

pfSense 網頁 multi-home 備援建置

游子興

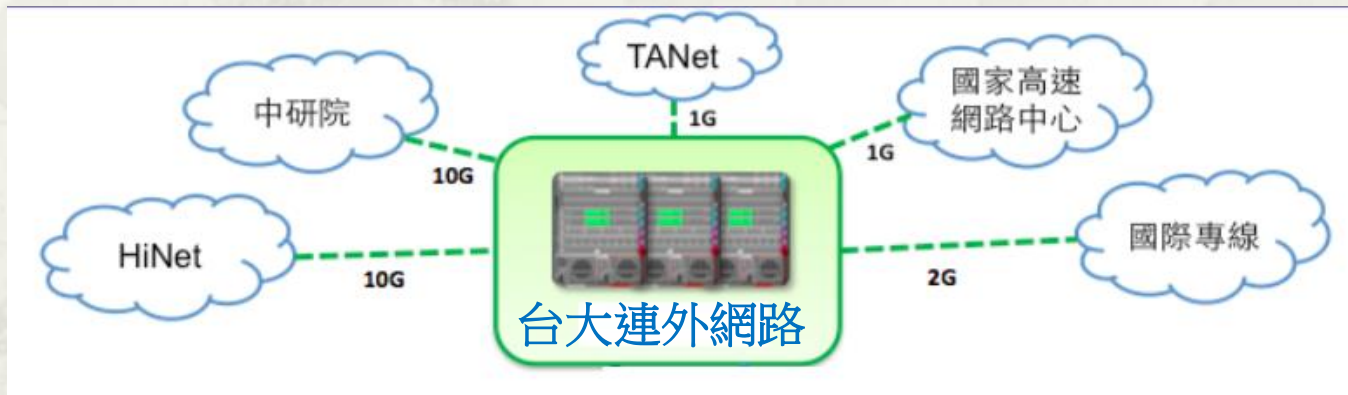
台大計中網路組

davisyou@ntu.edu.tw

02-33665008

臺大區網網頁備援建置

- * 臺大連外網路為 Multi-Home 架構
- * 建構TANet與臺大網路互為備援之區網網頁
- * TANet 斷線時仍可由臺大網路在網頁公告事項



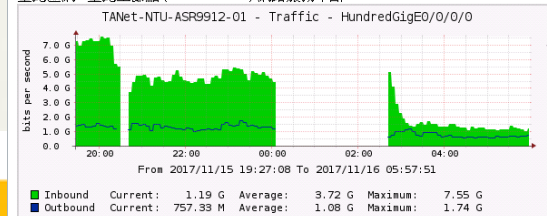
11/16 凌晨區網斷線近 3小時

本次施工貴公司未依程序施工(詳前信申請施工之注意事項),已導致本網(TANet)服務中斷,請查明原因。

受此施工中斷之服務(中斷)為:

1. 臺北區網(臺大)對外(臺北&新竹)的 TANet 服務, 於 106.11.16 00:00 - 02:04 處於完全中斷, 所屬連線學校/單位均無網路服務。
2. 中研院主節點-新竹主節點的 TANet 服務, 於 106.11.16 00:00 - 02:04 處於完全中斷。

