????

- OpenVPN (pfSense 2.0)

?? OpenVPN ??????????????????(Windows ? Linux)???????????????????????? Linux ?????????

??? Linux?????? OpenVPN ???
http://openvpn.net/index.php/downloads.html

$wget http://openvpn.net/release/openvpn-2.0.9.tar.gz
$tar xzf openvpn-2.0.9.tar.gz
$cd openvpn-2.0.9/
$cd easy-rsa/
$vi vars

reference to undefined name 'syntax' Exception of type 'MindTouch.Deki.Script.Runtime.DekiScriptUndefinedNameException' was thrown. (click for details)
???????????

$source ./vars
$./clean-all
$./build-ca

```
 .....
......
Country Name (2 letter code) [TW]:(? Enter)
State or Province Name (full name) [ALANG]:(? Enter)
Locality Name (eg, city) [HsinChu]:(? Enter)
Organization Name (eg, company) [pfSense-VPN]:(? Enter)
Organizational Unit Name (eg, section) []:(? Enter)
Common Name (eg, your name or your server's hostname) []:alang-pfsense
Email Address [alang@myhost.mydomain]:(? Enter)
```

??Common Name ????

$./build-key-server server

```
....
....
Country Name (2 letter code) [TW]:(? Enter)
State or Province Name (full name) [ALANG]:(? Enter)
Locality Name (eg, city) [HsinChu]:(? Enter)
Organization Name (eg, company) [pfSense-VPN]:(? Enter)
Organizational Unit Name (eg, section) []:(? Enter)
Common Name (eg, your name or your server's hostname) []:server
Email Address [alang@myhost.mydomain]:(? Enter)
...
```

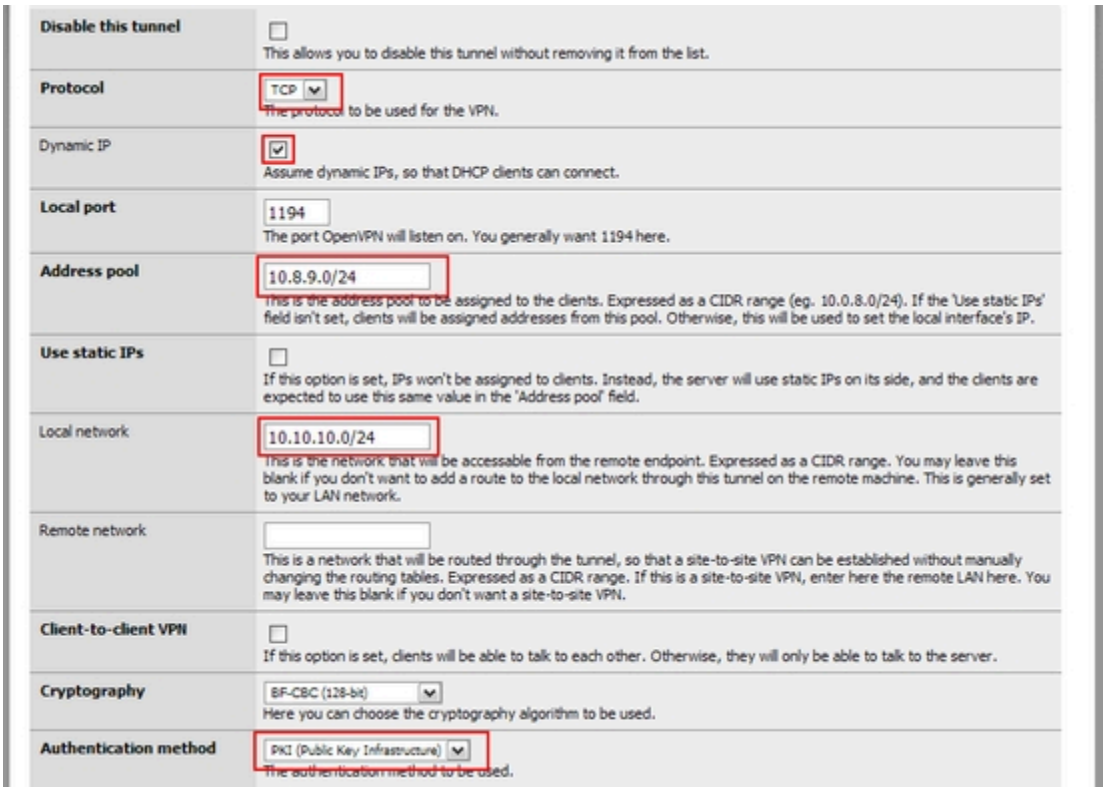
```
...
A challenge password []:(? Enter)
An optional company name []:(? Enter)
...
...
Sign the certificate? [y/n]:y
...
1 out of 1 certificate requests certified, commit? [y/n]y
```

