

pfSense

WNAM pfSense (<http://www.pfsense.org>) , WNAM 1.2.567. pfSense FreeBSD , x86 , -. pfSense c WNAM pfSense, DHCP, (Wi-Fi) (, Internet) .

! pfSense 2.2., 2.3 .

pfSense Captive Portal. "Services" "Captive Portal". "".

Sense

SystemInterfacesFirewallServicesVPNStatusDiagnosticsGoldHelp

pfSense

Captive Portal: Zones

Zone	Interfaces	Number of users	Description
HomeK18	LAN	0	

() , (LAN, Wi-Fi) ., "", , .

Services: Captive portal: HomeK18



Captive portal(s) **MAC** Allowed IP addresses Allowed Hostnames Vouchers File Manager

☒ Enable captive portal

Interfaces

WAN
LAN

Select the interface(s) to enable for captive portal.

Maximum concurrent connections

per client IP address (0 = no limit)

This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 connections.

Idle timeout

minutes

Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout

minutes

Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Pass-through credits allowed per MAC address

per client MAC address (0 or blank = none)

This setting allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

Waiting period to restore pass-through credits

hours

Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.

Reset waiting period on attempted access

☐ Enable waiting period reset on attempted access

If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.

Logout popup window

☐ Enable logout popup window

If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Pre-authentication redirect URL

http://172.16.130.5:8080/cp/pfsense

Use this field to set \$PORTAL_REDIRECTURLS variable which can be accessed using your custom captive portal index.php page or error pages.

After authentication Redirection URL

If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

Blocked MAC address redirect URL

If you provide a URL here, MAC addresses set to be blocked will be redirect to that URL when attempt to access anything.

Concurrent user logins

☐ Disable concurrent logins

If this option is set, only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.

MAC filtering

☐ Disable MAC filtering

If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Pass-through MAC Auto Entry

☐ Enable Pass-through MAC automatic additions

If this option is set, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry you either have to log in and remove it manually from the MAC tab or send a POST from another system to remove it. If this is enabled, RADIUS MAC authentication cannot be used. Also, the logout window will not be shown.

☐ Enable Pass-through MAC automatic addition with username

If this option is set, with the automatically MAC passthrough entry created the username, used during authentication, will be saved. To remove the passthrough MAC entry you either have to log in and remove it manually from the MAC tab or send a POST from another system to remove it.

Per-user bandwidth restriction

☐ Enable per-user bandwidth restriction

Default download Kbit/s

Default upload Kbit/s

If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty or set to 0 for no limit.

Authentication

☐ No Authentication
☐ Local User Manager / Vouchers

☒ Allow only users/groups with 'Captive portal login' privilege set

☒ RADIUS Authentication

RADIUS Protocol

- ☒ PAP
☐ CHAP_MD5
☐ MSCHAPv1
☐ MSCHAPv2

Primary Authentication Source

Primary RADIUS server

IP address

172.16.130.13

Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Port

Leave this field blank to use the default port (1812).

Shared secret

secret

Leave this field blank to not use a RADIUS shared secret (not recommended).

Secondary RADIUS server

IP address

If you have a second RADIUS server, you can activate it by entering its IP address here.

Port

Shared secret

Secondary Authentication Source

Primary RADIUS server

IP address

If you have a third RADIUS server, you can activate it by entering its IP address here.

Port

Shared secret

Secondary RADIUS server

IP address

If you have a fourth RADIUS server, you can activate it by entering its IP address here.

Port

Shared secret

Accounting

☒ send RADIUS accounting packets

If this is enabled, RADIUS accounting packets will be sent to the primary RADIUS server.

Accounting port

Leave blank to use the default port (1813).

Accounting updates

- ☐ no accounting updates
☐ stop/start accounting
☒ interim update

RADIUS options

Reauthentication

☐ Reauthenticate connected users every minute

If reauthentication is enabled, Access-Requests will be sent to the RADIUS server for each user that is logged in every minute. If an Access-Reject is received for a user, that user is disconnected from the captive portal immediately.

RADIUS MAC authentication

☐ Enable RADIUS MAC authentication

If this option is enabled, the captive portal will try to authenticate users by sending their MAC address as the username and the password entered below to the RADIUS server.

MAC authentication secret

password

RADIUS NAS IP attribute

WAN - 172.16.130.4

Choose the IP to use for calling station attribute.