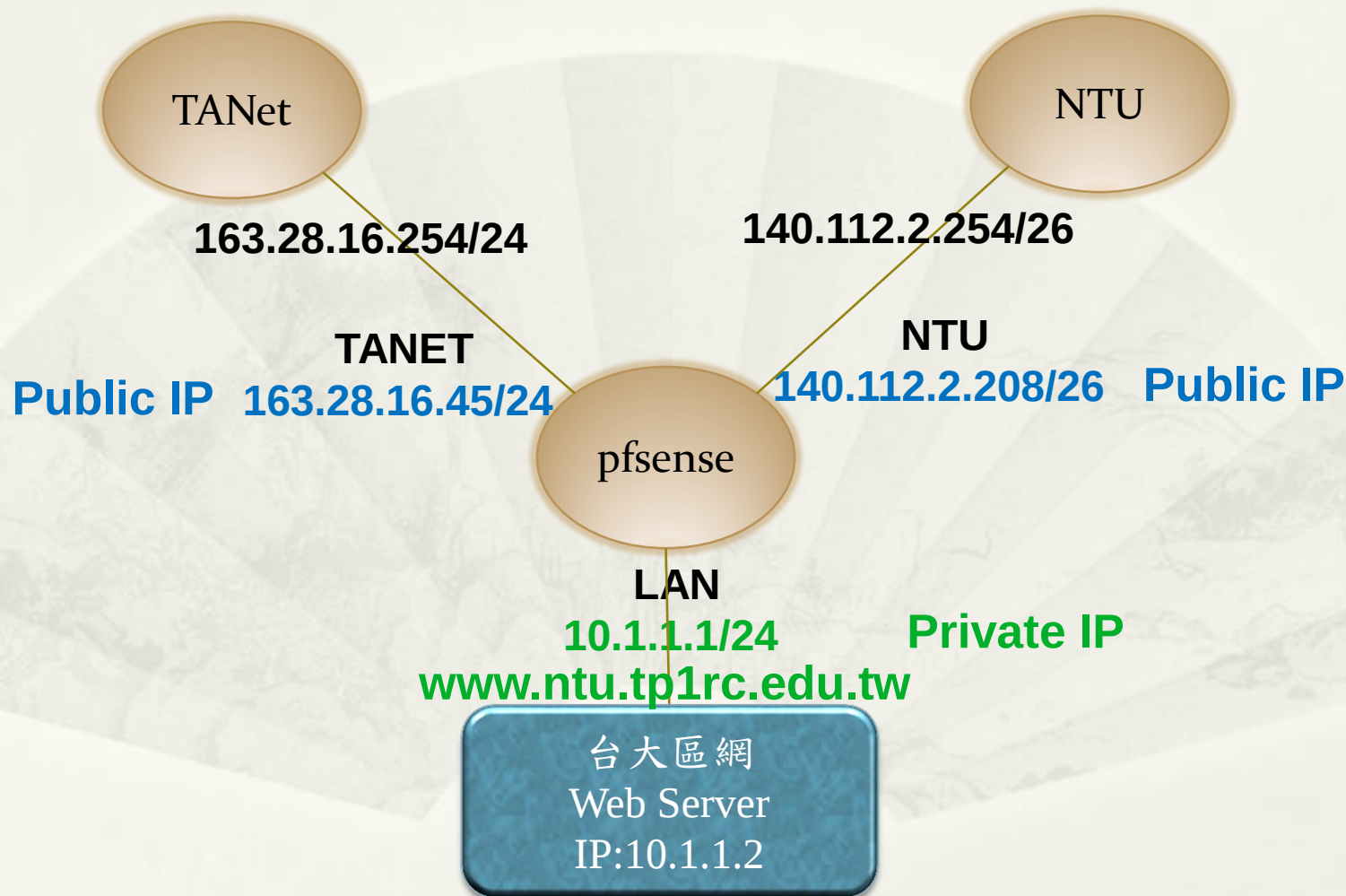
臺北區網-臺北主節點 (00:00 - 02:40) 網路服務中斷。



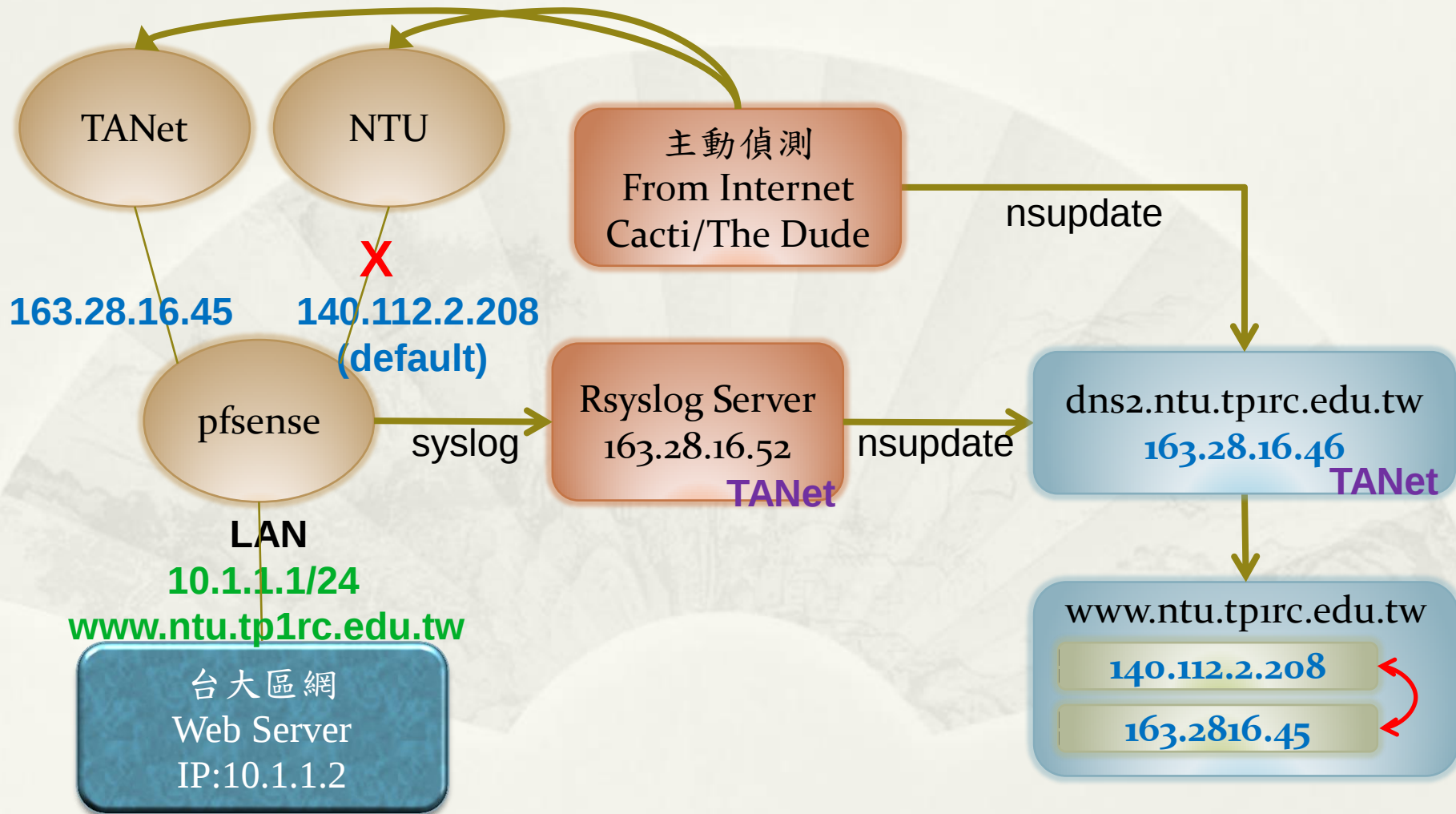


NAT MODE MULTI-WAN WEB SERVER

網頁備援運作架構



NAT & Multi-WAN



Interfaces > NTU

Interfaces / NTU   

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type
▼

IPv6 Configuration Type
▼

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex
▼
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /
▼

IPv4 Upstream gateway
▼
+ Add a new gateway

Interfaces > TANET

Interfaces / TANET ≡ |dl ?

General Configuration

Enable ☒ Enable interface

Description

TANET

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

▼

IPv6 Configuration Type

None

▼

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

▼

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

163.28.16.45

/ 24 ▼

IPv4 Upstream gateway

TANETGW - 163.28.16.254

▼

+ Add a new gateway

System > Routing > Gateways

System / Routing / Gateways

Gateways

Static Routes

Gateway Groups

Gateways

	Name	Interface	Gateway	Monitor IP	Description	Actions
☒	NTUGW (default)	NTU	140.112.2.254	140.112.2.254		   
☒	TANETGW	TANET	163.28.16.254	163.28.16.254		   

Advanced

Weight

1

Weight for this gateway when used in a Gateway Group.

Data Payload

0

Define data payload to send on ICMP packets to gateway monitor IP.

Latency thresholds

200

500

Low and high thresholds for latency in milliseconds. Default is 200/500.

Packet Loss thresholds

10

20

Low and high thresholds for packet loss in %. Default is 10/20.

Probe Interval

500

How often an ICMP probe will be sent in milliseconds. Default is 500.

Loss Interval

2000

Time interval in milliseconds before packets are treated as lost. Default is 2000.

