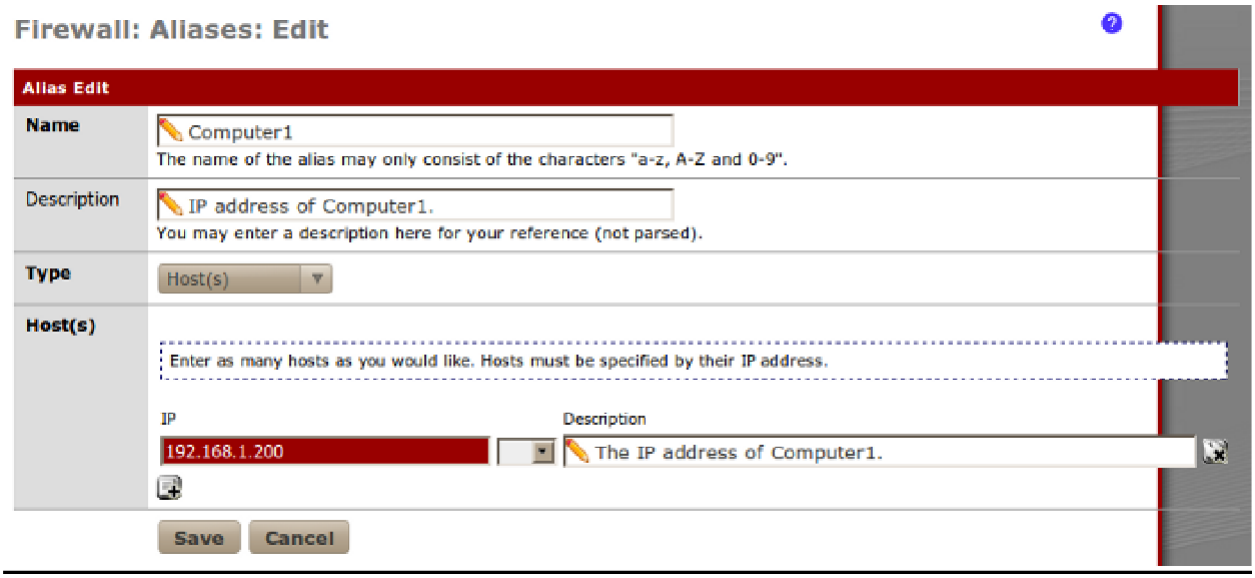
535 pfSense - NAT and Firewall Rules

Step 1: Creating NAT Port-Forwarding Rules

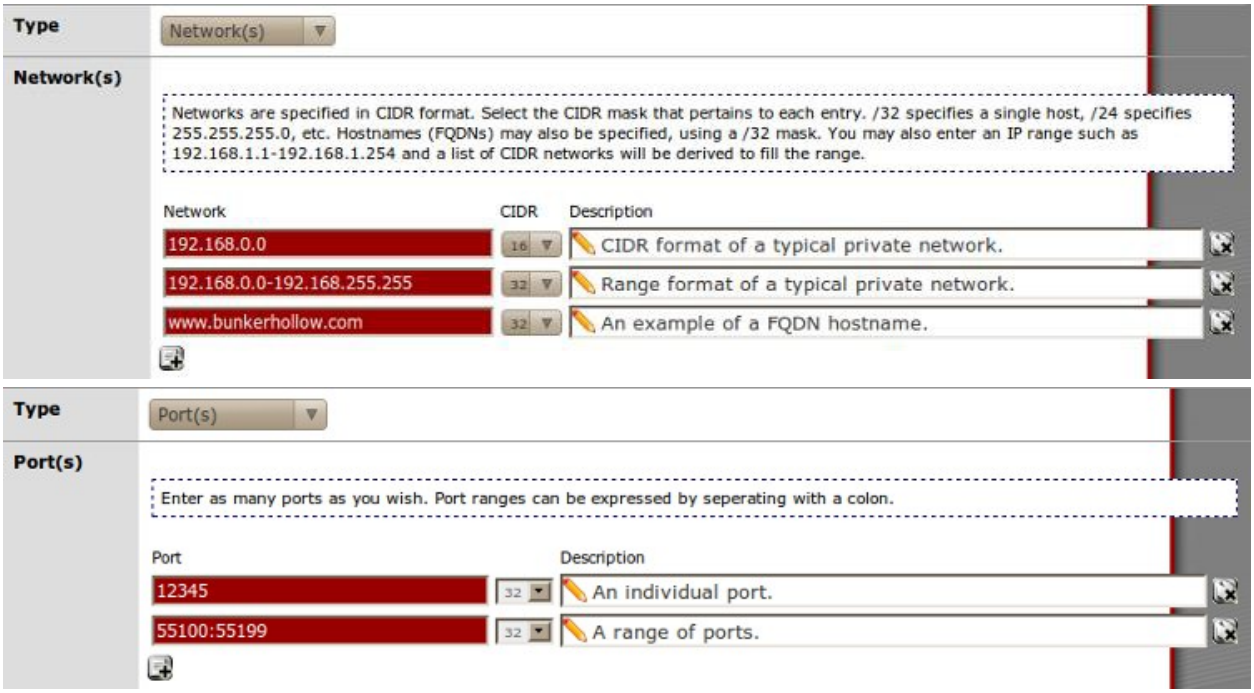
- With a sense of purpose, I delved into the realm of network address translation (NAT) within pfSense, accessing the web interface with eager anticipation.
- Navigating to Firewall > NAT, I embarked on the journey of creating port-forwarding rules by switching to the "Port Forward" tab.
- With a few clicks of the mouse, I initiated the creation of a new port forwarding rule, selecting the WAN interface to direct incoming traffic from the outside world to specific services within my LAN.
- Methodically configuring the rule, I specified the protocol, destination port range, and the internal IP address of the server or device to which the traffic should be forwarded.
- With a sense of satisfaction, I saved the rule and applied changes, confident in its ability to efficiently manage incoming traffic.

