Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

Home > Faq > CentOS

Linux Demilitarized Zone (DMZ) Ethernet Interface Requirements and Configuration

Posted by Vivek Gite <vivek@nixcraft.com>

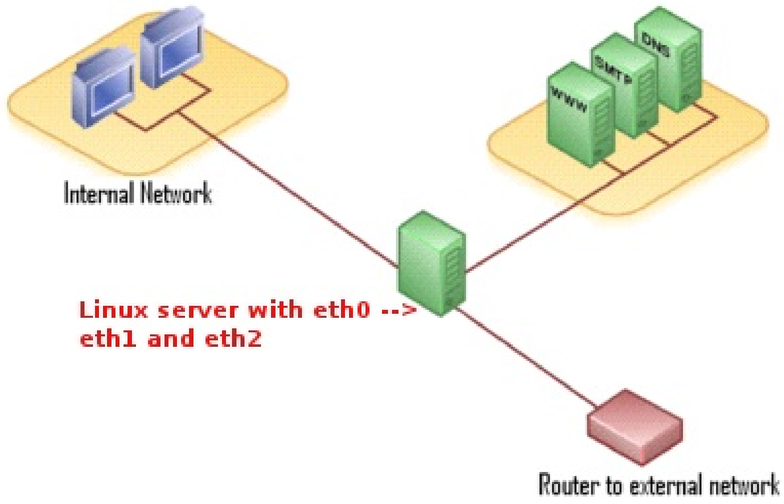
[1]

Q. Can you tell me more about Linux Demilitarized Zone and Ethernet Interface Card Requirements for typical DMZ implementation? How can a rule be set to route traffic to certain machines on a DMZ for HTTP or SMTP?

A. Demilitarized zone, used to secure an internal network from external access. You can use Linux firewall to create DMZ easily. There are many different ways to design a network with a DMZ. The basic method is to use a single Linux firewall with 3 Ethernet cards. The following simple example discusses DMZ setup and forwarding public traffic to internal servers.

Sample Example DMZ Setup

Consider the following DMZ host with 3 NIC:
[a] eth0 with *192.168.1.1* private IP address - Internal LAN ~ Desktop system
[b] eth1 with *202.54.1.1* public IP address - WAN connected to ISP router
[c] eth2 with *192.168.2.1* private IP address - DMZ connected to Mail / Web / DNS and other private servers



[2]

(Fig 01: A typical Linux based DMZ setup [Image modified from Wikipedia article])

Routing traffic between public and DMZ server

To set a rule for routing all incoming SMTP requests to a dedicated Mail server at IP address 192.168.2.2 and port 25, network address translation (NAT) calls a PREROUTING table to forward the packets to the proper destination.

This can be done with appropriate IPTABLES firewall rule to route traffic between LAN to DMZ and public interface to DMZ. For example, all incoming mail traffic from internet (202.54.1.1) can be send to DMZ mail server (192.168.2.2) with the following iptables prerouting rule (assuming default DROP all firewall policy):

```
### end init firewall .. Start DMZ stuff ####
# forward traffic between DMZ and LAN
iptables -A FORWARD -i eth0 -o eth2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# forward traffic between DMZ and WAN servers SMTP, Mail etc
iptables -A FORWARD -i eth2 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Route incoming SMTP (port 25 ) traffic to DMZ server 192.168.2.2
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 25 -j DNAT --to-destinat
```

```
# Route incoming HTTP (port 80 ) traffic to DMZ server load balancer IP 192.168.2.3
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 80 -j DNAT --to-destinat

# Route incoming HTTPS (port 443 ) traffic to DMZ server reverse load balancer IP 192.168.2
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 --dport 443 -j DNAT --to-destina
### End DMZ .. Add other rules ###
```

Where,

- **-i eth1** : Wan network interface
- **-d 202.54.1.1** : Wan public IP address
- **--dport 25** : SMTP Traffic
- **-j DNAT** : DNAT target used set the destination address of the packet with --to-destination
- **--to-destination 192.168.2.2**: Mail server ip address (private IP)