System > Routing > Gateway Groups

System / Routing / Gateway Groups / Edit



Edit Gateway Group Entry

Group Name

Gateway Priority

NTUGW

Tier 1



Interface Address



Group Name

TANETGW

Tier 2



Interface Address



Group Name

Gateway

Tier

Virtual IP

Description

Link Priority

The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.

Virtual IP

The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.

Trigger Level

Member down
Packet Loss
High Latency
Packet Loss or High latency

Description

A description may be entered here for administrative reference (not parsed).

Firewall > Rules > LAN

- * LAN to any 全部開放
- * Gateway= GW_GROUP

Firewall / Rules / LAN

Floating TANET LAN NTU

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1 / 5.66 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
☐	✓ ⚙️ 3 / 17.37 MiB	IPv4 *	LAN net	*	*	*	GW_GROUP	none		Default allow LAN to any rule	📌 ✎ 📄 🚫 🗑
☐	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 ✎ 📄 🚫 🗑

Firewall > NAT > Port Forward

Firewall / NAT / Port Forward



Port Forward 1:1 Outbound NPt

Rules

			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	☒		NTU	TCP	*	*	NTU address	80 (HTTP)	10.1.1.2	80 (HTTP)		
☐	☒		NTU	TCP	*	*	NTU address	443 (HTTPS)	10.1.1.2	443 (HTTPS)		
☐	☒		NTU	TCP	*	*	NTU address	22 (SSH)	10.1.1.2	22 (SSH)		
☐	☒		TANET	TCP	*	*	TANET address	80 (HTTP)	10.1.1.2	80 (HTTP)		
☐	☒		TANET	TCP	*	*	TANET address	443 (HTTPS)	10.1.1.2	443 (HTTPS)		

Status > Gateways

Status / Gateways / Gateways

Gateways

Gateway Groups

Gateways

Name	Gateway	Monitor	RTT	RTTsd	Loss	Status
NTUGW	140.112.2.254	140.112.2.254	0.785ms	0.921ms	0.0%	Online
TANETGW	163.28.16.254	163.28.16.254	0.874ms	0.823ms	0.0%	Online

Status / Gateways / Gateway Groups

Gateways

Gateway Groups

Gateway Groups

Group Name	Gateways	
GW_GROUP	Tier 1	Tier 2
	NTUGW Online	
		TANETGW Online

```
[root@tp1rc ~]# traceroute -n 168.95.1.1
traceroute to 168.95.1.1 (168.95.1.1), 30 hops max, 60 byte packets
 1  140.112.2.254  1.707 ms  1.614 ms  1.635 ms
 2  * * *
 3  140.112.0.190  1.546 ms  1.540 ms  1.556 ms
 4  140.112.0.198  2.068 ms  1.985 ms  2.027 ms
 5  211.22.226.202  2.057 ms  1.999 ms  2.219 ms
 6  220.128.12.58  8.311 ms  220.128.2.50  3.101 ms  220.128.12.54  8.583 ms
 7  220.128.1.249  1.396 ms  1.590 ms  1.591 ms
 8  210.59.204.217  1.358 ms  1.743 ms  1.544 ms
 9  220.128.32.68  1.864 ms  1.923 ms  2.079 ms
```

Status > Gateways

Status / Gateways / Gateways

Gateways

Gateway Groups

Gateways

Name	Gateway	Monitor	RTT	RTTsd	Loss	Status
NTUGW	140.112.2.254	140.112.2.254	0.641ms	0.473ms	50%	Offline
TANETGW	163.28.16.254	163.28.16.254	0.802ms	0.182ms	0.0%	Online

Status / Gateways / Gateway Groups

Gateways

Gateway Groups

Gateway Groups

Group Name	Gateways	
GW_GROUP	Tier 1	Tier 2
	NTUGW Offline	
		TANETGW Online

```
[root@tp1rc ~]# traceroute -n 168.95.1.1
traceroute to 168.95.1.1 (168.95.1.1), 30 hops max, 60 byte packets
 1  163.28.16.254  1.181 ms  1.271 ms  1.266 ms
 2  211.20.43.62   0.719 ms 211.22.226.186  0.653 ms 211.20.43.62  0.632 ms
 3  210.59.204.225 0.609 ms  0.725 ms  0.603 ms
 4  220.128.32.68  0.682 ms  0.697 ms  0.661 ms
```

