

Как настроить выход в интернет из двух (трех...) локальных подсетей в PFSENSE 2.1?

Исходные данные. Машина с тремя сетевыми интерфейсами. Вы установили (не сбросили на дефолт) Pfsense и у вас нет никаких правил установленных пакетов, авторизации и т.п.

**Если у вас на WAN не "белый" он же "реальный" ip адрес, а что-то вида 192.168.0....
Уберите две галочки как показано на рисунке!**

Автор:

02.08.12 10:34 - Последнее обновление 08.10.13 14:26

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help pfSense

Interfaces: WAN

General configuration

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

Type

MAC address
Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

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

MSS
If you enter a value 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: - Show advanced option

Static IP configuration

IP address

Gateway -or- add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Private networks

☒ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

☒ **Block bogon networks**
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

1. Добавим интерфейс. Проверим наличие трех интерфейсов в системе.

192.168.1.1 https://192.168.1.1/interfaces_assign.php

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help pfSense

(assign)

Interface assign network ports

Interface assignments > Interface Groups > Wireless > VLANs > QinQs > PPPs > GRE > GIF > Bridges > LAGG

Interface	Network port
WAN	<input type="text" value="fxp0 (00: d)"/>
LAN	<input type="text" value="fxp1 (00: 5)"/>
OPT1	<input type="text" value="fxp2 (00:)"/>

2. Вспомогательный интерфейс WAN (фреймворк), Второй LAN (опт) (портой)

Автор:

02.08.12 10:34 - Последнее обновление 08.10.13 14:26

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help pfSense

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

Type

MAC address
Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

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

MSS
If you enter a value 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 - Show advanced option

Static IP configuration

IP address /

Gateway -or- add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above.

Private networks

☐ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

☐ **Block bogon networks**
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Автор:

02.08.12 10:34 - Последнее обновление 08.10.13 14:26

System Interfaces Firewall Services VPN Status Diagnostics Help pfSense

Interfaces: OPT1

General configuration

Enable ☒ **Enable Interface**

Description
Enter a description (name) for the interface here.

Type

MAC address
Insert my local MAC address
This field can be used to modify ("spooft") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

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

MSS
If you enter a value 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 - Show advanced option

Static IP configuration

IP address /

Gateway -or- add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add one using the link above

Private networks

☐ **Block private networks**
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

☐ **Block bogon networks**
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

4. Настраиваем DHCP на каждом LAN интерфейсе. Пример ниже:

Автор:

02.08.12 10:34 - Последнее обновление 08.10.13 14:26

System > Interfaces > Firewall > **Services** > VPN > Status > Diagnostics > Help pfSense

Services: DHCP server S L ?

WAN LAN **OPT1**

☒ **Enable DHCP server**

☐ **Deny unknown clients**
If this is checked, only the clients listed below will get DHCP leases from this server.

Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	192.168.1.1 192.168.1.245
WINS servers	
DNS servers	192.168.1.1 8.8.8.8
Gateway	192.168.1.1
Domain name	
Domain search list	
Default lease time	seconds This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP:	

Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP.

Автор:

02.08.12 10:34 - Последнее обновление 08.10.13 14:26

System > Interfaces > Firewall > Services > VPN > Status > Diagnostics > Help pfSense

Services: DHCP server

WAN LAN **OPT1**

☒ **Enable DHCP server on OPT1 interface**

☐ **Deny unknown clients**
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet: 192.168.0.0
Subnet mask: 255.255.255.0
Available range: 192.168.0.1 - 192.168.0.254
Range: 192.168.0.100 to 192.168.0.254

WINS servers:
DNS servers: 192.168.0.1, 8.8.8.8
NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.

Gateway: 192.168.0.1
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.

Domain name:
The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.

Domain search list:
The DHCP server can optionally provide a domain search list.

Default lease time: seconds
This is used for clients that do not ask for a specific expiration time.
The default is 7200 seconds.

Maximum lease time: seconds
This is the maximum lease time for clients that ask for a specific expiration time.
The default is 86400 seconds.

Fallover peer IP:
Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using DHCP.

168.1.1 https://192.168.1.1/firewall_rules.php?if=lan

System > Interfaces > **Firewall** > Services > VPN > Status > Diagnostics > Help pfSense

Firewall: Rules

Floating WAN LAN **OPT1**

Aliases
NAT
Rules
Schedules
Traffic Shaper
Virtual IPs

ID	Proto	Source	Destination	Port	Gateway	Queue	Schedule	Description
1	*	*	LAN Address	80 443	*	*		Anti-Lockout Rule
2	*	LAN net	*	*	*	none		Default allow LAN to any rule

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

Пример ниже:

Автор:

02.08.12 10:34 - Последнее обновление 08.10.13 14:26

System > Interfaces > Firewall > Rules > Edit

Firewall: Rules: Edit

Edit Firewall rule

Action
 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
 Choose on which interface packets must come in to match this rule.

Protocol
 Choose which IP protocol this rule should match.
 Hint: in most cases, you should specify *TCP* here.

Source ☐ **not**
 Use this option to invert the sense of the match.
 Type:
 Address: /

Destination ☐ **not**
 Use this option to invert the sense of the match.
 Type:
 Address: /

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 you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).

Description
 You may enter a description here for your reference.

System > Interfaces > Firewall > NAT > Outbound

Firewall: NAT: Outbound

Port Forward 1:1 **Outbound** NPT

Mode: ☐ Automatic outbound NAT rule generation (IPsec passthrough included) ☒ **Manual Outbound NAT rule generation (ADN - Advanced Outbound NAT)**

Mappings:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input type="checkbox"/>	WAN	192.168.2.0/24	*	*	*	WAN address	*	NO	
<input type="checkbox"/>	WAN	192.168.1.0/24	*	*	*	WAN address	*	NO	

Не забудьте про настройку правил брандмауэра, чтобы не было проблем с доступом к интернету. Обновить

<http://thin.kiev.ua/router-es/50-pfsense/655-wan-2-lan-pfsense-20.html>