Role of Firewall, IPS
&
IDS Model

NAVNEET
Scientist `B`
CERT-In, DIT

Firewall

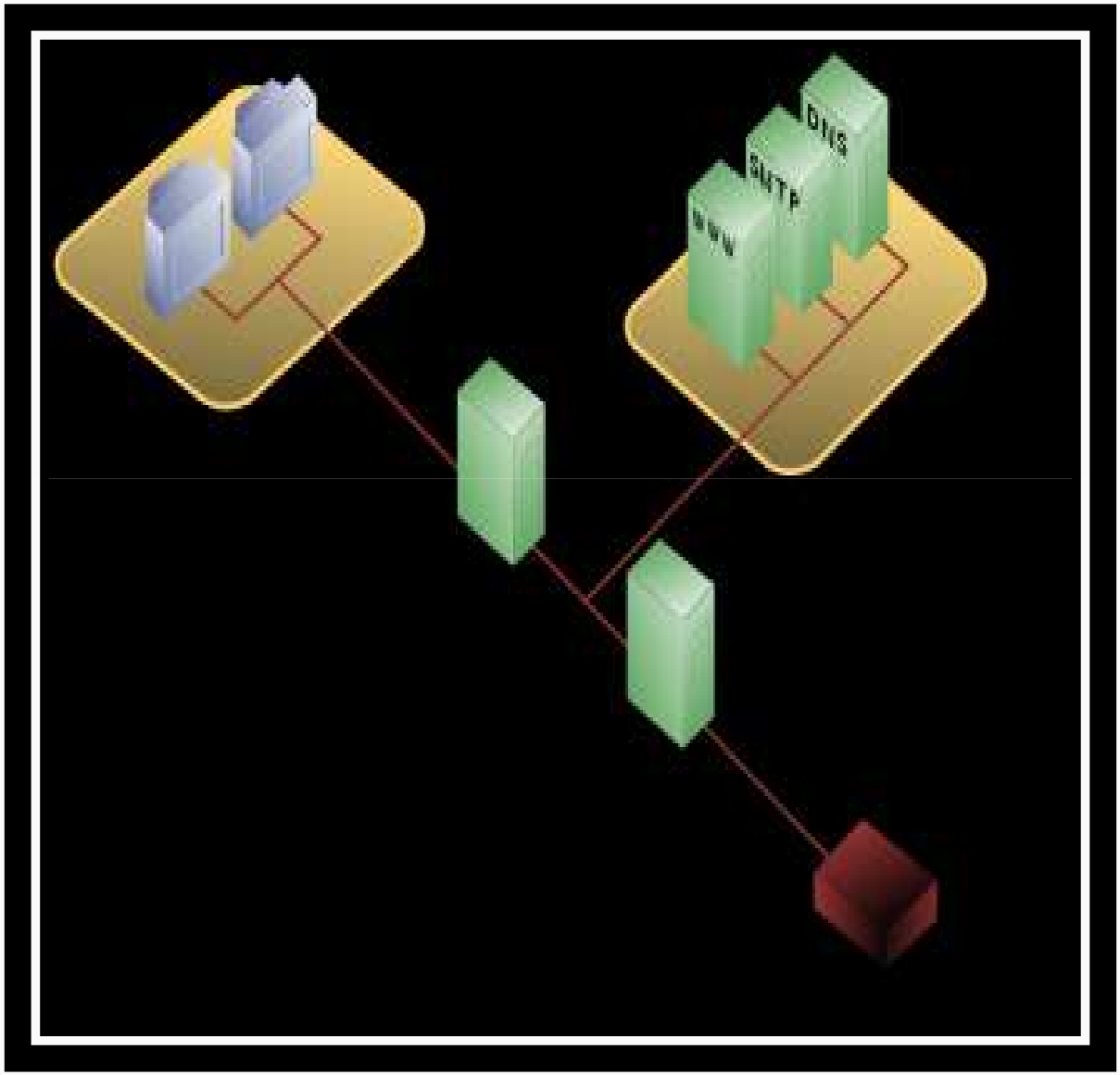
- A firewall is a hardware or software system that prevents unauthorized access to or from a network.
- Implemented in both hardware and software, or a combination of both.
- Sits between two networks
  - Used to protect one network from the other
  - Places a bottleneck between the networks
    - All communications must pass through the bottleneck – this gives us a single point of control