Status > System Logs > System > Gateways

Status / System Logs / System / Gateways

System Firewall DHCP Captive Portal Auth IPsec PPP

General Gateways Routing DNS Resolver Wireless

Last 50 Gateways Log Entries. (Maximum 50)

Time	Process	PID	Message
Oct 30 22:41:30	dpinger		NTUGW 140.112.2.254: sendto error: 64
Oct 30 22:41:30	dpinger		NTUGW 140.112.2.254: sendto error: 64
Oct 30 22:41:31	dpinger		NTUGW 140.112.2.254: sendto error: 64
Oct 30 22:41:31	dpinger		NTUGW 140.112.2.254: sendto error: 64
Oct 30 22:41:55	dpinger		NTUGW 140.112.2.254: Alarm latency 13226299us stddev 24088921us loss 89%
Oct 30 22:42:10	dpinger		NTUGW 140.112.2.254: Alarm latency 15719us stddev 60230us loss 74%
Oct 30 22:42:54	dpinger		NTUGW 140.112.2.254: Clear latency 5155us stddev 32132us loss 5%

Status > System Logs > System > General

Status / System Logs / System / General



System Firewall DHCP Captive Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

General Gateways Routing DNS Resolver Wireless

Last 50 General Log Entries. (Maximum 50)

Time	Process	PID	Message
Oct 30 22:41:12	rc.gateway_alarm	30853	>>> Gateway alarm: NTUGW (Addr:140.112.2.254 Alarm:1 RTT:803ms RTTsd:919ms Loss:22%)
Oct 30 22:41:12	check_reload_status		updating dyndns NTUGW
Oct 30 22:41:12	check_reload_status		Restarting ipsec tunnels
Oct 30 22:41:12	check_reload_status		Restarting OpenVPN tunnels/interfaces
Oct 30 22:41:12	check_reload_status		Reloading filter
Oct 30 22:41:13	php-fpm	54569	/rc.dyndns.update: MONITOR: NTUGW is down, committing from routing group GW_GROUP 140.112.2.254 140.112.2.208 NTUGW 0.813ms 0.933ms 24% down
Oct 30 22:42:54	rc.gateway_alarm	67329	>>> Gateway alarm: NTUGW (Addr:140.112.2.254 Alarm:0 RTT:5155ms RTTsd:32132ms Loss:5%)
Oct 30 22:42:54	check_reload_status		updating dyndns NTUGW
Oct 30 22:42:54	check_reload_status		Restarting ipsec tunnels
Oct 30 22:42:54	check_reload_status		Restarting OpenVPN tunnels/interfaces
Oct 30 22:42:54	check_reload_status		Reloading filter
Oct 30 22:42:55	php-fpm	65659	/rc.dyndns.update: MONITOR: NTUGW is available now, adding to routing group GW_GROUP 140.112.2.254 140.112.2.208 NTUGW 5.078ms 31.859ms 3% none

Status > System Logs > Settings

Status / System Logs / Settings

System Firewall DHCP Captive Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Remote Logging Options

Enable Remote Logging ☒ Send log messages to remote syslog server

Source Address Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers 163.28.16.52

IP[:port]