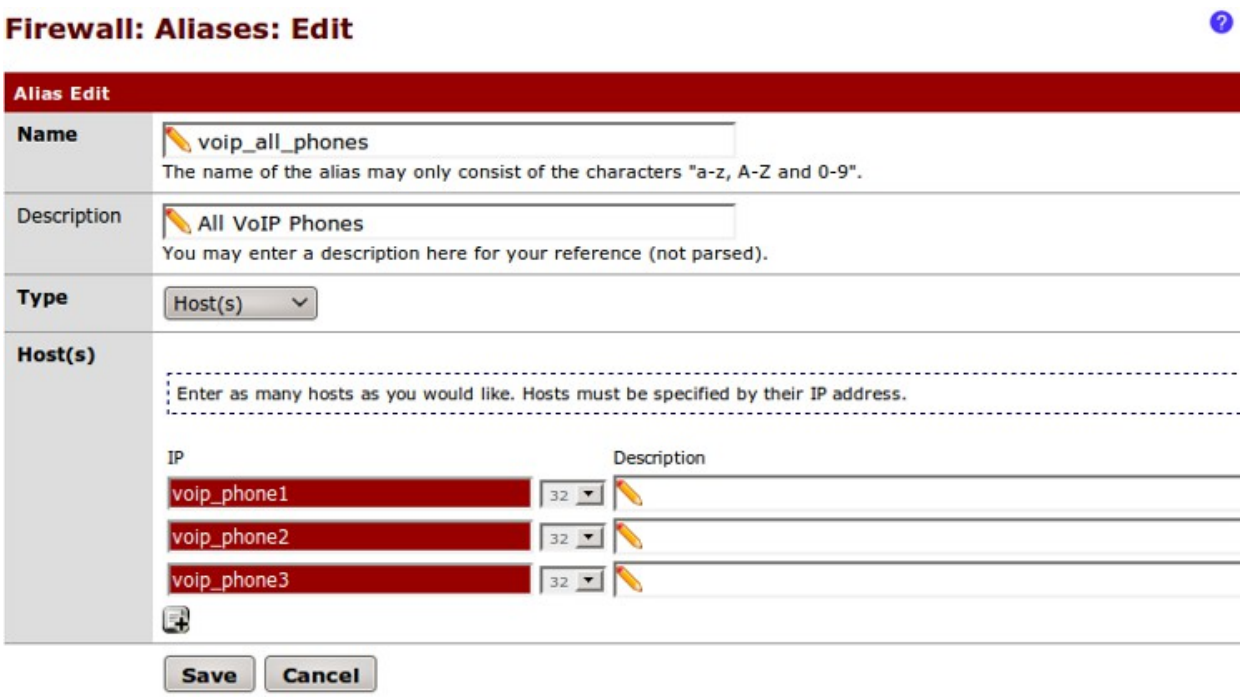


Step 2: Developing Firewall Rules to Control Traffic

- Transitioning seamlessly into the realm of firewall rules, I navigated to Firewall > Rules, ready to define rules to allow or deny traffic based on my network policies.

- With a clear understanding of my objectives, I meticulously crafted each firewall rule, specifying the action (pass, block, or reject), protocol, source, destination, and port as needed.
- Taking care to arrange the rules in the desired order, I ensured that they would be processed from top to bottom, with the first matching rule taking precedence.
- With a sense of purpose, I saved the rules and applied changes, eager to test their efficacy in controlling and directing traffic within my network.





Step 3: Testing and Validating Rules with Various Network Devices

- With a spirit of curiosity, I embarked on the crucial phase of testing and validating the configured rules, ensuring they functioned as intended.
- Testing NAT port forwarding, I attempted to access internal services from external devices using the WAN IP and the forwarded ports, verifying their accessibility.
- Transitioning to testing firewall rules, I generated traffic that matched the defined rules, carefully observing the firewall logs to confirm whether the traffic was allowed or blocked as expected.
- With each successful test and validation, I iterated on the rules as necessary, making modifications and adjustments until achieving the desired outcomes.

Verification and Troubleshooting:

- In the event of any discrepancies or unexpected behavior, I diligently reviewed the configured NAT port-forwarding rules, ensuring the correctness of WAN IP addresses, internal IPs, and port settings.

- Similarly, I meticulously scrutinized the firewall rules, verifying their order and structure to identify any overlapping or conflicting rules that may affect traffic flow.
- Leveraging the diagnostic tools within pfSense, I meticulously reviewed logs and system states, using the insights gained to troubleshoot and resolve any issues related to blocked or allowed traffic.

With a sense of accomplishment, I successfully configured NAT and firewall rules within pfSense, empowering myself to control and direct traffic through my network with precision and confidence.