Firewall Functions

- Filtering
- Inspection
- Detection
- Logging
- Alerting
- Allow Address Reuse

Securing DMZ

- Single/ Dual Firewalls is used in creating DMZ



Types of Firewall

- NETWORK LAYER FIREWALLS
- APPLICATION LAYER FIREWALLS
  (Proxy firewall)
- UNIFIED THREAT MANAGEMENT
- WEB APPLICATION FIREWALL

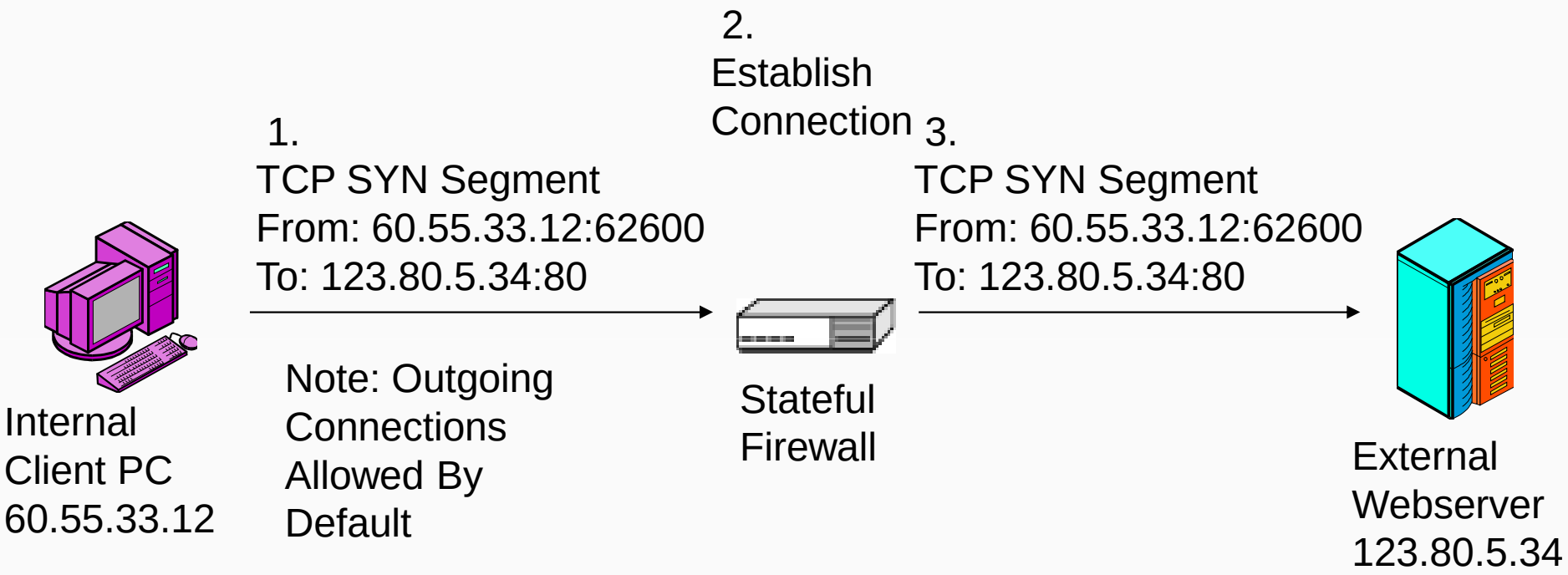
Network layer firewall

- Not allowing packets to pass through the firewall unless they match the established filter rule set.
- Firewall administrator may define the rules
- Filtering rules is based on source and destination address and ports.
- Operates very fast.
- Network layer firewalls generally fall into two sub-categories, stateful and non-stateful.

Stateful Firewall

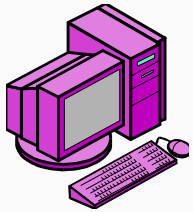
- State of Connection: Open or Closed
  - State: Order of packet within a dialog
  - Often simply whether the packet is part of an open connection

- Stateful Firewall Operation
  - For TCP, record two IP addresses and port numbers in state table as OK (open)
  - By default, permit connections from internal clients (on trusted network) to external servers (on untrusted network)
    - This default behavior can be changed with an ACL
  - Accept future packets between these hosts and ports with little or no inspection



Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

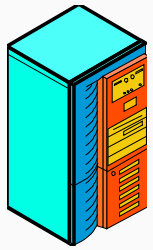


Internal
Client PC
60.55.33.12

6.
TCP SYN/ACK Segment
From: 123.80.5.34:80
To: 60.55.33.12:62600

Stateful
Firewall

4.
TCP SYN/ACK Segment
From: 123.80.5.34:80
To: 60.55.33.12:62600



External
Webserver
123.80.5.34

5.
Check Connection
OK

Connection Table

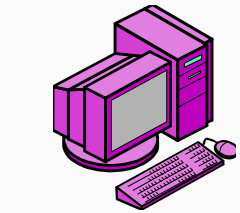
Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK