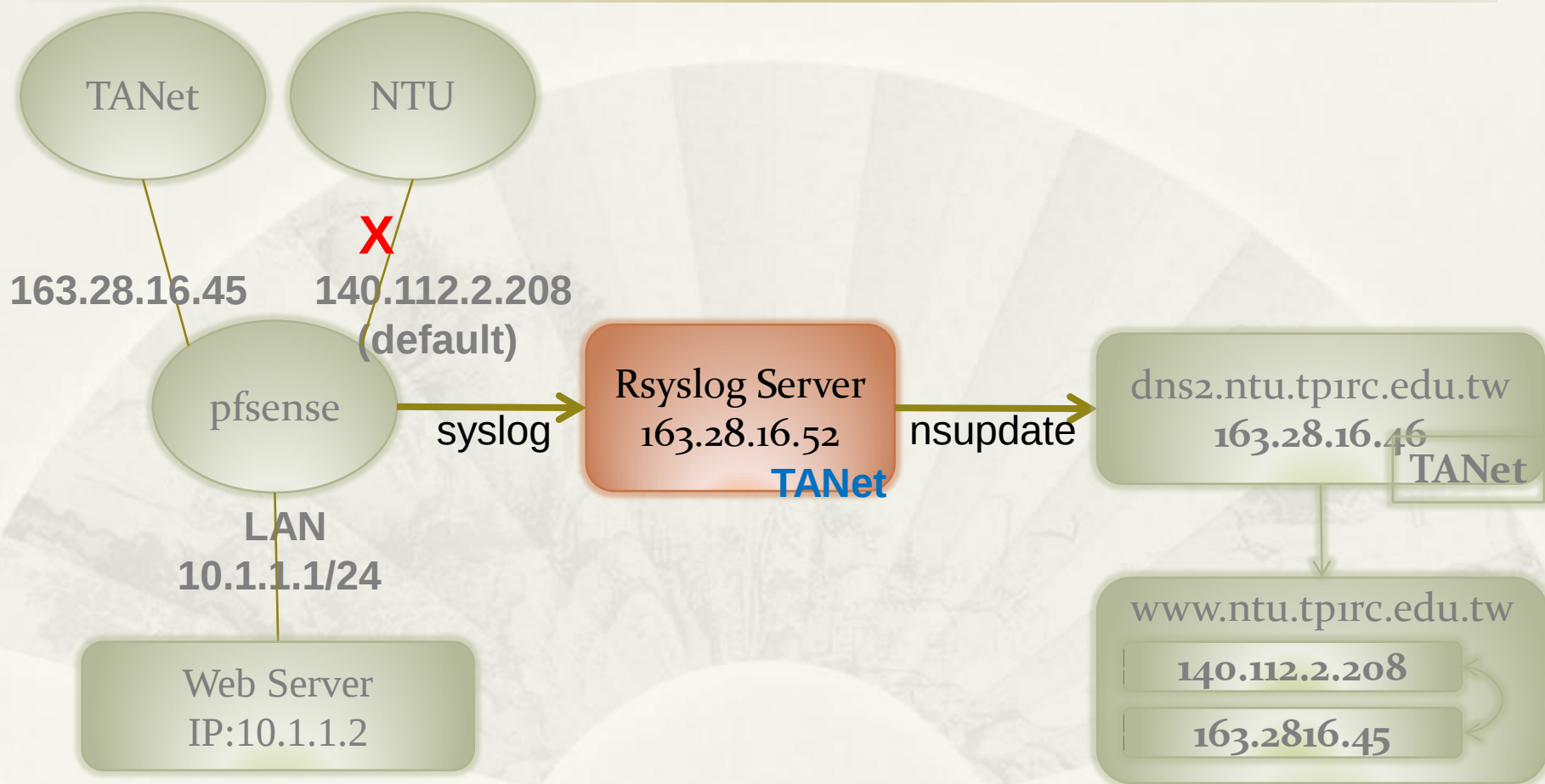
IP[:port]

Remote Syslog Contents

- ☐ Everything
- ☒ System Events
- ☐ Firewall Events
- ☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- ☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- ☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
- ☐ Captive Portal Events
- ☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
- ☐ Gateway Monitor Events
- ☐ Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)
- ☐ Server Load Balancer Events (relayd)
- ☐ Network Time Protocol Events (NTP Daemon, NTP Client)
- ☐ Wireless Events (hostapd)



NAT & Multi-WAN



* /etc/rsyslog.conf

Provides UDP syslog reception

\$ModLoad imudp

\$UDPServerRun 514

module(load="omprog")

if (\$msg contains "NTUGW is down") then {

 action(type="omprog" binary="/usr/bin/nsupdate -v
 /root/nsupdate_tp1rc.txt")