Session-Timeout

☒ Use RADIUS Session-Timeout attributes

When this is enabled, clients will be disconnected after the amount of time retrieved from the RADIUS Session-

Timeout attribute.

Type
 If RADIUS type is set to Cisco, in Access-Requests the value of Calling-Station-Id will be set to the client's IP address and the Called-Station-Id to the client's MAC address. Default behavior is Calling-Station-Id = client's MAC address and Called-Station-Id = pfSense's WAN IP address.

Accounting Style ☐ **Invert Acct-Input-Octets and Acct-Output-Octets**
 When this is enabled, data counts for RADIUS accounting packets will be taken from the client perspective, not the NAS. Acct-Input-Octets will represent download, and Acct-Output-Octets will represent upload.

NAS Identifier
 Specify a NAS identifier to override the default value (pfSense.k18.netams.com)

MAC address format
 This option changes the MAC address format used in the whole RADIUS system. Change this if you also need to change the username format for RADIUS MAC authentication.
 default: 00:11:22:33:44:55
 singledash: 001122-334455
 ieth: 00-11-22-33-44-55
 cisco: 0011.2233.4455
 unformatted: 001122334455

HTTPS login ☐ **Enable HTTPS login**
 If enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name
 This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL Certificate
 webConfigurator default (56a90c4cdd495)

Disable HTTPS forwards ☐ **Disable HTTPS forwards**
 If this option is set, attempts to connect to SSL/HTTPS (Port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

Portal page contents Файл не выбран
 View current page
 Download current page
 Restore default portal page
 Upload an HTML/PHP file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "/>

Interfaces	LAN - ,
Idle timeout	- (,)
Hard timeout	- . ""

Pre-authentication redirect URL	WNAM, : http://_:cp/pfsense , http://10.200.0.2/cp/pfsense
Per-user bandwidth restriction	(/), (Enable per-user bandwidth restriction), . WNAM ("")
Authentication	RADIUS Authentication - RADIUS Protocol - PAP
Primary RADIUS server - IP address	IP- WNAM, , 10.200.0.2
Primary RADIUS server - Shared secret	RADIUS-, /etc/freeradius/clients.conf WNAM
Accounting	send RADIUS accounting packets
Accounting updates	interim update
RADIUS NAS IP attribute	WAN, ()
Session-Timeout	Use RADIUS Session-Timeout attributes
Type	default
MAC address format	default
Portal page contents	: http://www.netams.com/files/wnam/misc/index-pfsense.php , index.php . pfSense HTTP- WNAM

, (WNAM), index.php, ("site-id"), WNAM. (- HomeK18). (), WNAM. , pfSense.
pfSense , DNS- (- Google 8.8.8.8) WNAM (: 172.16.130.5).

Services: Captive portal: HomeK18

Captive portal(s)MACAllowed IP addressesAllowed HostnamesVouchersFile Manager

IP address	Description
172.16.130.5	
8.8.8.8	

Note:

Adding allowed IP addresses will allow IP access to/from these addresses through the captive portal without being taken to the portal page. This can be used for a web server serving images for the portal page or a DNS server on another network, for example.

() WNAM NetFlow. **softflowd** (pfSense). .

softflowd: Settings



General Settings

Interface	LAN WAN loopback Pick an interface from which to collect netflow data. A separate instance of softflowd will be launched for each interface.
Host	172.16.130.13 Specify the host to which datagrams will be sent.
Port	20002 Enter the port to which datagrams will be sent.
Max Flows	Specify the maximum number of flows to concurrently track before older flows are expired. Default: 8192.
Hop Limit	Set the IPv4 TTL or the IPv6 hop limit to hoplimit. softflowd will use the default system TTL when exporting flows to a unicast host. When exporting to a multicast group, the default TTL will be 1 (i.e. link-local).
Netflow version	5 Select the desired version of the NetFlow protocol.
Flow Tracking Level	Full Specify which flow elements softflowd should be used to define a flow. track_level may be one of: "full" (track everything in the flow, the default), "proto" (track source and destination addresses and protocol), or "ip" (only track source and destination addresses). Selecting either of the latter options will produce flows with less information in them (e.g. TCP/UDP ports will not be recorded). This will cause flows to be consolidated, reducing the quantity of output and CPU load that softflowd will place on the system at the cost of some detail being lost.