- Stateful Firewall Operation
  - For UDP, also record two IP addresses in port numbers in the state table

Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	OK
UDP	60.55.33.12	63206	1.8.33.4	69	OK

Port-Switching Applications with Stateful Firewalls



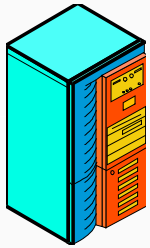
Internal
Client PC
60.55.33.12

1.
TCP SYN Segment
From: 60.55.33.12:62600
To: 123.80.5.34:21

2.
To Establish
Connection

Stateful
Firewall

3.
TCP SYN Segment
From: 60.55.33.12:62600
To: 123.80.5.34:21

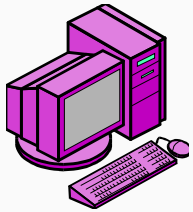


External
FTP Server
123.80.5.34

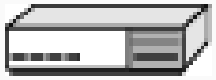
State Table

	Type	Internal IP	Internal Port	External IP	External Port	Status
Step 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK

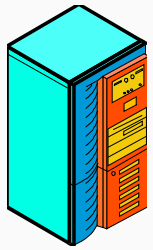
Port-Switching Applications with Stateful Firewalls



Internal
Client PC
60.55.33.12



Stateful
Firewall



External
FTP
Server
123.80.5.34

6.
TCP SYN/ACK Segment
From: 123.80.5.34:21
To: 60.55.33.12:62600
Use Ports 20
and 55336 for
Data Transfers

5.
To Allow,
Establish
Second
Connection

4.
TCP SYN/ACK Segment
From: 123.80.5.34:21
To: 60.55.33.12:62600
Use Ports 20
and 55336 for
Data Transfers

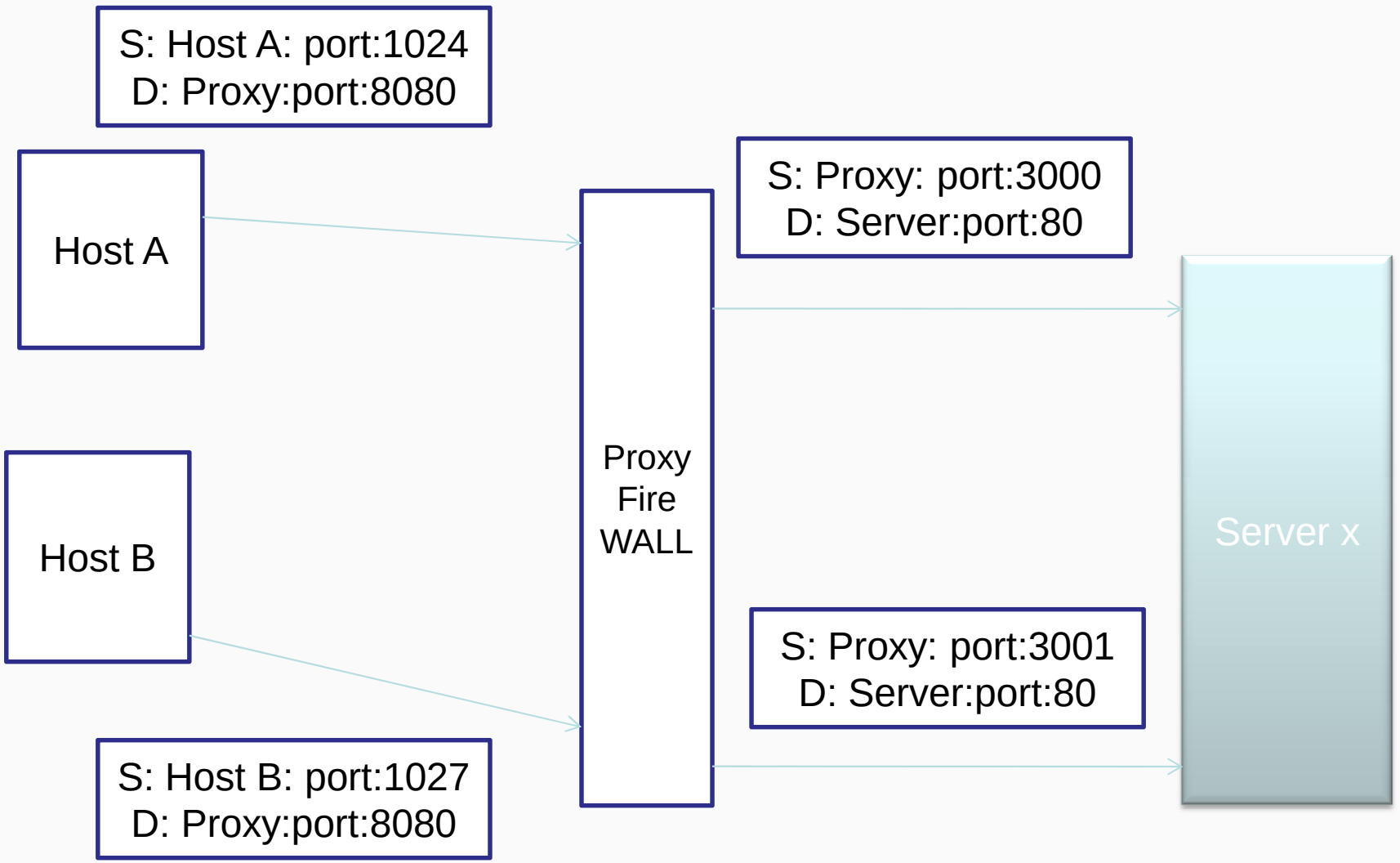
State Table

	Type	Internal IP	Internal Port	External IP	External Port	Status
Step 2 →	TCP	60.55.33.12	62600	123.80.5.34	21	OK
Step 5 →	TCP	60.55.33.12	55336	123.80.5.34	20	OK

Stateful Inspection Firewalls

- Stateful Inspection Access Control Lists (ACLs)
  - Primary allow or deny applications
  - Simple because probing attacks that are not part of conversations do not need specific rules because they are dropped automatically
  - In integrated firewalls, ACL rules can specify that messages using a particular application protocol or server be authenticated or passed to an application firewall for inspection

Network-based application firewall Proxy Firewall



Web Application Firewall

- A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation.
- These rules cover common attacks such as Cross-site Scripting(XSS) and SQL Injection.
- Customizing the rules according to your application.
- Many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

Web Application Risks

- Potential damage:
  - Defacement
  - Client attacks
  - DoS/DDoS
  - Data manipulation / retrieval / deletion

  Attack techniques:
  - SQL / Command injection
  - Cross-site scripting (XSS)
  - Cookie poisoning
  - Session hijacking
  - More….

Unified Threat Management (UTM)

- Unified Threat Management is a firewall appliance that not only guards against intrusion but performs content filtering, spam filtering, intrusion detection and anti-virus duties traditionally handled by multiple systems.