$./build-dh
$./build-key pfsense-client

```
 ..
...
Country Name (2 letter code) [TW]:(? Enter)
State or Province Name (full name) [ALANG]:(? Enter)
Locality Name (eg, city) [HsinChu]:(? Enter)
Organization Name (eg, company) [pfSense-VPN]:(? Enter)
Organizational Unit Name (eg, section) []:(? Enter)
Common Name (eg, your name or your server's hostname) []:client
Email Address [alang@myhost.mydomain]:(? Enter)
...
...
A challenge password []:(? Enter)
An optional company name []:(? Enter)
...
...
Sign the certificate? [y/n]:y
...
1 out of 1 certificate requests certified, commit? [y/n]y
```

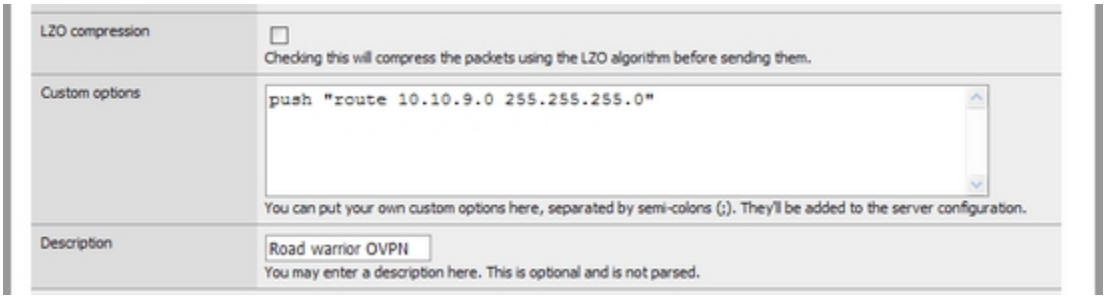
???????????????????????????????? keys ????????
ca.crt
ca.key
dh{xxx}.pem
server.crt
server.key
pfsense-client.crt
pfsense-client.key

????????????????????? 0 ?????????????????????? ?? pfSense ?????????Firewall??OpenVPN??Server??????????

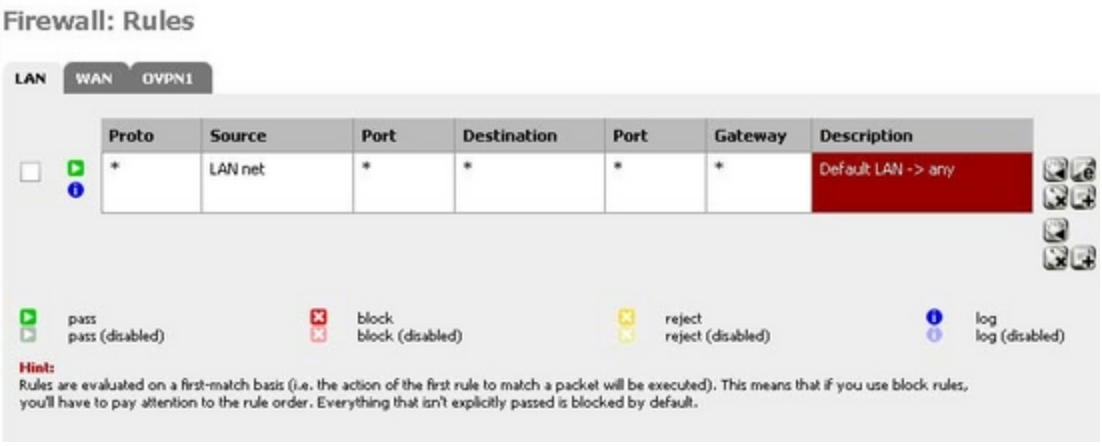


Protocol = TCP
Dynamic IP = yes
Address Pool = ?? VPN Client ??????????????????LAN/WAN/DMZ/LAN2?
Local network = ??????????? LAN?????????VPN ?????????????
Authentication method = PKI ?????????????????????????? Linux ???????????? cat $cat ca.crt ????? -----BEGIN CERTIFICATE----- ? -----END CERTIFICATE---- ???????? ??????

