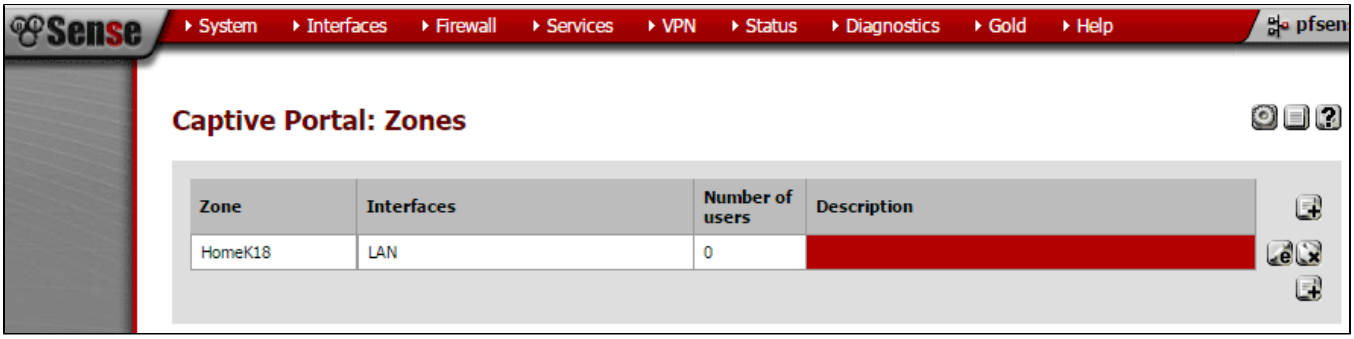
pfSense

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". "".



() , (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 $PORTAL_REDIRURL$ 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

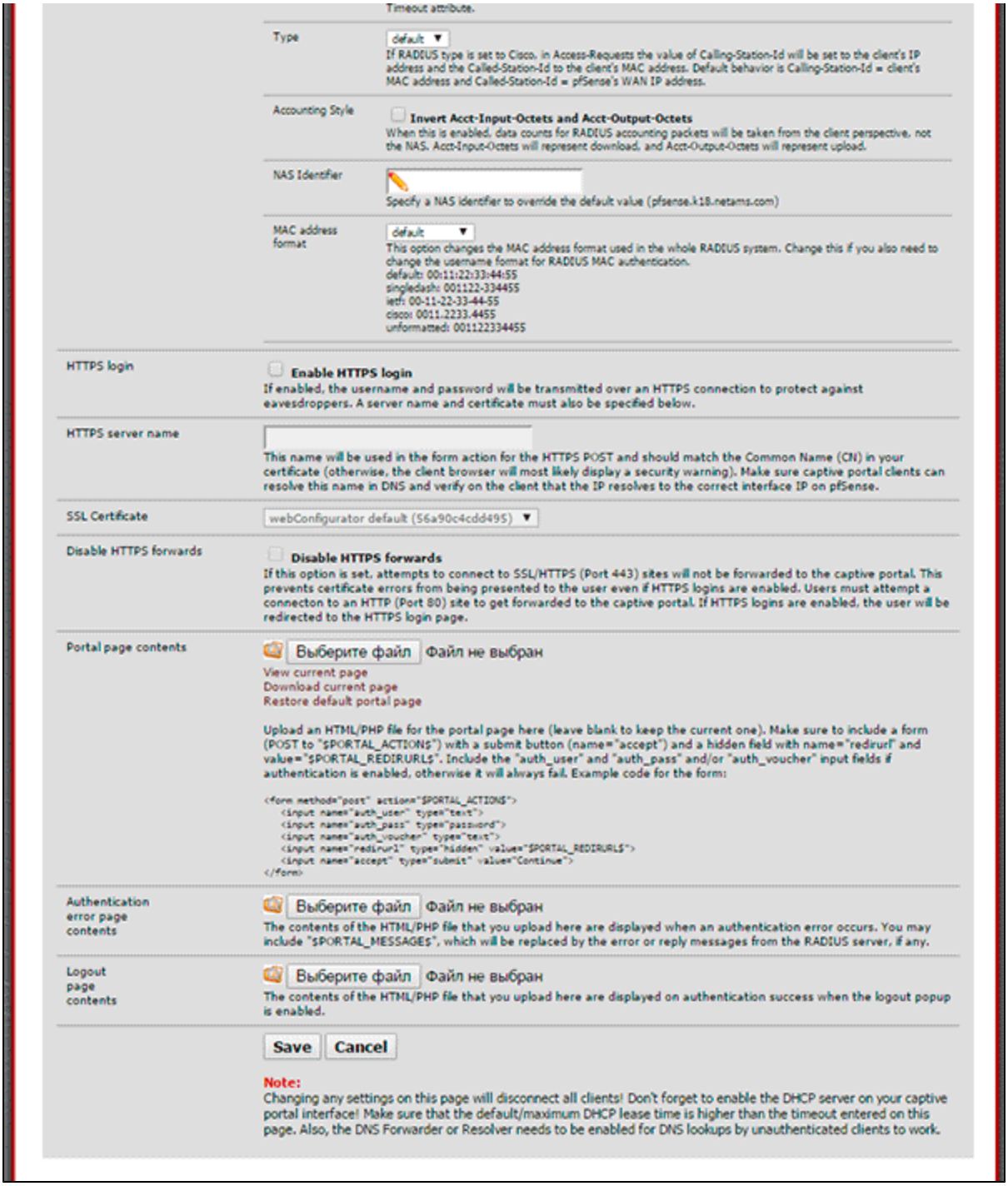
Reauthentication
Reauthenticate connected users every minute
If reauthentication is enabled, Access-Requests will be sent to the RADIUS server for each user that is logged in every minute. If an Access-Reject is received for a user, that user is disconnected from the captive portal immediately.