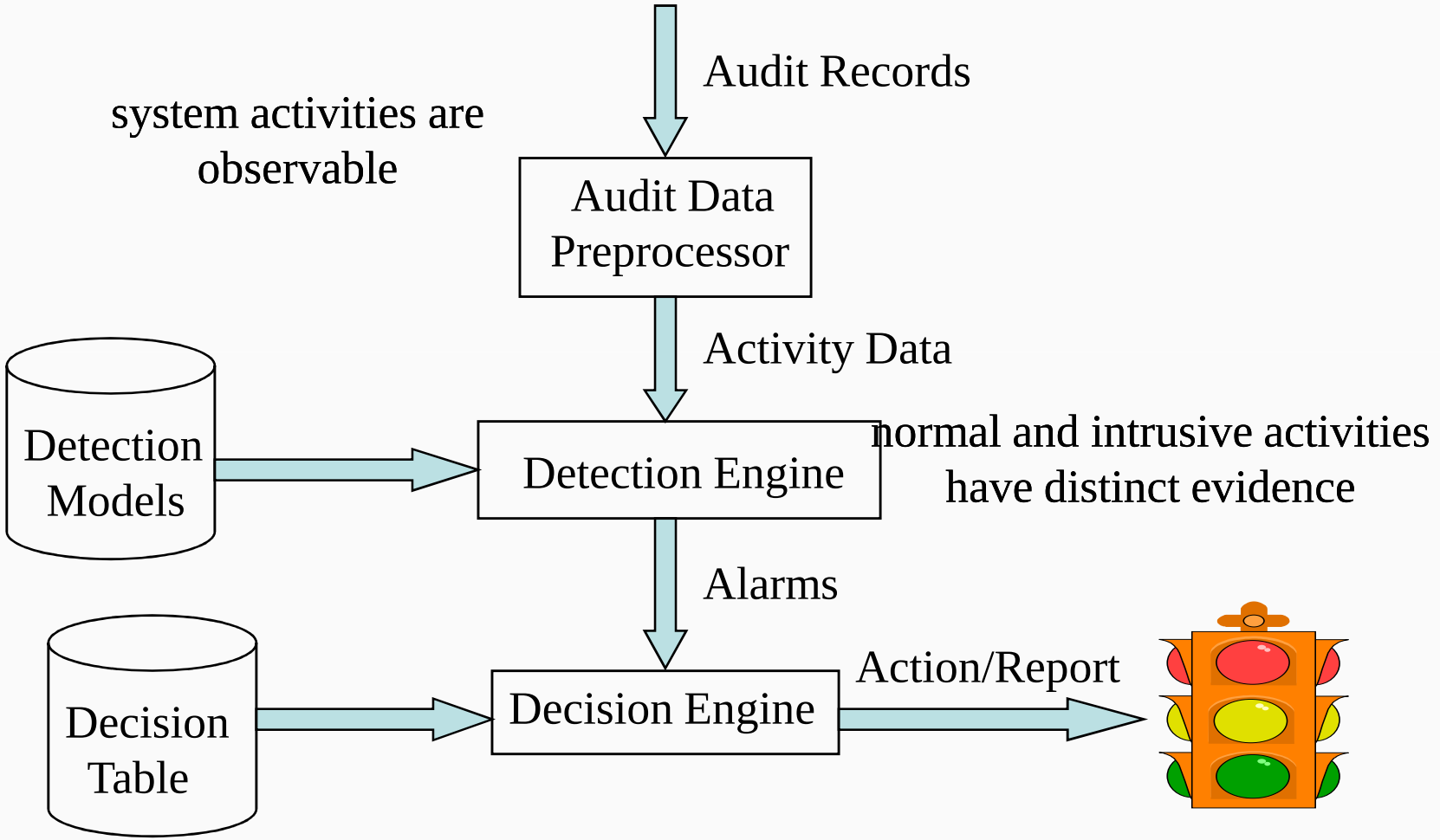
Free Firewall software packages

- IP Tables
  - comes with most linux distributions
- SELinux (Security Enabled Linux – NSA)
  - comes with some Linux distributions
    - Fedora, Red Hat
- IPCop – specialized Linux distribution

Intrusion Detection/Prevention System

- Intrusion
  - A set of actions aimed to compromise the security goals, namely
    - Integrity, confidentiality, or availability of a computing and networking resource
