

???

- [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?????????????

Disable this tunnel	<input type="checkbox"/> This allows you to disable this tunnel without removing it from the list.
Protocol	TCP The protocol to be used for the VPN.
Dynamic IP	<input checked="" type="checkbox"/> Assume dynamic IPs, so that DHCP clients can connect.
Local port	1194 The port OpenVPN will listen on. You generally want 1194 here.
Address pool	10.8.9.0/24 This is the address pool to be assigned to the clients. Expressed as a CIDR range (eg. 10.0.8.0/24). If the 'Use static IPs' field isn't set, clients will be assigned addresses from this pool. Otherwise, this will be used to set the local interface's IP.
Use static IPs	<input type="checkbox"/> If this option is set, IPs won't be assigned to clients. Instead, the server will use static IPs on its side, and the clients are expected to use this same value in the 'Address pool' field.
Local network	10.10.10.0/24 This is the network that will be accessible from the remote endpoint. Expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Remote network	<input type="text"/> This is a network that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a CIDR range. If this is a site-to-site VPN, enter here the remote LAN here. You may leave this blank if you don't want a site-to-site VPN.
Client-to-client VPN	<input type="checkbox"/> If this option is set, clients will be able to talk to each other. Otherwise, they will only be able to talk to the server.
Cryptography	SF-CBC (128-bit) Here you can choose the cryptography algorithm to be used.
Authentication method	PKI (Public Key Infrastructure) The authentication method to be used.

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----- ?????????? ???????

Paste your shared key here.

CA certificate

```
-----BEGIN CERTIFICATE-----
MIIDgzCCAuygAwIBAgIBADANBgkqhkiG9w0BAQQF
EDA0BgNVBAGTB0JlbnRkSSUExDzANBgNVBACTBk1V
bG9nRGFOYTEMMAoGA1UECXMdTVVDMQ0wCwYDVQQD
AQkBFhthZG1pbmlzdHJhdG9yQGRpYWxvZ2RhZGEu
WhcNMTYwOTE3MTYzMDUzMCBjbjELMAkGA1UEBhMC
SUEExDzANBgNVBACTBk1VTk1DSDETMDEGA1UEChMK
```

<-CA.CRT

Paste your CA certificate in X.509 format here.

Server certificate

```
ChMKRG1hbG9nRGFOYTEMMAoGA1UECXMdTVVDMQ0w
KoZlIhvcNAQkBFhthZG1pbmlzdHJhdG9yQGRpYWxv
hvcNAQEEDQADgYEAsPc9Vkp9A4D86JC5PGdI347A
q+PW2o7yYkpVO
7tIv9ZAKHj852ceFjs+17zzVVKH+qSZwHFVUNeng
A8CioMniHEV7+K+3XupWOUeKPlcHGNJUvCOZhhqP
-----END CERTIFICATE-----
```

<-SERVER.CRT

Paste your server certificate in X.509 format here.

Server key

```
WQUiavp7ZC2cVS5jgVYtuLOZchYYI#SeOMCQCov
HaaCfWjXfmk6rvyXWenXVBbGhmoQQR9OvGW72XGZ
zaSmjGCoZP
56I3lItZH2a0fd3zcyMCQGD8A03enOrObQMR8gvg
VDVrPropvY5L+hb/
mOK9CGa25G8RLQYR1z3yuP3DGeHu=
-----END RSA PRIVATE KEY-----
```

<-SERVER.KEY

Paste your server key in RSA format here.

DH parameters

```
-----BEGIN DH PARAMETERS-----
MIGHAoGBAODy2ajTcUFzaf0MhGeOHZ1HKGLIc289
Y8SAz65Va7yD9OpP/
QX7J9WBE1y2n6WPinoQSUnSC4ejdJy+hSxqvOTjm
9tHXM7sm11juTFgvV+VpL5XQtch5mj96192BRQr4
-----END DH PARAMETERS-----
```

<-DH1024.PEM

LZO compression = ??????????????????????????????

Custom options = ?????????????? DMZ ? LAN2 ?????????? VPN Client ?????????????????? LAN2 ? 10.10.9.0/24 ??
????

push "route 10.10.9.0 255.255.255.0"

????????????????????

LZO compression Checking this will compress the packets using the LZO algorithm before sending them.

Custom options

```
push "route 10.10.9.0 255.255.255.0"
```

You can put your own custom options here, separated by semi-colons (;). They'll be added to the server configuration.

Description

Road warrior OVPN

You may enter a description here. This is optional and is not parsed.

????????? 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
 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
 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: /
 - Show source port range

Source OS OS Type:
 Note: this only works for TCP rules

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).

Advanced Options - Show advanced options

State Type - Show state

No XMLRPC Sync
 HINT: This prevents the rule from automatically syncing to other carp members.

Gateway
 Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

Description
 You may enter a description here for your reference (not parsed).

? WAN ??????????

Firewall: Rules

LAN WAN **OVPN1**

Proto	Source	Port	Destination	Port	Gateway	Description
TCP/UDP	*	*	*	1194	*	Allow TCP/UDP to OpenVPN Server Port

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 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 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: /

Source OS OS Type: Note: this only works for TCP rules

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

Destination port range from: to:

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 - Show advanced options

State Type - Show state

No MRLRPC Sync HINT: This prevents the rule from automatically syncing to other carp members.

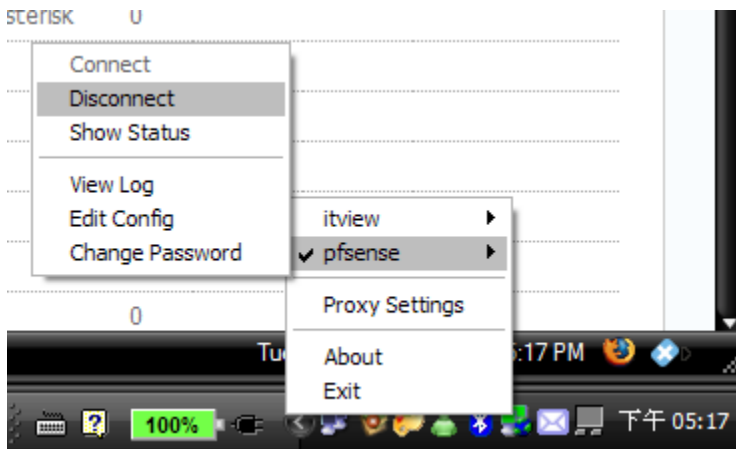
Gateway Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.

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



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>

2987