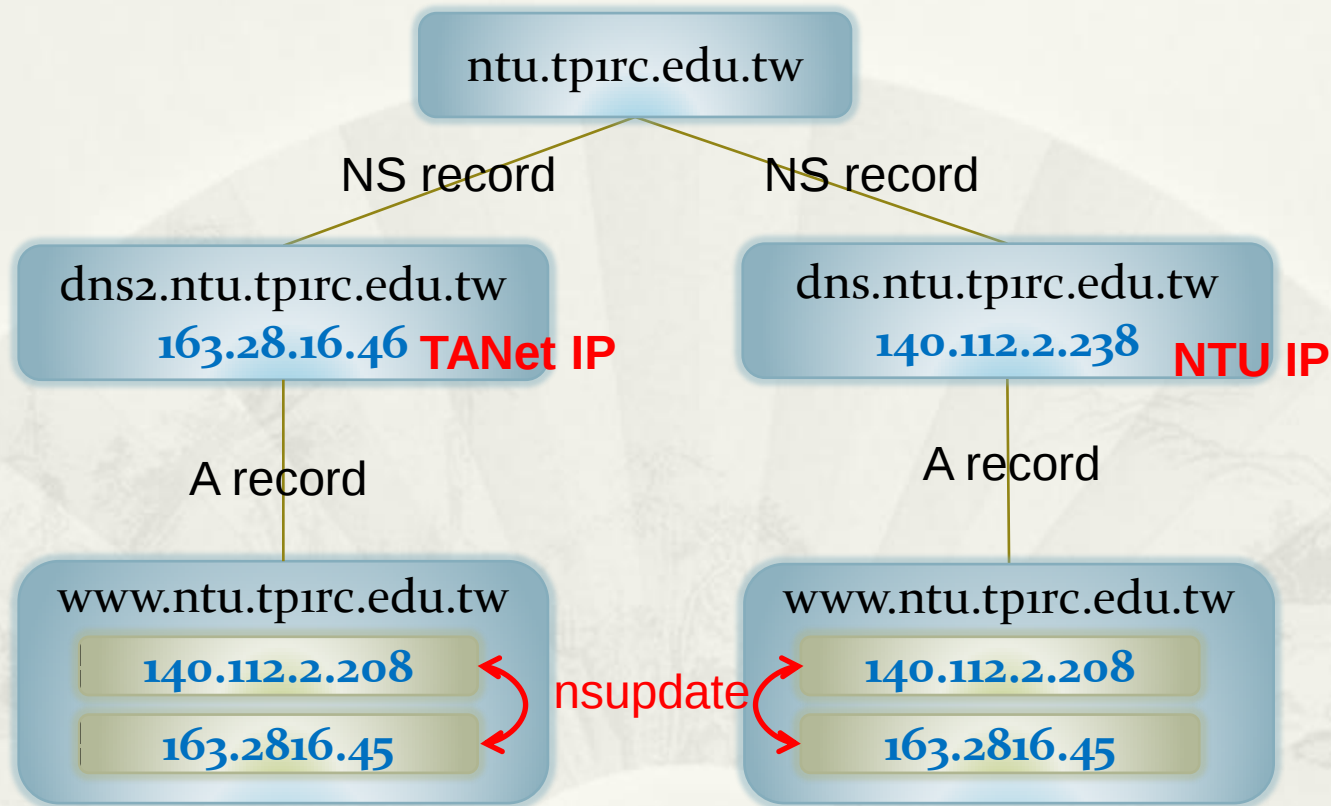
} else if (\$msg contains "NTUGW is available now") then {

 action(type="omprog" binary="/usr/bin/nsupdate -v
 /root/nsupdate_ntu.txt")}

```
Oct 30 22:41:12 cacheflow5.tplrc.edu.tw rc.gateway_alarm[30853]: >>> Gateway alarm: NTUGW (Addr:140.112.2.254 Alarm:1 RTT:803ms RTTsd:919ms Loss:22%)
Oct 30 22:41:12 cacheflow5.tplrc.edu.tw check_reload_status: updating dyndns NTUGW
Oct 30 22:41:12 cacheflow5.tplrc.edu.tw check_reload_status: Restarting ipsec tunnels
Oct 30 22:41:12 cacheflow5.tplrc.edu.tw check_reload_status: Restarting OpenVPN tunnels/interfaces
Oct 30 22:41:12 cacheflow5.tplrc.edu.tw check_reload_status: Reloading filter
Oct 30 22:41:13 cacheflow5.tplrc.edu.tw php-fpm[54569]: /rc.dyndns.update: MONITOR: NTUGW is down, omitting from routing group GW_GROUP 140.112.2.254|140.112.2.208|NTUGW|0.813ms|0.933ms|24%|down
Oct 30 22:41:13 smtp2 rsyslogd: Child 2704 has terminated, reaped by main-loop. [v8.24.0 try http://www.rsyslog.com/e/0 ]
```

```
Oct 30 22:42:54 cacheflow5.tplrc.edu.tw rc.gateway_alarm[67329]: >>> Gateway alarm: NTUGW (Addr:140.112.2.254 Alarm:0 RTT:5155ms RTTsd:32132ms Loss:5%)
Oct 30 22:42:54 cacheflow5.tplrc.edu.tw check_reload_status: updating dyndns NTUGW
Oct 30 22:42:54 cacheflow5.tplrc.edu.tw check_reload_status: Restarting ipsec tunnels
Oct 30 22:42:54 cacheflow5.tplrc.edu.tw check_reload_status: Restarting OpenVPN tunnels/interfaces
Oct 30 22:42:54 cacheflow5.tplrc.edu.tw check_reload_status: Reloading filter
Oct 30 22:42:55 cacheflow5.tplrc.edu.tw php-fpm[65659]: /rc.dyndns.update: MONITOR: NTUGW is available now, adding to routing group GW_GROUP 140.112.2.254|140.112.2.208|NTUGW|5.078ms|31.859ms|3%|none
Oct 30 22:42:55 smtp2 rsyslogd: Child 2719 has terminated, reaped by main-loop. [v8.24.0 try http://www.rsyslog.com/e/0 ]
```