Multi port redirection

You can also use multiport iptables module to matches a set of source or destination ports. Up to 15 ports can be specified. For example, route incoming HTTP (port 80) and HTTPS (port 443) traffic to WAN server load balancer IP 192.168.2.3:

```
iptables -t nat -A PREROUTING -p tcp -i eth1 -d 202.54.1.1 -m multiport --dport 80,443 -j I
```

Pitfalls

Above design has few pitfalls:

1. **Single point of failure - The firewall becomes a single point of failure for the network.**
2. **Hardware - The firewall Host must be able to handle all of the traffic going to the DMZ as well as the internal network.**

Linux / BSD Firewall Distros

If you find above discussion little hard to digest, I suggest getting a Linux / BSD distribution which aims to provide a simple-to-manage firewall appliance based on PC hardware to setup DMZ and gateways:

- IPCop [3]
- Shorewall [4]
- PfSense [5] (FreeBSD based)

Further readings:

- Wes Sonnenreich. Building Linux And Openbsd Firewalls. [6] - A step-by-step guide to bulding a commercial-grade firewall with open source software.
- Eric Maiwald. Network Security: A Beginner's Guide. Second Edition. [7] - It gives a brief overview of most of the security related topics, perhaps one of the best books to start with.
- Michael Rash. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort [ILLUSTRATED] [8] - Linux Firewalls discusses the technical details of the iptables firewall and the Netfilter framework that are built into the Linux kernel, and it explains how they provide strong filtering, Network Address Translation (NAT), state tracking, and application layer inspection capabilities that rival many commercial tools. You'll learn how to deploy iptables as an IDS with psad and fwsnort and how to build a strong, passive authentication layer around iptables with fwknop.

Updated for accuracy.

you don't miss a single tip/tricks. Alternatively, subscribe via RSS/XML feed.

Article printed from Frequently Asked Questions About Linux / UNIX: **http://www.cyberciti.biz/faq/**

URL to article: **http://www.cyberciti.biz/faq/linux-demilitarized-zone-howto/**

URLs in this post:

[1] Image: **http://www.cyberciti.biz/faq/faq/category/linux/**
[2] Image: **http://www.cyberciti.biz/faq/wp-content/uploads/2007/12/linux-dmz-network-diagram-firewall.png**
[3] IPCop: **http://ipcop.org/**
[4] Shorewall: **http://shorewall.net/**
[5] PfSense: **http://www.pfsense.com/**
[6] Wes Sonnenreich. Building Linux And Openbsd Firewalls.: **http://www.amazon.com/gp/redirect.html?ie=UTF8&location=http%3A%2F%2Fwww.amazon.com%2FBuilding-Linux-Openbsd-Firewalls-Sonnenreich%2Fdp%2F0471353663%3Fie%3DUTF8%26s%3Dbooks%26qid%3D1197694572%26sr%3D8-2&tag=cyberciti-20&linkCode=ur2&camp=1789&creative=9325**
[7] Eric Maiwald. Network Security: A Beginner's Guide. Second Edition.: **http://www.amazon.com/gp/redirect.html?ie=UTF8&location=http%3A%2F%2Fwww.amazon.com%2FNetwork-Security-Beginners-Guide-Second%2Fdp%2F0072229578%3Fie%3DUTF8%26s%3Dbooks%26qid%3D1197694870%26sr%3D8-1&tag=cyberciti-20&linkCode=ur2&camp=1789&creative=9325**
[8] Michael Rash. Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort [ILLUSTRATED]: **http://www.amazon.com/gp/redirect.html?ie=UTF8&location=http%3A%2F%2Fwww.amazon.com%2FLinux-Firewalls-Detection-Response-iptables%2Fdp%2F1593271417%3Fie%3DUTF8%26s%3Dbooks%26qid%3D1197694572%26sr%3D8-3&tag=cyberciti-20&linkCode=ur2&camp=1789&creative=9325**