- Intrusion detection
  - The process of identifying and responding to intrusion activities
- Intrusion prevention
  - Extension of ID with exercises of access control to protect computers from exploitation

Components of Intrusion Detection System



Types of Intrusion Detection

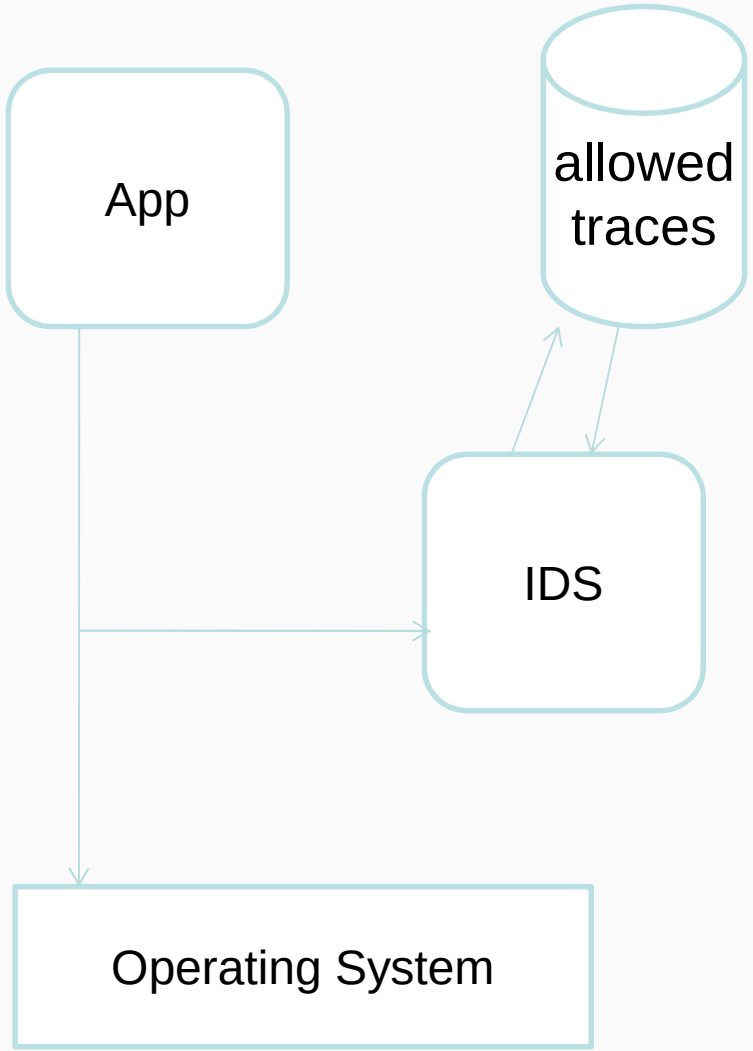
Based on the sources of the audit information used by each IDS, the IDSs may be classified into