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-



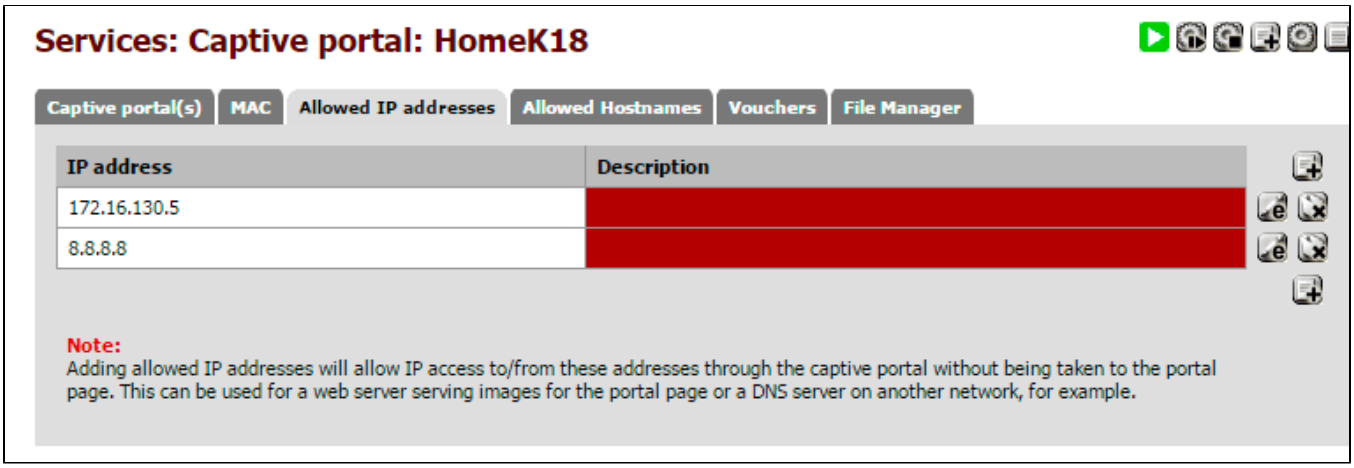
, .

