

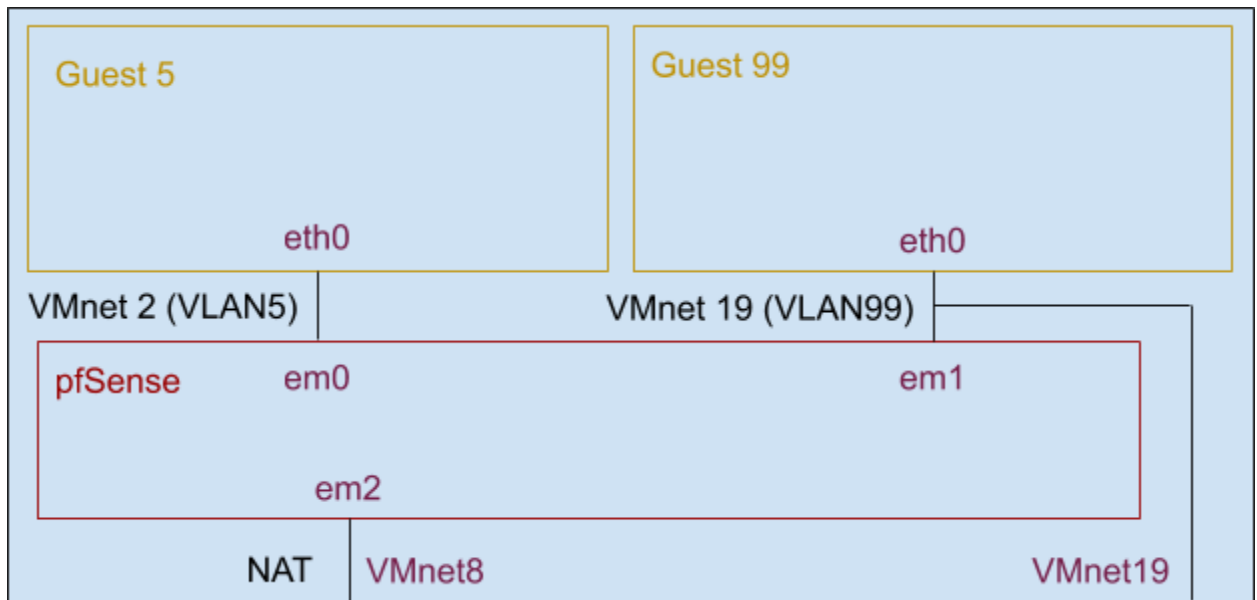
# Network Administration/System Administration (NTU CSIE, Spring 2019)

## Homework #4





### Network Administration

#### 1. pfSense

##### 1. install



##### 2. Interfaces > VLANs

Interfaces / VLANs				
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs
PPPs	GREs	GIFs	Bridges	LAGGs
VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
em2	5	1	user	 
em1	99	7	control	 

##### 3. Interfaces > Assignments

Interfaces / Interface Assignments

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port	
WAN	em0 (00:0c:29:02:df:4d)	
Vlan5	VLAN 5 on em2 (user)	Delete
Vlan99	VLAN 99 on em1 (control)	Delete

#### 4. Interfaces > Vlan5 (em2.5)

Interfaces / Vlan5 (em2.5)

General Configuration

Enable

☒ Enable interface

Description

Vlan5

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxxxxxx

The MAC address of a VLAN interface must be set on its parent interface

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

192.168.5.1

/ 24

IPv4 Upstream gateway

None

Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
 On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

#### 5. Interfaces > Vlan99 (em1.99)

Interfaces / **Vlan99 (em1.99)**

General Configuration

Enable

☒ Enable interface

Description

Vlan99

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

The MAC address of a VLAN interface must be set on its parent interface

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

192.168.99.1

/ 24

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

## 6. DHCP Server > VLAN5

☒ enable

Services / **DHCP Server / VLAN5**

VLAN5

VLAN99

General Options

Enable

☒ Enable DHCP server on VLAN5 interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

☐ Only the clients defined below will get DHCP leases from this server.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.  
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.  
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.5.0