- Host-base IDSs
- Distributed IDSs
- Network-based IDSs

- Host-based IDSs
  - Get audit data from host audit trails.
  - Detect attacks against a single host
- Distributed IDSs
  - Gather audit data from multiple host and possibly the network that connects the hosts
  - Detect attacks involving multiple hosts
- Network-Based IDSs
  - Use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services
  - Detect attacks from network.

Anomaly detection:

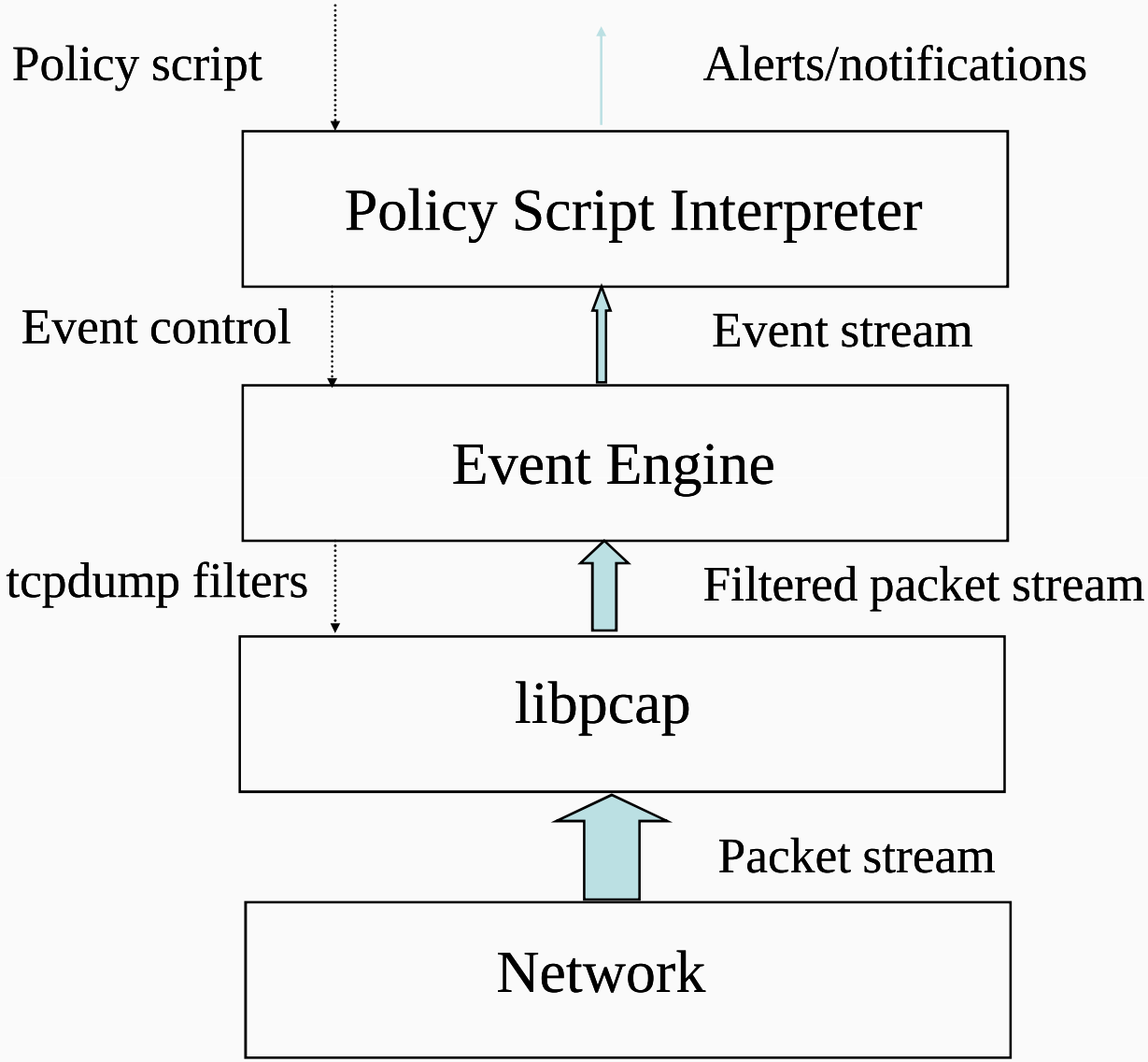
- IDS monitors system call trace from the app
- DB contains a list of subtraces that are allowed to appear
- Any observed subtrace not in DB sets off alarms