Timeout Values

General	300 (Seconds) This is the general timeout applied to all traffic unless overridden by one of the other timeouts.
Maximum Lifetime	600 (Seconds) This is the maximum lifetime that a flow may exist for. All flows are forcibly expired when they pass maxlife seconds. To disable this feature, specify a maxlife of 0.
Expire Interval	30 (Seconds) Specify the interval between expiry checks. Increase this to group more flows into a NetFlow packet. To disable this feature, specify a expire of 0.
TCP	300 (Seconds) This is the general TCP timeout, applied to open TCP connections.
TCP RST	20 (Seconds) This timeout is applied to a TCP connection when a RST packet has been sent by one or both endpoints.
TCP FIN	10 (Seconds) This timeout is applied to a TCP connection when a FIN packet has been sent by both endpoints.
UDP	300 (Seconds) This is the general UDP timeout, applied to all UDP connections.

Save

(LAN), IP- WAN, (20002), (5), (full), . softflowd "Status" "Services".



, RADIUS Accounting-Interim, () - NetFlow.

WNAM (), 5 (pfSense - 1).

WNAM IP- , pfSense DHCP- :

1. DHCP- , Web- DHCP- .
2. (shell) pfSense :
 - a. pkg bootstrap;

- b. `pkg install perl5;`
 - c. `pkg install p5-IO-Socket-IP;`
 - d. `pkg install joe.`
3. - `WNAM /usr/local/bin/joe /usr/local/bin/wnam-dhcpd-bridge.pl:`

```
#!/usr/local/bin/perl

use constant WNAM_HOST => "172.16.130.5";

use IO::Socket::INET;

$_ = 1;

my $sock = new IO::Socket::INET(PeerAddr => WNAM_HOST, PeerPort => 20001, Proto => 'tcp', Timeout => 0.5) or undef $sock;

if (defined $sock) {
    if (defined $ARGV[0]){
        my $type = $ARGV[0];
        my $ip = $ARGV[1];
        my $mac = uc $ARGV[2];
        my $name = $ARGV[3];
        if (defined $type and defined $ip and defined $mac) {
            print $sock "DHCP type=$type ip=$ip mac=$mac name=$name\n";
        }
    }
}
```

4. :

```
chmod +x /usr/local/bin/wnam-dhcpd-bridge.pl
```

5. DHCP: `/usr/local/bin/joe /var/dhcpd/etc/dhcpd.conf` :

```
on commit {
    set clip = binary-to-ascii(10, 8, ".", leased-address);
    set clhw = binary-to-ascii(16, 8, ":", substring(hardware, 1, 6));
    set clhost = pick-first-value(host-decl-name, option fqdn.hostname, option
host-name, "");
    execute("/usr/local/bin/wnam-dhcpd-bridge.pl", "commit", clip, clhw, clhost);
}
```

6. DHCP: "Services - DHCP Server".

pfSense WNAM (" "), (WAN) pfSense. .

Изменение сервера доступа

Параметры

RADIUS

SNMP/TACACS+

Категории

Клиент

Тип

pfSense

Имя устройства

IP адрес (NAS-IP-Address)

172.16.130.4

Внешний IP адрес

192.168.1.1

Местоположение

TEST Location

Комментарий

Логин ?

Пароль ?

☒Использовать счетчики аккаунтинга

☒Менять местами счетчики приёма/передачи

☒Определять имена устройств абонентов

☒Принимать детализацию потоков NetFlow

получено 0 записей

получено 0 записей

Вкл.

Сохранить изменения

Закреть

!

IP-, pfSense () RADIUS- .