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

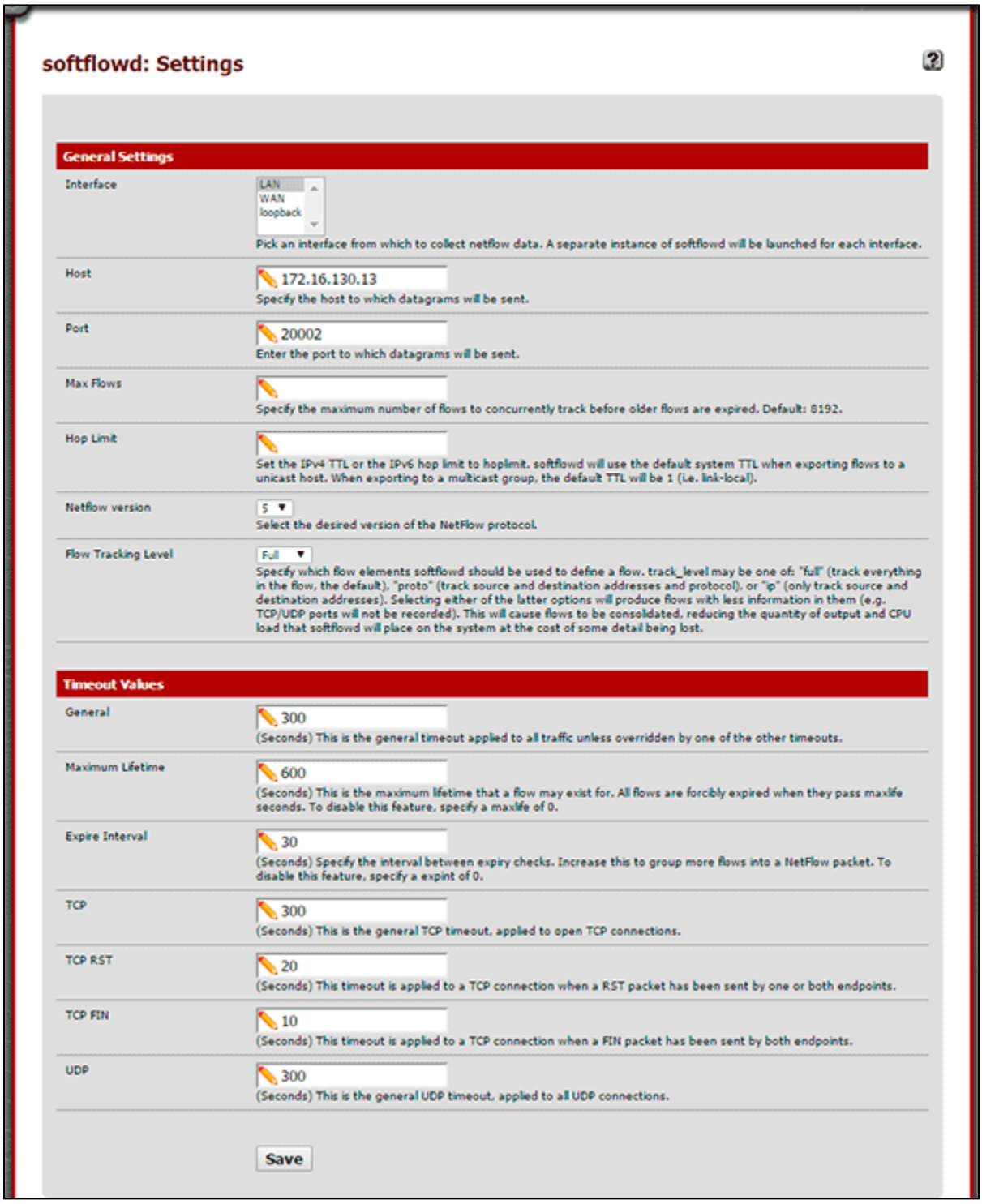
Pre-authentication redirect URL	WNAM, : *http://_:/cp/pfsense* , http://10.200.0.2/cp/pfsense
Per-user bandwidth restriction	(/), (Enable per-user bandwidth restriction), . WNAM ("")
Authentication	RADIUS Authentication - RADIUS Protocol - PAP
Primary RADIUS server - IP address	IP- WNAM, , 10.200.0.2
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).