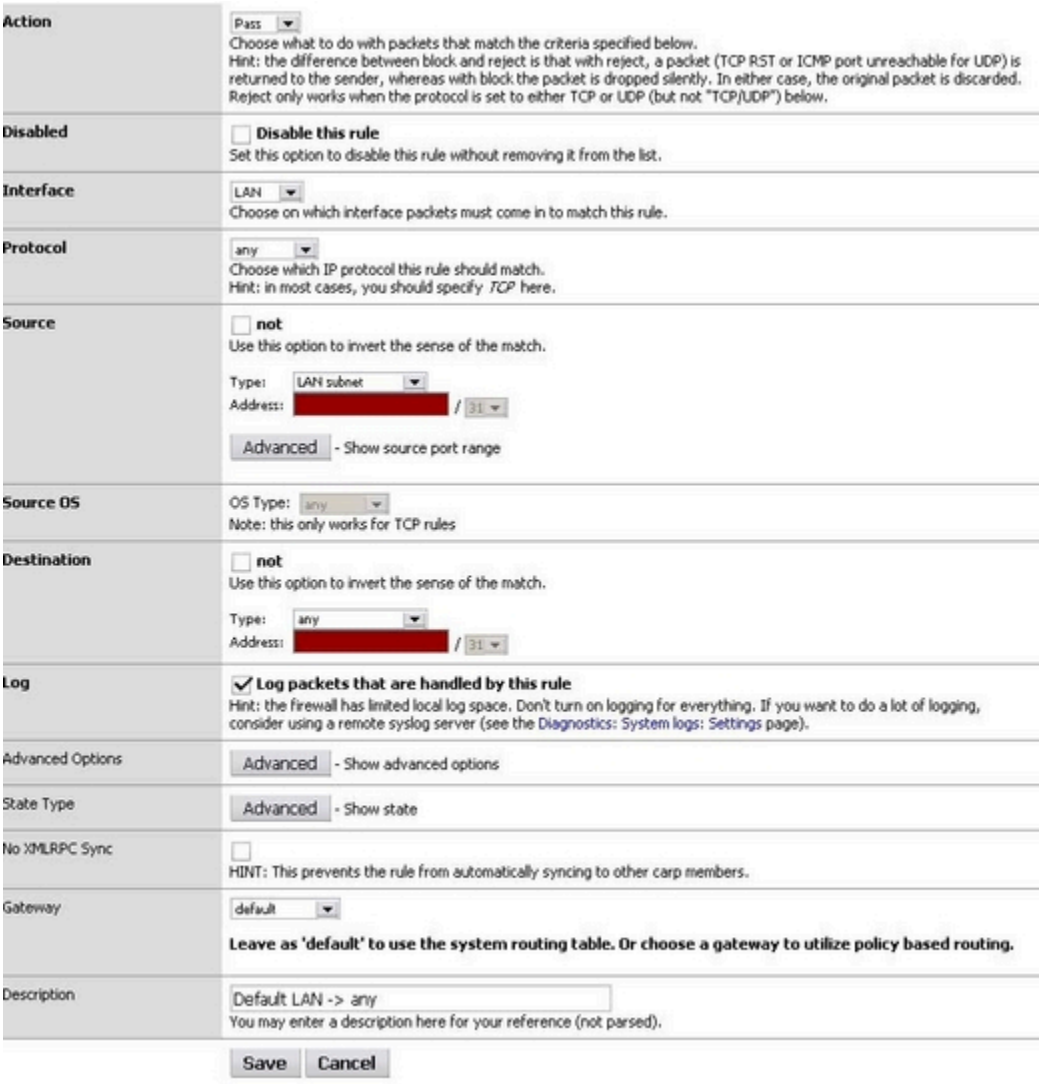
LZO compression = ????????????????????????????
Custom options = ????????????? DMZ ? LAN2 ????????? VPN Client ???????????????? LAN2 ? 10.10.9.0/24 ?? ????
push "route 10.10.9.0 255.255.255.0"
????????????????



