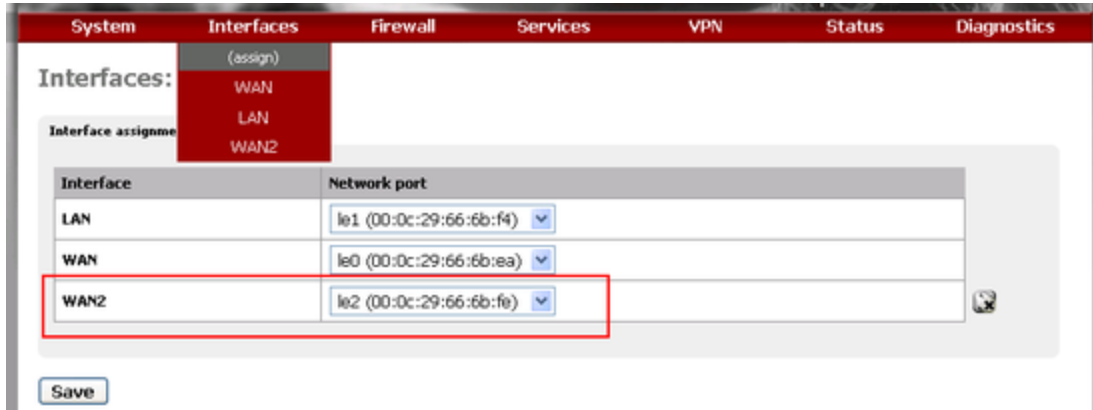


(?:alang)

??????? pfSense ???? WAN ???? Public IP???????????????? IP ??????????????????????IP????????????????????  
?????????????????????????????Outbound loading Balance?

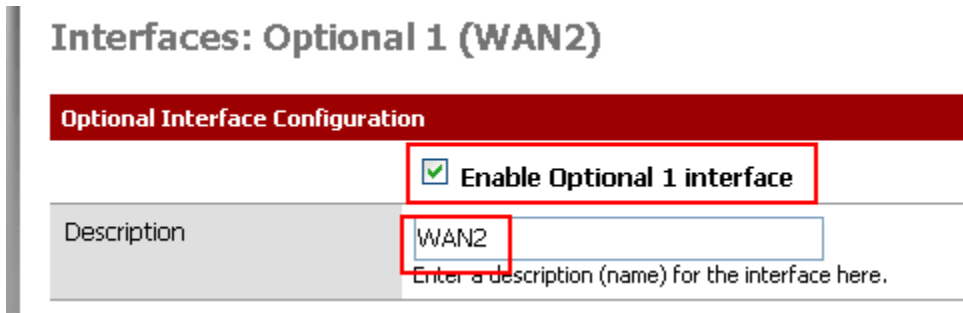
????????? WAN?LAN ?????????????????????? IP ??????????????????????

?Interface??assign???? ?????????????????????????????????? OPT1????????????????? WAN2?



??????????

?Interface??OPT1?????? WAN2?



IP Configuration ? Bridge with WAN  
Gateway ?? ?IP?????????