NAT & Multi-WAN



Zone file for tp1rc.edu.tw

* Named record

\$ORIGIN tp1rc.edu.tw.

@ IN SOA dns.ntu.edu.tw. madeline.ntu.edu.tw (

...

ntu IN NS dns.ntu.tp1rc.edu.tw.

IN NS dns2.ntu.tp1rc.edu.tw.

dns.ntu IN A 140.112.2.238

dns2.ntu IN A 163.28.16.46

```
> set type=ns
> ntu.tp1rc.edu.tw
伺服器: dns.ntu.edu.tw
Address: 140.112.254.4
```

未經授權的回答:

```
ntu.tp1rc.edu.tw
ntu.tp1rc.edu.tw
```

```
nameserver = dns.ntu.tp1rc.edu.tw
```

```
nameserver = dns2.ntu.tp1rc.edu.tw
```

Config file for ntu.tp1rc.edu.tw

```
zone "ntu.tp1rc.edu.tw"{  
    type master;  
    file "named.ntu";  
    allow-update { 163.28.16.0/24; };  
};
```

Zone file for ntu.tp1rc.edu.tw

\$TTL 120 ; 2 minutes

@ IN SOA dns.ntu.tp1rc.edu.tw. root.mail.ntu.tp1rc.edu.tw.

(2017102101 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H) ; minimum

IN NS dns.ntu.tp1rc.edu.tw.

IN NS dns2.ntu.tp1rc.edu.tw.

dns IN A 140.112.2.238

dns2 IN A 163.28.16.46

www IN A 140.112.2.208

nsupdate

- * nsupdate -v /root/nsupdate_tpirc.txt

- * nsupdate_tpirc.txt

server 140.112.2.238

update delete www.ntu.tpirc.edu.tw A

update add www.ntu.tpirc.edu.tw 120 A 163.28.16.45

send

server 163.28.16.46

update delete www.ntu.tpirc.edu.tw A

update add www.ntu.tpirc.edu.tw 120 A 163.28.16.45

send

nsupdate

- * nsupdate -v /root/nsupdate_ntu.txt

- * nsupdate_ntu.txt

server 140.112.2.238

update delete www.ntu.tpirc.edu.tw A

update add www.ntu.tpirc.edu.tw 120 A 140.112.2.208

send

server 163.28.16.46

update delete www.ntu.tpirc.edu.tw A

update add www.ntu.tpirc.edu.tw 120 A 140.112.2.208

send

```
C:\Windows\System32>ping www.ntu.tp1rc.edu.tw

Ping www.ntu.tp1rc.edu.tw [140.112.2.208] <使用 32 位元組的資料>:
Control-C
^C
C:\Windows\System32>ping www.ntu.tp1rc.edu.tw

Ping www.ntu.tp1rc.edu.tw [163.28.16.45] <使用 32 位元組的資料>:
```

* index.html

```
<html>
```

```
<head>
```

```
  <META HTTP-EQUIV="Refresh" CONTENT="0;  
url=http://www.ntu.tp1rc.edu.tw/index.php">
```

```
</head>
```

```
</html>
```



簡報完畢
謝謝