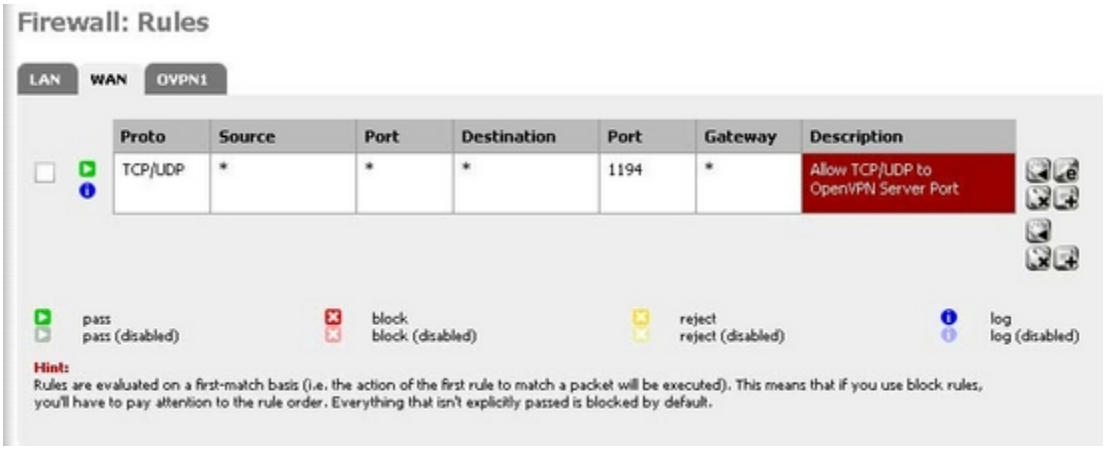
???????? LAN & WAN? ? LAN ???????


Firewall: Rules
LAN
WAN
OVPN1
Proto
Source
Port
Destination
Port
Gateway
Description
*
LAN net
*
*
*
*
Default LAN -> any
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.

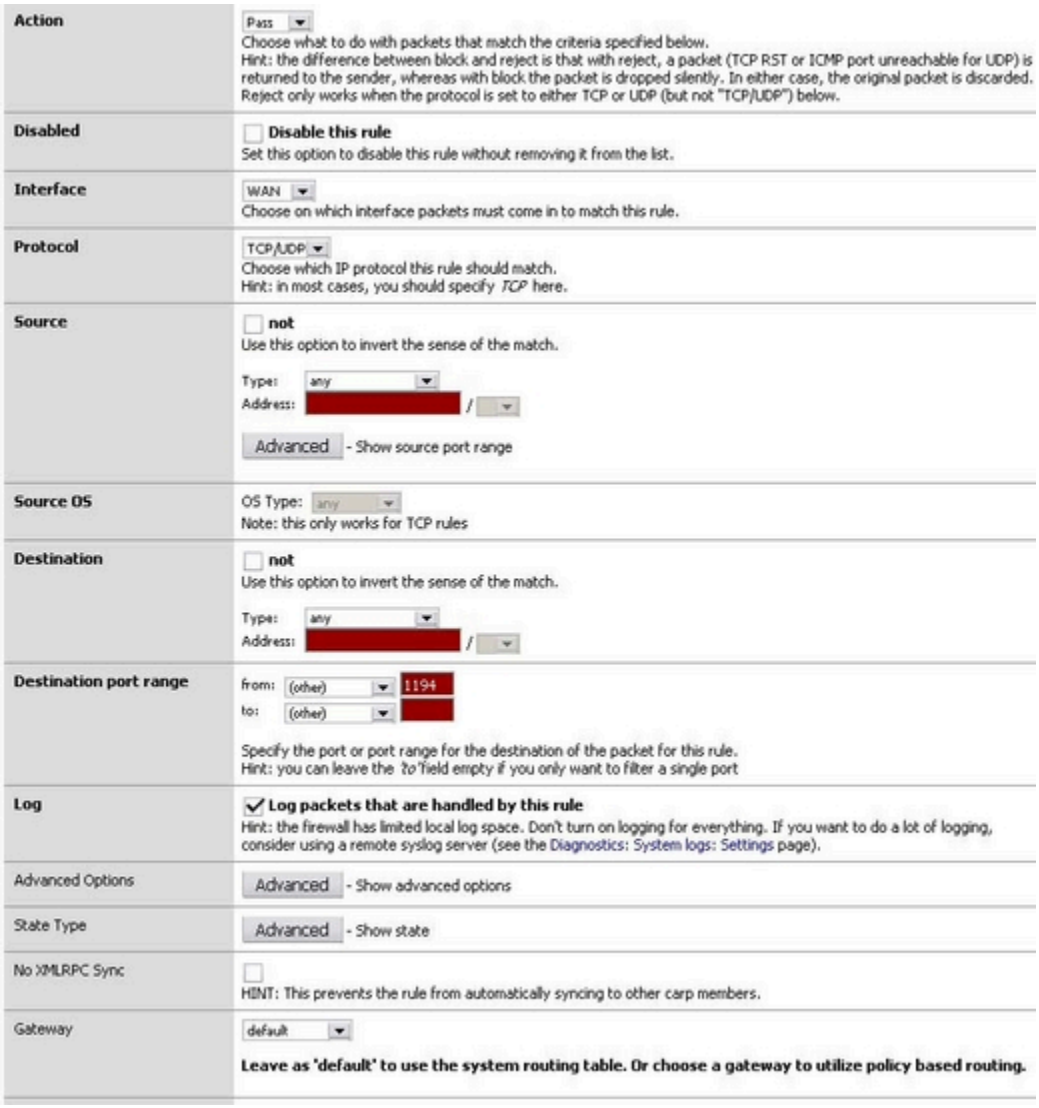
??????????


