opnSense DMZ

DMZ

The goal here is to create a DMZ on the same router as our LAN. A DMZ a separate network, which a LAN has access to, but does not have access to the LAN. We can then put servers in the DMZ which we can make publicly available (ie, accessed via public IP's) while maintaining the integrity of our LAN behind the same firewall.

NOTE: this is **not** as secure as having too separate networks with two separate firewalls, as a blackhat could crack one of your publicly available servers, and from there crack your router, then gain access to your LAN. However, it is cheaper, and it is more secure than just putting a server on your LAN with Port Forward access.

To create a DMZ, you'll need a separate network, either through a VLAN or through a separate physical setup. How you get there is up to you, but this article assumes you have a third network interface, and you have named it DMZ (the others labeled LAN and WAN, and they were working before).

We'll set up the DMZ interface, optionally allow a DHCP server on it, then set up some firewall rules. These are absolutely the simplest firewall rules you can get by with, but some of the articles in the Links section will show you more complex (and secure) ideas.

1. DMZ
    1. Enable Interface
    2. Prevent Removal
    3. Static IP
    4. IPV4 Address
    5. auto-detect IPv4 upstream gateway
2. DHCP (optional)
    1. enable for DMZ
    2. set range
3. Firewall (two rules, but see https://homenetworkguy.com/how-to/create-basic-dmz-network-opnsense/)
    1. Allow dmz to access everything but local network
        1. Action: Pass
        2. Interface: DMZ
        3. Protocol: Any
        4. Source: DMZ net
        5. Source port: any
        6. Destination Invert: check
        7. Destination: LAN net
        8. Destination Port: any
        9. Category: DMZ
        10. Description: Allow access to Internet and block access to all local networks
    2. Allow LAN full access to DMZ
        1. Action: pass
        2. Interface: lan

3. TCP/IP Version: IPV4+IPv6
4. protocol: tcp
5. source: LAN net
6. Source port: any
7. Destination: DMZ net
8. Destination Port: any
9. Category: DMZ
10. Description: Allow access to web server in DMZ network from LAN

NAT a DMZ machine using Port Forward

NAT (Network Address Translation) allows you to use one IP address to access multiple internal machines, so long as they have unique network port requirements. For example, you could have a public web server on port 80 and 443 (http and https), then a separate server for e-mail using smtp(s) (ports 25,465, 587), imap(s) (ports 143 and 993) and pop(s) (ports 110 and 995). They could both be on the same public IP address, and NAT would send all http(s) traffic to one machine and all e-mail traffic to the other. Obviously, these machines could be inside a DMZ.

Why do you want to do this? Several reasons, but the main one is to decrease complexity in your servers. You have one server which is only a web server, with apache, php and maybe mysql. A completely separate machine handles your e-mail.

OPNSense has NAT built in, but parts of it are broken as of 23.7; it may be fixed by the time you read this, so I'll show the standard way of doing it, then the patch.

Firewall Aliases

You can skip this first step, though I like it because it makes the entire setup more maintainable. I like to use Firewall Aliases for my ports and, sometimes, for my hosts. I would definitely recommend doing the ports part, however, as you would otherwise have to write one NAT for each port.

1. Firewall | Aliases
2. Add (plus sign)
    1. Name: web_ports
    2. Type: Ports
    3. Categories: DMZ
    4. Contents: enter the web ports, placing a comma between them (ie, 80,443)
    5. Description: Ports used by web server
    6. Save
3. Add (plus sign)
    1. Name: mail_ports
    2. Type: Ports
    3. Categories: DMZ
    4. Content: 25,465,587
    5. Description: Ports used by mail server
    6. Save
4. Add
    1. Name: webserver

2. Type: Host(s)
3. Categories: DMZ
4. Content: 192.168.52.3 (the IP of your web server, in the DMZ)
5. Description: the target for our web traffic
6. Save

5. Add
    1. Name: mailserver
    2. Type: Host(s)
    3. Categories: DMZ
    4. Content: 192.168.52.4 (the IP of your mail server, in the DMZ)
    5. Description: the target for our mail traffic
    6. Save

Build the Forward

All that is left to do is tell the router to forward the port groups to the appropriate host.

1. Firewall | NAT | Port Forward
    1. Add
        1. Interface: WAN
        2. TCP/IP Version: Select your requirements
        3. Protocol: TCP (or, TCP/UDP if you also need UDP)
        4. Destination: WAN address
        5. Destination port range: Select web_ports from the dropdown (hint, it is higher in the dropdown)
        6. Redirect target IP:
            1. Single host or Network
                1. If you created an alias, select web_server from the dropdown
                2. if not, enter the IP address of the target machine
        7. Redirect target port: should be already set to web_ports
        8. Category: DMZ
        9. Description: forward web ports to web server
        10. NAT reflection: Use system default (**See Below**)
        11. Filter rule association: Associate this with a regular firewall rule. (**See Below**)
        12. Save
    2. Repeat for other server(s)

Note: Here we are forwarding ports to the same port on the internal target server. So, port 25 on the WAN targets port 25 on the mail server. This is NOT a requirement, though I don't think you can use aliases on the ports (never tried). Simply choose the Destination Port (25) as what you want on the public IP, then choose a different *Redirect target port* for what it translates to the server. One reason to do this is to hide the actual ports. For example, you might want to use port 54321 as your ssh port to a specific server from the outside. You could change the port in the sshd config, but if you simply put 54321 as the Destination Port (both start and finish), the put port 22 as the Redirection Port, you don't have to reconfigure your server.

NAT Reflection

NAT Reflection is a nice little function that rewrites network traffic if you are in the LAN and try to

access a DMZ IP by it's public IP. This cuts down on your public IP network traffic, short circuiting the whole “out and in” thing.

You can set NAT Reflection manually for each NAT, but you can also just set a system default and leave that. To set the default on NAT Reflection to On for all NAT's that have the default, do the following:

1. Firewall | Settings | Advanced
2. Place a check box in Reflection for port forwards
3. You might also want *Reflection for 1:1* and *Automatic outbound NAT for Reflection*, but I won't go into that. The latter is definitely not necessary in this case.

Filter rule association

As of v23.7, the *Associate this with a regular firewall rule* does not appear to generate the correct rules. The rule shows up in the firewall, but does not work.

This has been reported a few times (see https://forum.homenetworkguy.com/index.php?topic=128.0] for one of them, and I'm assuming the excellent coders will fix it soon, but a work around is to choose *Pass* as the correct value for this. **Note:** You can change *Associate this with a regular firewall rule* to *Pass* with no problem, but once it is set to *Pass* you can not change back.

Links

- https://homenetworkguy.com/how-to/create-basic-dmz-network-opnsense/
- https://doc.m0n0.ch/handbook/examples.html
- https://homenetworkguy.com/how-to/create-basic-dmz-network-opnsense/
- https://docs.opnsense.org/manual/nat.html
- https://forum.opnsense.org/index.php?topic=5424.0
- https://forum.opnsense.org/index.php?topic=5174.0
- https://forum.opnsense.org/index.php?topic=429.0
- https://doubleoctopus.com/security-wiki/network-architecture/demilitarized-zone/
- https://docs.opnsense.org/manual/how-tos/carp.html
- https://docs.opnsense.org/manual/hacarp.htmlnetwork-opnsense/