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



(LAN), IP- WNAM, (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. :

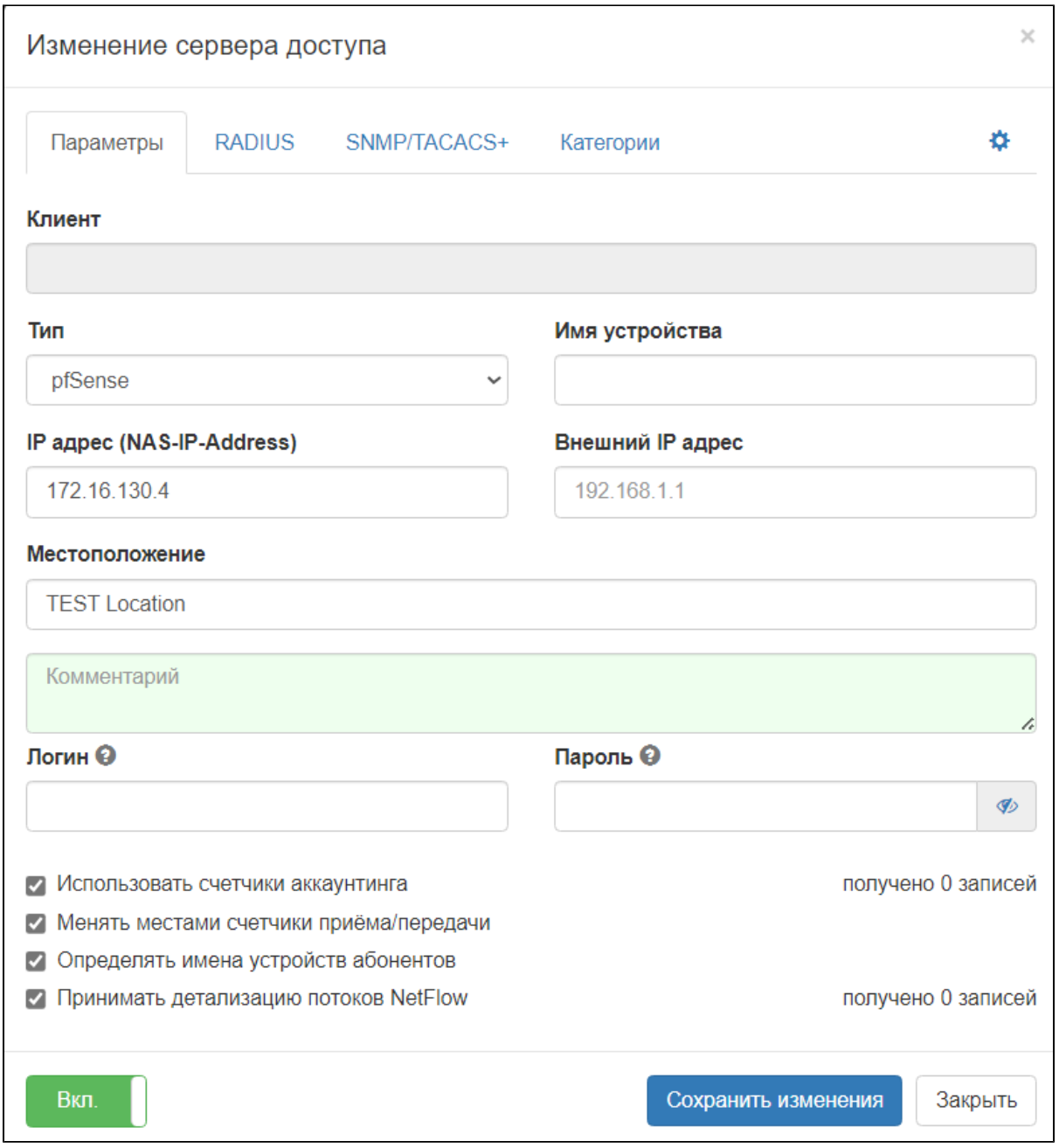
```
chmod +x /usr/local/bin/wnam-dhcpd-bridge.pl
```

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".

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



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: WNAM 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=GLOB(0x1456770)
rlm_perl: WNAM 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: WNAM 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=GLOB(0x1456770)
rlm_perl: WNAM 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.
```