9. :

```
pkg add http://pkg.freebsd.org/freebsd:10:x86:64/release\_3/All/nano-2.4.3.txz
```

:

```
[2.3.2-RELEASE][admin@pfsense.k18.netams.com]/etc/inc: nano /usr/local/captiveportal/radius_authentication.inc
```

```
// Extra data to identify the client and nas
$rauth->putAttribute(RADIUS_FRAMED_IP_ADDRESS, $clientip, addr);
$rauth->putAttribute(RADIUS_CALLED_STATION_ID, $calledstationid);
$rauth->putAttribute(RADIUS_CALLING_STATION_ID, $callingstationid);
$rauth->putVendorAttribute(14122, 1, "9");
```

```
// Send request
$result = $rauth->send();
```

```
:
```

```
[2.3.2-RELEASE][admin@pfsense.k18.netams.com]/etc/inc: nano /usr/local/captiveportal/radius_accounting.inc
```

```
$racct->putAttribute(RADIUS_FRAMED_IP_ADDRESS, $clientip, "addr");
$racct->putAttribute(RADIUS_CALLED_STATION_ID, $calledstationid);
$racct->putAttribute(RADIUS_CALLING_STATION_ID, $callingstationid);
$racct->putVendorAttribute(14122, 1, "9");
```

```
// Send request
$result = $racct->send();
```

```
// Evaluation of the response
```

- RADIUS- :

```
rad_recv: Access-Request packet from host 172.16.130.4 port 40167, id=96,
length=138
NAS-IP-Address = 172.16.130.4
NAS-Identifier = "pfsense"
User-Name = "4C:57:CA:2C:0F:4C"
User-Password = "password"
Service-Type = Login-User
NAS-Port-Type = Ethernet
NAS-Port = 2042
Framed-IP-Address = 172.16.70.48
Called-Station-Id = "172.16.130.4"
Calling-Station-Id = "4c:57:ca:2c:0f:4c"
WISPr-Location-ID = "9"
# Executing section authorize from file /etc/freeradius/sites-enabled/default
+group authorize {
++[preprocess] = ok
[pap] WARNING! No "known good" password found for the user. Authentication may
fail because of this.
++[pap] = noop
++[chap] = noop
rlm_perl: WNAME Q: AUTH NAS-Port-Type=Ethernet Called-Station-Id=172.16.130.4 NAS-
IP-Address=172.16.130.4 Calling-Station-Id=4c:57:ca:2c:0f:4c Framed-IP-
Address=172.16.70.48 NAS-Identifier=pfsense User-Name=4C:57:CA:2C:0F:4C User-
Password=password Service-Type=Login-User WISPr-Location-ID=9 NAS-Port=2042
rlm_perl: RECV: IO::Socket::INET=GLOBAL(0x1456770)
rlm_perl: WNAME A: OK Acct-Interim-Interval=300 Session-Timeout=300 (48)
rlm_perl: authorize reply: .OK.
rlm_perl: Added pair NAS-Port-Type = Ethernet
rlm_perl: Added pair Called-Station-Id = 172.16.130.4
rlm_perl: Added pair NAS-IP-Address = 172.16.130.4
rlm_perl: Added pair Calling-Station-Id = 4c:57:ca:2c:0f:4c
rlm_perl: Added pair Framed-IP-Address = 172.16.70.48
rlm_perl: Added pair NAS-Identifier = pfsense
rlm_perl: Added pair User-Name = 4C:57:CA:2C:0F:4C
rlm_perl: Added pair User-Password = password
rlm_perl: Added pair Service-Type = Login-User
rlm_perl: Added pair WISPr-Location-ID = 9
rlm_perl: Added pair NAS-Port = 2042
rlm_perl: Added pair Acct-Interim-Interval = 300
rlm_perl: Added pair Session-Timeout = 300
rlm_perl: Added pair Cleartext-Password = password
rlm_perl: Added pair Auth-Type = PAP
++[perl] = ok
+} # group authorize = ok
Found Auth-Type = PAP
```

```

# Executing group from file /etc/freeradius/sites-enabled/default
+group PAP {
[pap] login attempt with password "password"
[pap] Using clear text password "password"
[pap] User authenticated successfully
++[pap] = ok
+} # group PAP = ok
WARNING: Empty post-auth section. Using default return values.
# Executing section post-auth from file /etc/freeradius/sites-enabled/default
Sending Access-Accept of id 96 to 172.16.130.4 port 40167
Acct-Interim-Interval += 300
