

Firewall and Advanced Packet Routing

Getting the MOST out of your LINUX firewall box

You may be wondering, "I have given due attention to my Application and Operating System level security, why would I need a firewall or what is a firewall and how will that benefit my business?"

Well, you may want to ponder over the following before making any rational decisions:

- * Your corporate network uses a leased line provided by a third party for internet access. The bad news is, your organization does not control the physical security of those lines. Is there any useful first step towards controlling traffic to and from your LAN?
- * The internet is not the environment you intent to trust. How can you possibly disclose very little information about your Network layout, but still get your job done? How do you get the internet to see your network as a single Host?
- * Your network happens to be huge, and it's sub-netted. Another thing is, it sees all kinds of traffic; voice traffic (which requires low latency and high throughput), web traffic, SSH sessions etc. How can you handle all these traffic, and still get the most out of your finite bandwidth?
- * Let's say you want your public servers to be accessible to the internet. To get this to work, you need, at a minimum, a routable address for each server. The catch is, routable addresses are not free. The question is, is there a work-around? This is the only course which makes you prepare for a solid scripting foundation which requires for Linux automation.

Who should attend

System administrators, network administrators and software developers who want to implement Firewall.

prerequisites

Attendees should already have a basic understanding of the Internet and Unix operating systems. You should already be comfortable with editing configuration files and installing software on your system. You should understand fundamentals such as networking, user-ids, file systems, service management and file permissions.

Prior knowledge of firewall and packet routing is not required.

ENROLL FOR OUR TRAINING

Course Outline

UNIT 1: Firewall Concepts

What is firewall?

What is Packet Filtering?

Network Address Translation (NAT)?

IPTables modules and supporting files

IPTables Access Control List (ACL) syntax

ACL management

LAB Task: Save & Restore IPTables ACLs

UNIT 2: Chain Management

Usage of Default Tables:

Filter

NAT

Mangle

Explore Chains in the default tables

INPUT: For packets send to this host

OUTPUT: For packets send from this host

FORWARD: For packets send through this host

PREROUTING: For DNAT

POSTROUTING: For SNAT

UNIT 3: Usage of Iptables Command

List rules

Flush rules

Append rules

UNIT 4: Packet Matching & Handling

Source/Dest IPs, Source/Dest Ports

Packet matching/handling based on

TCP streams

UDP datagrams

ICMP Traffic

UNIT 5: Match Handling - Iptables Target

Write rules with the below targets for packet handling

REJECT

LOG

ACCEPT

DROP

SNAT

DNAT

REDIRECT

UNIT 6: ICMP Types

echo-request

echo-reply

LAB Exercises:

LAB 1: Drop ICMP Packets for inbound and outbound

LAB 2: Denying SSH Connection for port 22

LAB 3: Protect against Spoofed Addresses

LAB 4: Configure Outgoing TCP/UDP Connections

LAB 5: Writing rules to match packets based on layer-2 addresses

UNIT 7: State Maintenance - Stateful Firewall

Concept: Stateless Connection / Statefull Connection

Types of states:

NEW

ESTABLISHED

RELATED

INVALID

List kernel modules to support the stateful firewall

Deploying stateful TCP inspection

UNIT 8: Iptables Logging

Access Control Entry (ACEs) to perform logging

Log traffic

Implement catch-all ACE

Label the log entries

UNIT 9: Iptables Statistics

Packet counts & bytes traversing the various chains

Reset all counters

UNIT 10: Packet Routing

Linux Router

Forward chain

Write ACEs to permit routing

Talk: IPTables/Netfilter Recent Module

UNIT 11: Network Address Translation (NAT)

Iptables Masquerading:

Usage: POSTROUTING

Usage: Source NAT (SNAT)

Usage: PREROUTING

Usage: Destination NAT (DNAT)

UNIT 12: Configure Port Forwarding:

Usage: sysctl

sysctl.conf

UNIT 13: Demilitarized Zone (DMZ) Configuration

Port Address Translation (PAT) rules to permit inbound traffic

DMZ forwarding (Routing)

LAB Exercises:

Creating user defined chains

Zero packet counts & bytes - bandwidth usage monitoring

Allowing access to ssh in day time: 9am to 6pm

Allowing DNS Access To Your Firewall

Allowing WWW And SSH Access To Your Firewall

Deploy Transparent Proxying

UNIT 14: Linux advanced routing

It is implemented in two parts:

1. Rules

2. Routing tables

UNIT 15: The Tools

ip command

iproute2

tc command

cbq.init

Marriage of iproute2, iptables, kernel

UNIT 16: Linux Quality of Service

Using the traffic control and netfilter infrastructure to manage bandwidth more effectively and how to collect

statistics to aid with that process.