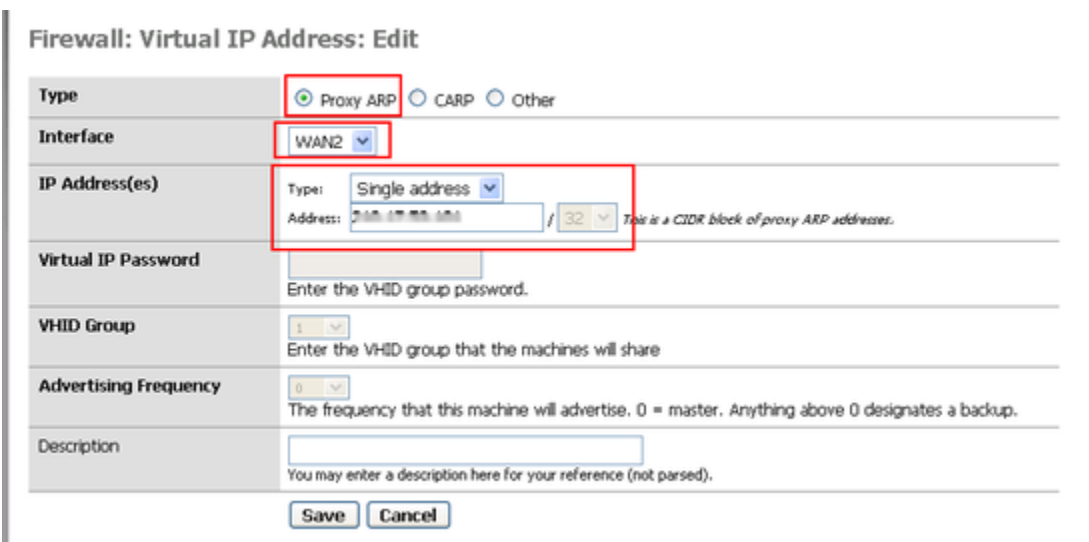


?????? Virtual IPs

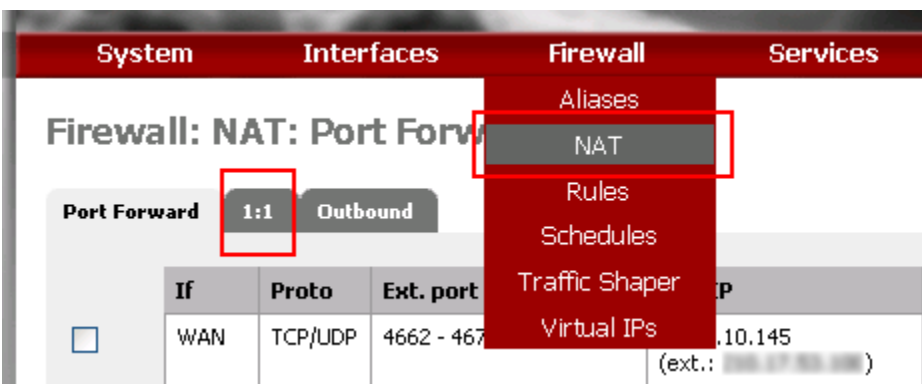
?Firewall??Virtual IPs?



Type ? proxy ARP  
 Interface ? WAN2  
 IP Address ???????? IP ??



?????? NAT 1:1  
 ?Firewall??NAT??1:1?



Interface ? WAN2  
 External subnet ???????? IP ??(????)???? sub-mask ??? 32?  
 Internal subnet ???????? IP ???

### Firewall: NAT: 1:1: Edit

Interface	WAN2	
External subnet	200.1.1.0/24	32
Internal subnet	10.10.10.112	
Description	Test	

??????????

?Firewall??Rules?

System Interfaces Firewall Services

### Firewall: Rules

LAN WAN **WAN2** PPTP VPN

Aliases  
NAT  
**Rules**  
Schedules  
Traffic Shaper  
Virtual IPs

	Proto	Source	Destination	Port	Gateway
<input type="checkbox"/> <input checked="" type="checkbox"/>	TCP/UDP	*		*	*
<input type="checkbox"/> <input checked="" type="checkbox"/>	ICMP	*	*	*	*

Action ? Pass

Interface ? WAN2

Protocol ? TCP/UDP

**Firewall: Rules: Edit**

<b>Action</b>	Pass <input type="button" value="v"/> <small>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.</small>
<b>Disabled</b>	<input type="checkbox"/> <b>Disable this rule</b> <small>Set this option to disable this rule without removing it from the list.</small>
<b>Interface</b>	WAN2 <input type="button" value="v"/> <small>Choose on which interface packets must come in to match this rule.</small>
<b>Protocol</b>	TCP/UDP <input type="button" value="v"/> <small>Choose which IP protocol this rule should match.          Hint: in most cases, you should specify TCP here.</small>
<b>Source</b>	<input type="checkbox"/> <b>not</b> <small>Use this option to invert the sense of the match.</small> Type: any <input type="button" value="v"/> Address: [redacted] / 31 <input type="button" value="v"/> <input type="button" value="Advanced"/> - Show source port range
<b>Source OS</b>	OS Type: any <input type="button" value="v"/> <small>Note: this only works for TCP rules</small>

Destination ?? Any ???????? IP  
 Destination Port ?? Any ??? Port ??

<b>Destination</b>	<input type="checkbox"/> <b>not</b> <small>Use this option to invert the sense of the match.</small> Type: any <input type="button" value="v"/> Address: [redacted] / 31 <input type="button" value="v"/>
<b>Destination port range</b>	from: any <input type="button" value="v"/> [redacted] to: any <input type="button" value="v"/> [redacted] <small>Specify the port or port range for the destination of the packet for this rule.          Hint: you can leave the 'to' field empty if you only want to filter a single port.</small>

?? Ping ??????????????????????

Action ? PASS  
 Interface ? WAN2  
 Protocol ? ICMP  
 ?? Source ? Destination ??? Any ??? ping ???

<b>Action</b>	<input type="text" value="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.
<b>Disabled</b>	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="text" value="WAN2"/> Choose on which interface packets must come in to match this rule.
<b>Protocol</b>	<input type="text" value="ICMP"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.
<b>ICMP type</b>	<input type="text" value="any"/> If you selected ICMP for the protocol above, you may specify an ICMP type here.
<b>Source</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="31"/> <input type="button" value="Advanced"/> - Show source port range
<b>Source OS</b>	OS Type: <input type="text" value="any"/> Note: this only works for TCP rules

<b>Destination</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <input type="text" value="any"/> Address: <input type="text" value=""/> / <input type="text" value="31"/>
<b>Log</b>	<input type="checkbox"/> <b>Log packets that are handled by this rule</b> 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 <a href="#">Diagnostics: System logs: Settings</a> page).
<b>Advanced Options</b>	<input type="button" value="Advanced"/> - Show advanced options

??!!

????

- [How to Setup Failover and Load Balancing in PfSense](#)