Session-Timeout += 300
Finished request 36.
Going to the next request
Waking up in 4.9 seconds.

rad_recv: Accounting-Request packet from host 172.16.130.4 port 64326, id=19,
length=159
NAS-IP-Address = 172.16.130.4
NAS-Identifier = "pfsense"
User-Name = "4C:57:CA:2C:0F:4C"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
NAS-IP-Address = 172.16.130.4
NAS-Identifier = "pfsense"
NAS-Port-Type = Ethernet
NAS-Port = 2042
Acct-Session-Id = "214606a2575e53cd"
Framed-IP-Address = 172.16.70.48
Called-Station-Id = "172.16.130.4"
Calling-Station-Id = "4c:57:ca:2c:0f:4c"
WISPr-Location-ID = "9"
# Executing section preacct from file /etc/freeradius/sites-enabled/default
+group preacct {
++[preprocess] = ok
[acct_unique] Hashing 'NAS-Port = 2042,NAS-Identifier = "pfsense",NAS-IP-Address
= 172.16.130.4,Acct-Session-Id = "214606a2575e53cd",User-Name = "4C:57:CA:2C:0F:
4C"'
[acct_unique] Acct-Unique-Session-ID = "5e89ff48449fd085".
++[acct_unique] = ok
+} # group preacct = ok
# Executing section accounting from file /etc/freeradius/sites-enabled/default
+group accounting {
[detail] expand: %{Packet-Src-IP-Address} -> 172.16.130.4
[detail] expand: /var/log/freeradius/radacct/%{Packet-Src-IP-Address}:-%
{Packet-Src-IPv6-Address}}/detail-%Y%m%d -> /var/log/freeradius/radacct/172.
16.130.4/detail-20170209
[detail] /var/log/freeradius/radacct/%{Packet-Src-IP-Address}:-%{Packet-Src-
IPv6-Address}}/detail-%Y%m%d expands to /var/log/freeradius/radacct/172.16.130.4
/detail-20170209
[detail] expand: %t -> Thu Feb 9 19:51:29 2017
++[detail] = ok
[radutmp] expand: /var/log/freeradius/radutmp -> /var/log/freeradius/radutmp
[radutmp] expand: %{User-Name} -> 4C:57:CA:2C:0F:4C
++[radutmp] = ok
rlm_perl: WNAME Q: ACCT NAS-Port-Type=Ethernet Called-Station-Id=172.16.130.4
Acct-Session-Id=214606a2575e53cd Acct-Status-Type=Start NAS-IP-Address=172.
16.130.4 Calling-Station-Id=4c:57:ca:2c:0f:4c Framed-IP-Address=172.16.70.48 NAS-
Identifier=pfsense Acct-Authentic=RADIUS User-Name=4C:57:CA:2C:0F:4C WISPr-
Location-ID=9 NAS-Port=2042 Acct-Unique-Session-Id=5e89ff48449fd085
rlm_perl: RECV: IO::Socket::INET=GLOBAL(0x1456770)
rlm_perl: WNAME A: OK (2)
rlm_perl: Added pair NAS-Port-Type = Ethernet
rlm_perl: Added pair Called-Station-Id = 172.16.130.4
rlm_perl: Added pair Acct-Session-Id = 214606a2575e53cd
rlm_perl: Added pair Acct-Status-Type = Start
rlm_perl: Added pair NAS-IP-Address = 172.16.130.4
rlm_perl: Added pair NAS-IP-Address = 172.16.130.4
rlm_perl: Added pair Calling-Station-Id = 4c:57:ca:2c:0f:4c
rlm_perl: Added pair Framed-IP-Address = 172.16.70.48

```

```
rlm_perl: Added pair NAS-Identifier = pfsense
rlm_perl: Added pair NAS-Identifier = pfsense
rlm_perl: Added pair Acct-Authentic = RADIUS
rlm_perl: Added pair User-Name = 4C:57:CA:2C:0F:4C
rlm_perl: Added pair WISPr-Location-ID = 9
rlm_perl: Added pair NAS-Port = 2042
rlm_perl: Added pair Acct-Unique-Session-Id = 5e89ff48449fd085
++[perl] = ok
[attr_filter.accounting_response] expand: %{User-Name} -> 4C:57:CA:2C:0F:4C
attr_filter: Matched entry DEFAULT at line 12
++[attr_filter.accounting_response] = updated
+} # group accounting = updated
Sending Accounting-Response of id 19 to 172.16.130.4 port 64326
Finished request 37.
Cleaning up request 37 ID 19 with timestamp +1486
Going to the next request
Waking up in 4.9 seconds.
Cleaning up request 36 ID 96 with timestamp +1486
Ready to process requests.
```