Network IDSs

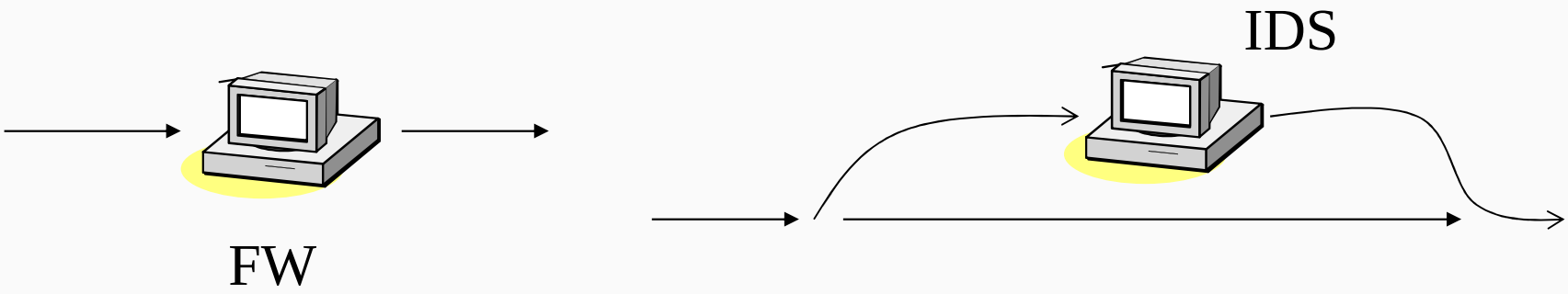
- Deploying sensors at strategic locations
  - E.G., Packet sniffing via *tcpdump* at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
- Monitoring user activities
  - Look into the data portions of the packets for malicious command sequences
- May be easily defeated by encryption
  - Data portions and some header information can be encrypted
  - The decryption engine still there.
- Other problems …

Architecture of Network IDS



Firewall Versus Network IDS

- Firewall
  - Active filtering
  - Fail-close
- Network IDS
  - Passive monitoring
  - Fail-open



Requirements of Network IDS

- High-speed, large volume monitoring
  - No packet filter drops
- Real-time notification
- Mechanism separate from policy
- Extensible
- Broad detection coverage
- Economy in resource usage

Intrusion Detection Techniques

- Misuse detection
  - Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities.
- Anomaly detection
  - Detect any action that significantly deviates from the normal behavior.

Misuse Detection

- Based on known attack actions.
- Feature extract from known intrusions
- Integrate the Human knowledge.
- The rules are pre-defined
- Disadvantage:
  - Cannot detect novel or unknown attacks

Anomaly Detection

- Based on the normal behavior of a subject. Sometime assume the training audit data does not include intrusion data.
- Any action that significantly deviates from the normal behavior is considered intrusion.

Anomaly Detection Methods

Method
Statistical method
Machine Learning techniques • Time-Based inductive Machine • Instance Based Learning • Neural Network • …
Data mining approaches

Anomaly Detection Disadvantages

- Based on audit data collected over a period of normal operation.
  - When a noise(intrusion) data in the training data, it will make a mis-classification.
- How to decide the features to be used. The features are usually decided by domain experts.

Misuse Detection vs. Anomaly Detection

	Advantage	Disadvantage
Misuse Detection	Accurately and generate much fewer false alarm	Cannot detect novel or unknown attacks
Anomaly Detection	Is able to detect unknown attacks based on audit	High false-alarm and limited by training data.

