ СЕРВИС Krot VPN
Скорость интернет соединения Проверка анонимности Время загрузки файла Объем загружаемого файла
Информация об IP адресе или домене IP интернет ресурса Время реакции вашего компьютера Система управления сайтом (CMS)
Хостинг сайта Расстояние до сайта Информация о сайте Сайты на одном IP
Все домены одного владельца Доступность сайта Посещаемость сайта Наличие IP в СПАМ базах
Проверка существования email Безопасность вашего компьютера Проверка порта Проверка файла на вирусы
DNS параметры домена Проверка сайта на вирусы Проверка актуальности браузера Конвертер ip2unicode для .оф доменов
Ответ сервера Поиск доменного имени Определение IP адреса по E-mail Стойкость пароля
labuzhskiy@MINT-LIN-CIN-X64 ~ \$ smbclient -L tehnoprom.lan
WARNING: The "syslog" option is deprecated
Enter TEHNOPROM\labuzhskiy's password:
Sharename Type Comment
----- ----
1DOCuCoresp Disk Удаленный Admin
ADMIN\$ Disk Удаленный Admin
C\$ Disk Стандартный общий ресурс
E\$ Disk Стандартный общий ресурс
HP DesignJet T520 24in HPGL2 Printer HP DesignJet T520 24in HPGL2
IPC\$ IPC Удаленный IPC
Kyocera ECOSYS M6526cdn KX Printer Kyocera ECOSYS M6526cdn KX
NETLOGON Disk Общий сервер входа
print\$ Disk Драйверы принтеров
SYSVOL Disk Общий сервер входа
Reconnecting with SMB1 for workgroup listing.
Connection to tehnoprom.lan failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
labuzhskiy@MINT-LIN-CIN-X64 ~ \$
Средняя скорость labuzhskiy@MINT-LIN-CIN-X64 ~ \$



Настройки подключения:

