大綱

- Routing
  - InterVLAN Routing
  - Static Routing
- LAB環境&設定
- NAT
  - NAT設定步驟
  - NAT LAB架構
- PPTP VPN
  - PPTP VPN設定步驟
  - PPTP VPN LAB架構
**InterVLAN Routing**

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dest IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>192.168.2.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Src Mac</th>
<th>Dest Mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC A Mac</td>
<td>VLAN11 Mac</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dest IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>192.168.2.1</td>
</tr>
<tr>
<td>192.168.2.1</td>
<td>192.168.3.1</td>
</tr>
<tr>
<td>192.168.2.2</td>
<td>192.168.3.2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dest IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>192.168.2.2</td>
</tr>
<tr>
<td>192.168.2.2</td>
<td>192.168.3.2</td>
</tr>
</tbody>
</table>

VLAN11: 192.168.1.254
VLAN12: 192.168.2.254
VLAN13: 192.168.3.254

PC A Mac: 192.168.1.254
PC E Mac: 192.168.3.254
**STATIC ROUTING**

- ip route 10.1.1.0 255.255.255.0 gw 172.16.1.2
- ip route 10.1.2.0 255.255.255.0 gw 172.16.1.2

172.16.1.1

Trunk

172.16.1.2

Trunk

VLAN 11
A
192.168.1.1
Gw:192.168.1.254

VLAN 12
B
192.168.2.1
Gw:192.168.2.254

VLAN 1
C
10.1.1.1
Gw:10.1.1.254

VLAN 2
D
10.1.2.1
Gw:10.1.2.254

- ip route 192.168.1.0 255.255.255.0 gw 172.16.1.2
- ip route 192.168.2.0 255.255.255.0 gw 172.16.1.2
LAB 環境設定

- Virtual Box 新增虛擬網卡 (Host Only 2) — 步驟
- 停用兩張 Host Only 網卡之 DHCP 功能 — 步驟
- Host Only 1
  - IP：192.168.56.1/24
- Host Only 2 不設定 IP — 步驟
LAB環境

VM Win XP
Host Only 2
10.1.1.1/24
No Gateway

ToXP(em0)
10.1.1.254

VM pfsense

RealPCGW(em1)
192.168.56.254

Real PC
Host Only 1
192.168.56.1/24
GW:192.168.56.254
LAB環境 - 新增 Host Only 網卡
LAB環境-新增Host ONLY網卡
LAB環境-停用Host ONLY網卡之DHCP功能

LAB環境設定
LAB環境-停用Host ONLY網卡之DHCP功能

2
LAB環境-停用Host ONLY網卡之DHCP功能

![DHCP功能設定對話框](圖示.png)
LAB環境-停用Host ONLY網卡之DHCP功能

如果您的網路支援這項功能，您可以取得自動指派的IP設定。否則，您必須詢問網路系統管理員正確的IP設定。
NAT設定步驟

- 新增Static Routing — 步驟
  - `route add 10.1.1.0 mask 255.255.255.0 192.168.56.254`
- pfSense設定NAT — 步驟
- pfSense設定Firewall Rule — 步驟
- 驗證測試(以遠端桌面為例) — 步驟
NAT LAB 架構

VM Window XP Host Only 2
10.1.1.1/24
No Gateway

VM pfsense

Real PC Host Only 1
192.168.56.1/24
GW: 192.168.56.254

Source IP: 10.1.1.254
Dest IP: 10.1.1.1

Source IP: 192.168.56.1
Dest IP: 10.1.1.1
NAT設定步驟 - 新增 Static Routing

```
route add 10.1.1.0 mask 255.255.255.0 192.168.56.254
```
NAT設定步驟 - pfSense設定NAT
NAT設定步驟 - PFSENSE設定NAT

**Firewall: NAT: Outbound**

**Port Forward** | 1:1 | **Outbound**

**Mode:**
- ```Automatic outbound NAT rule generation (IPsec passthrough included)```
- ```Manual outbound NAT rule generation (AON - Advanced Outbound NAT)```

**Mappings:**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Source</th>
<th>Source Port</th>
<th>Destination</th>
<th>Destination Port</th>
<th>NAT Address</th>
<th>NAT Port</th>
<th>Static Port</th>
<th>Description</th>
</tr>
</thead>
</table>

**Note:**
- With automatic outbound NAT enabled, a mapping is automatically created for each interface's subnet (except WAN-type connections) and the rules on this page are ignored.
- If manual outbound NAT is enabled, outbound NAT rules will not be automatically generated and only the mappings you specify on this page will be used.
- If a target address other than a WAN-type interface's IP address is used, then depending on the way the WAN connection is setup, a Virtual IP may also be required.
- To completely disable outbound NAT, switch to Manual Outbound NAT then delete any NAT rules that appear in the list.
NAT設定步驟 - pfSense設定NAT

### Firewall: NAT: Outbound: Edit

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Do not NAT</strong></td>
<td>Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. Hint: in most cases, you won’t use this option.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Choose which interface this rule applies to. Hint: in most cases, you’ll want to use WAN here.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Choose which protocol this rule should match. Hint: in most cases, you should specify any here.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>Type: Network. Address: 192.168.66.0/24. Enter the source network for the outbound NAT mapping. Source port: Leave blank for any.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>Use this option to invert the sense of the match. Type: Network. Address: 10.1.1.0/24. Enter the destination network for the outbound NAT mapping. Destination port: Leave blank for any.</td>
</tr>
<tr>
<td><strong>Translation</strong></td>
<td>Packets matching this rule will be mapped to the IP address given here. If you want this rule to apply to another IP address rather than the IP address of the interface chosen above, select it here (you will need to define Virtual IP addresses on the interface first). Also note that if you are trying to redirect connections on the LAN select the “any” option. Port: Enter the source port for the outbound NAT mapping. Static-port:</td>
</tr>
<tr>
<td><strong>No XMLRPC Sync</strong></td>
<td>This prevents the rule from automatically syncing to other CARP members.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>You may enter a description here for your reference (not parsed).</td>
</tr>
</tbody>
</table>

[Save] [Cancel]
NAT設定步驟- pfSense設定Firewall Rule

<table>
<thead>
<tr>
<th>ID</th>
<th>Proto</th>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Gateway</th>
<th>Queue</th>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICMP</td>
<td>REALPCGW</td>
<td>*</td>
<td>REALPCGW Address</td>
<td>80</td>
<td>*</td>
<td>*</td>
<td>none</td>
<td>Default allow LAN to any rule</td>
</tr>
</tbody>
</table>

**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.
### NAT設定步驟: pfSense設定Firewall Rule

<table>
<thead>
<tr>
<th>Action</th>
<th>Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Disabled**
- Disable this rule
  - Set this option to disable the rule without removing it from the list.

**Interface**
- REALPCGW
  - Choose on which interface packets must come in to match this rule.

**Protocol**
- TCP
  - 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: REALPCGW subnet
  - Address: [Input]
  - Advanced: Show source port range

**Destination**
- not
  - Use this option to invert the sense of the match.
  - Type: TCP subnet
  - Address: [Input]

**Destination port range**
- from: MS RDP
  - to: MS RDP

**Log**
- Log packets that are handled by this rule
  - Hint: the firewall has limited 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.

[Save] [Cancel]
NAT設定步驟 - 驗證測試1
NAT設定步驟 - 驗證測試2
NAT設定步驟-驗證測試3
NAT設定步驟-驗證測試4
PPTP VPN 設定步驟

- 刪除Static Routing—步骤
  - route delete 10.1.1.0

- pfSense設定PPTP VPN—步骤

- pfSense設定Firewall PPTP撥接Rule —步骤

- pfSense設定PPTP VPN Firewall Rule —步骤

- 驗證測試(以遠端桌面為例) —步骤
PPTP VPN LAB 架構

VM Win XP
Host Only 2
10.1.1.1/24
No Gateway

ToXP(em0)
10.1.1.254

VM pfsense

RealPCGW(em1)
192.168.56.254

Real PC
Host Only 1
192.168.56.1/24

IP: 10.1.1.200
PPTP VPN 設定步驟-刪除Static Routing
PPTP VPN 設定步驟- PFSENSE設定PPTP VPN

![PPTP VPN配置界面](image)

- 一般設定
  - PPTP redireciton
    - Enter the IP address of a host which will accept incoming PPTP connections.
  - No. PPTP users
    - 16
    - Hint: 10 is ten PPTP clients
  - Server address
    - 192.168.56.254
    - Enter the IP address the PPTP server should give to clients as their "gateway". Typically this is set to an unused IP just outside of the client range.
    - NOTE: This should NOT be set to any IP address currently in use on this firewall.
PPTP VPN 設定步驟- pfSense設定PPTP VPN
PPTP VPN 設定步驟- PFSENSE設定PPTP VPN

![PPTP VPN 環境設定](image)
PPTP VPN 設定步驟- pfSense設定PPTP VPN
PPTP VPN 設定步驟 - pfSense 設定
FIREWALL PPTP 撥接 Rule

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.
PPTP VPN 設定步驟 - pfSense設定
FIREWALL PPTP撥接Rule
PPTP VPN 設定步驟- pfSense設定PPTP VPN Firewall Rule

No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until you add pass rules.
Click the button to add a new rule.

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.
PPTP VPN 設定步驟 - pfSense設定PPTP VPN Firewall Rule

<table>
<thead>
<tr>
<th>Firewall: Rules: Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Choose what to do with packets that match the criteria specified below.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Disabled</strong></td>
</tr>
<tr>
<td>Select this to disable this rule without removing it from the list.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td>Select through which interface packets must come to match this rule.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td>Select which protocol this rule should match.</td>
</tr>
<tr>
<td>Hint: in most cases, you should specify TCP here.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
</tr>
<tr>
<td>Use this option to invert the sense of the match.</td>
</tr>
<tr>
<td>Type: PPTP clients</td>
</tr>
<tr>
<td>Address:</td>
</tr>
<tr>
<td>Advanced - Show source port range</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>Use this option to invert the sense of the match.</td>
</tr>
<tr>
<td>Type: TCP subnet</td>
</tr>
<tr>
<td>Address:</td>
</tr>
<tr>
<td><strong>Destination port range</strong></td>
</tr>
<tr>
<td>Specify the port or port range for the destination of the packet for this rule.</td>
</tr>
<tr>
<td>Hint: you can leave the 'To' field empty if you only want to filter a single port.</td>
</tr>
<tr>
<td><strong>Log</strong></td>
</tr>
<tr>
<td>Log packets that are handled by this rule.</td>
</tr>
<tr>
<td>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).</td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>You may enter a description here for your reference.</td>
</tr>
</tbody>
</table>

Save  Cancel
PPTP VPN 設定步驟-驗證測試
PPTP VPN CLINET SETTING 1
PPTP VPN 設定步驟-驗證測試
PPTP VPN CLINET SETTING 2
PPTP VPN 設定步驟-驗證測試
PPTP VPN CLINET SETTING 3
PPTP VPN 設定步驟-驗證測試
PPTP VPN CLIENT SETTING 4
PPTP VPN 設定步驟-驗證測試
PPTP VPN CLINET SETTING 5
PPTP VPN 設定步驟 - 驗證測試

PPTP VPN CLINET SETTING 6
PPTP VPN 設定步驟-驗證測試
PPTP VPN 設定步驟-驗證測試
PPTP VPN 設定步驟-驗證測試
PPTP VPN 設定步驟 - 驗證測試

```
Active Connections

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.1.1.1:3389</td>
<td>10.1.1.200:52524</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:1025</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:445</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:500</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>10.1.1.1:123</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>10.1.1.1:127</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>10.1.1.1:130</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>10.1.1.1:1900</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:123</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:1040</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>127.0.0.1:1900</td>
<td>0.0.0.0:0</td>
<td></td>
</tr>
</tbody>
</table>
```

C:\Documents and Settings\NASAdmin>netstat -na