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. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
LAN
Choose on which interface packets must come in to match this rule.
Protocol
any
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:
LAN subnet
Address:
/
31
Advanced
- Show source port range
Source OS
OS Type:
any
Note: this only works for TCP rules
Destination
not
Use this option to invert the sense of the match.
Type:
any
Address:
/
31
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).
Advanced Options
Advanced
- Show advanced options
State Type
Advanced
- Show state
No XMLRPC Sync
HINT: This prevents the rule from automatically syncing to other carp members.
Gateway
default
Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
Description
Default LAN -> any
You may enter a description here for your reference (not parsed).
Save
Cancel

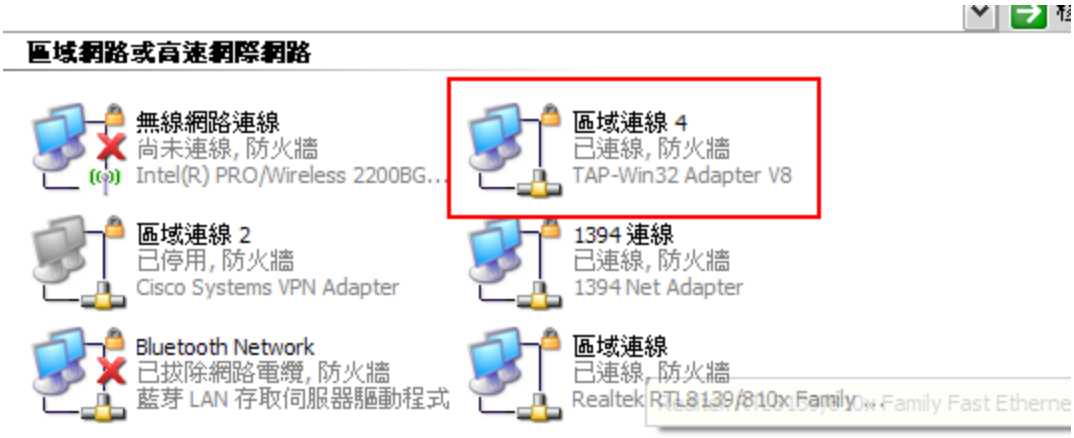
? WAN ?????????



??????????

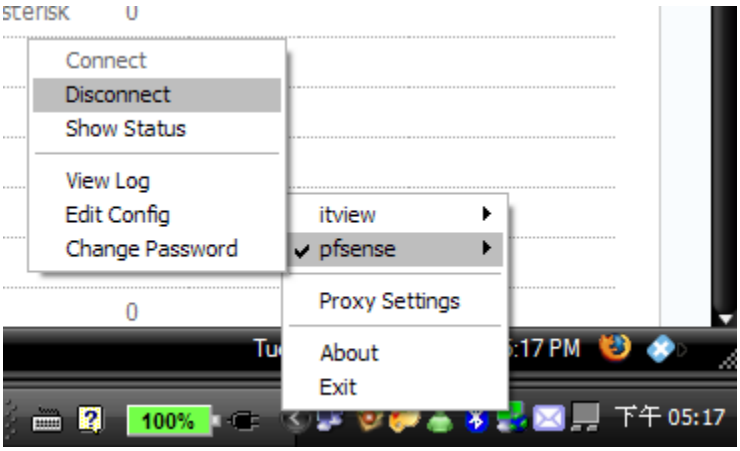


??? pfSense ?? OpenVPN ???????? ?????????????? Windows????? OpenVPN ????????????
http://openvpn.se/ ????????????????????? TAP-Win32 Adapter??????? VPN ???????



??????OpenVPN ??????????????OpenVPN??OpenVPN configuration file directory? ??????????????? pfsense.ovpn?????

reference to undefined name 'syntax' Exception of type 'MindTouch.Deki.Script.Runtime.DekiScriptUndefinedNameException' was thrown. (click for details)
?? pfsense ??? LZO compression???? comp-lzo ????????????????????????????????? ca.crt
pfsense-client.crt
pfsense-client.key
????????????????????????????????? OpenVPN ?????????? connect ? disconnect ???



???? LZO compression ?????????????????????

?????
http://www.pfsense.org/mirror.php?section=tutorials/openvpn/pfsense-ovpn.pdf

?????? 2916