Subnet mask

255.255.255.0

Available range

192.168.5.1 - 192.168.5.254

Range

192.168.5.100

From

192.168.5.199

To

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	8.8.8.8
	8.8.4.4

## 7. DHCP Server > VLAN99

☒ enable

Services / DHCP Server / VLAN99

VLAN5
VLAN99

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on VLAN99 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.99.0
Subnet mask	255.255.255.0
Available range	192.168.99.1 - 192.168.99.254
Range	<div> 192.168.99.100 192.168.99.199 </div> <div> From To </div>

Servers

WINS servers	WINS Server 1
	WINS Server 2
DNS servers	8.8.8.8
	8.8.4.4

## 8. System > Advance

☒ Enable Secure Shell

Reference:

<https://docs.netgate.com/pfsense/en/latest/usermanager/granting-users-access-to-ssh.html>

## 9. Alias

Diagnostics > DNS Lookup

Diagnostics / DNS Lookup ?

DNS Lookup

Hostname

linux1.csie.org

Lookup

Add alias

Results

Result	Record type
140.112.30.32	A
linux1.csie.ntu.edu.tw	CNAME

Add alias

Firewall > Aliases > IP

Firewall / Aliases / Edit ?

Properties

Name

linux1\_csie\_org

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

Description

Created from Diagnostics-> DNS Lookup

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

Type

Network(s)

Network(s)

Hint

Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN				Description	
140.112.30.32	/	32		Description	Delete
linux1.csie.ntu.edu.tw	/	32		Description	Delete

10. Firewall > Schedules
























1. Add NASA\_HW4\_5

Firewall / Schedules ?

Schedules

Name	Range: Date / Times / Name	Description	Actions
NASA_HW4_5	November 24 / 14:00-17:00 / November 23 / 14:00-17:00 /		

11. Firewall > Rules > VLAN99

Firewall / Rules / VLAN99											  
<div> Floating WAN VLAN5 VLAN99 </div>											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 1.34 MiB	IPv4 *	*	*	This Firewall	*	*	none		Access firewall (self)	   
<input type="checkbox"/>	✓ 0 / 1008 B	IPv4 *	*	*	VLAN5 net	*	*	none		Access VLAN5	   
<input type="checkbox"/>	✓ 0 / 5 KiB	IPv4 *	*	*	linux1_csie_org	*	*	none		Access linux1_csie_org	   
<input type="checkbox"/>	✓ 2 / 134 KiB	IPv4 *	*	*	google_dns	*	*	none		Access DNS	   
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	*	*	*	*	*	none		Access all	   

1. Add Access firewall (self)
2. Add Access VLAN5
3. Add Access linux1.csie.org

Edit Firewall Rule

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.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

VLAN99

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match.

any

Source Address

/

Destination

Destination

☐ Invert match.

Single host or alias

linux1\_csie\_org

/

Extra Options

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 doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description

Access linux1\_csie\_org

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

 Display Advanced













google\_dns for linux1.csie.org

12. Firewall > Rules > VLAN5

Firewall / Rules / VLAN5

Floating WAN VLAN5 VLAN99

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0 / 180 B	IPv4 TCP	*	*	This Firewall	*	*	none		Block firewall	  
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 TCP	VLAN5 net	*	VLAN99 net	*	*	none		Block VLAN99	  
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 UDP	*	*	*	*	*	none	NASA_HW4_5		  
<input type="checkbox"/>	✓ 0 / 25 KiB	IPv4 *	*	*	*	*	*	none		Allow all	  







1. Add block access to firewall (self)
2. Add block access to VLAN99
3. Add block any ⇔ any udp with schedule NASA\_HW4\_5
4. Add Allow any ⇔ at the end

#### 13. Firewall > Rules > WAN

Firewall / Rules / WAN

Floating WAN VLAN5 VLAN99

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0 / 312 B	IPv4 TCP	*	*	This Firewall	*	*	none		Block firewall	  
<input type="checkbox"/>	✓ 0 / 13.16 MiB	IPv4+6 *	*	*	*	*	*	none		Allow all ipv4+ipv6 via pfSsh.php	  

1. Add Block firewall (self)

#### 14. Tip

##### Manual set adapter's tag