Difference between IDS & FIREWALL

- IDS are a dedicated assistant used to monitor the rest of the security infrastructure
- Today's security infrastructure are becoming extremely complex, it includes firewalls, identification and authentication systems, access control product, virtual private networks, encryption products, virus scanners, and more. All of these tools performs functions essential to system security. Given their role they are also prime target and being managed by humans, as such they are prone to errors.
- Failure of one of the above component of your security infrastructure jeopardized the system they are supposed to protect

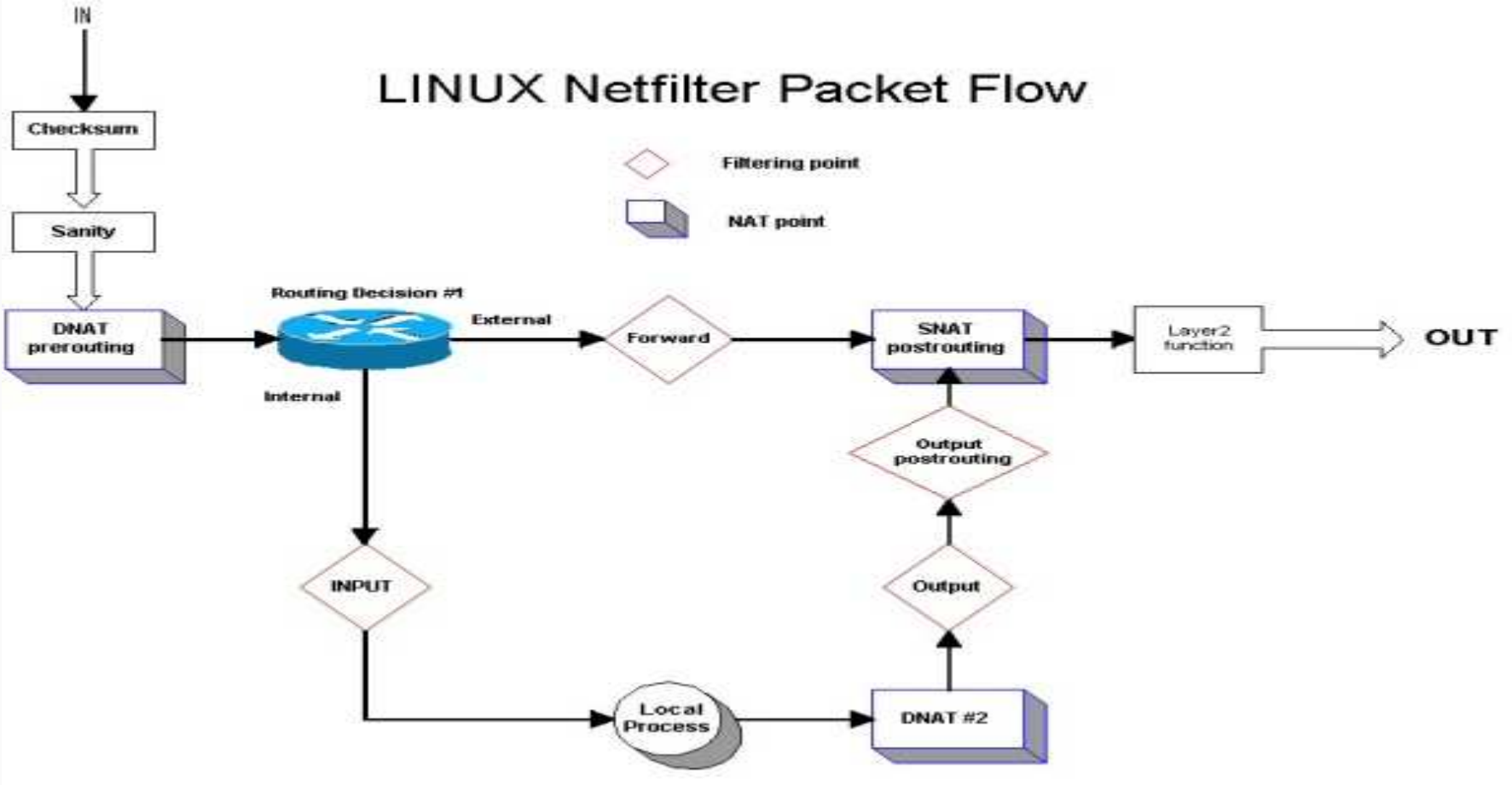
- Not all traffic may go through a firewall
  i:e modem on a user computer
- Not all threats originates from outside. As networks uses more and more encryption, attackers will aim at the location where it is often stored unencrypted (Internal network)
- Firewall does not protect appropriately against application level weakenesses and attacks
- Firewalls are subject to attacks themselves
- Protect against misconfiguration or fault in other security mechanisms

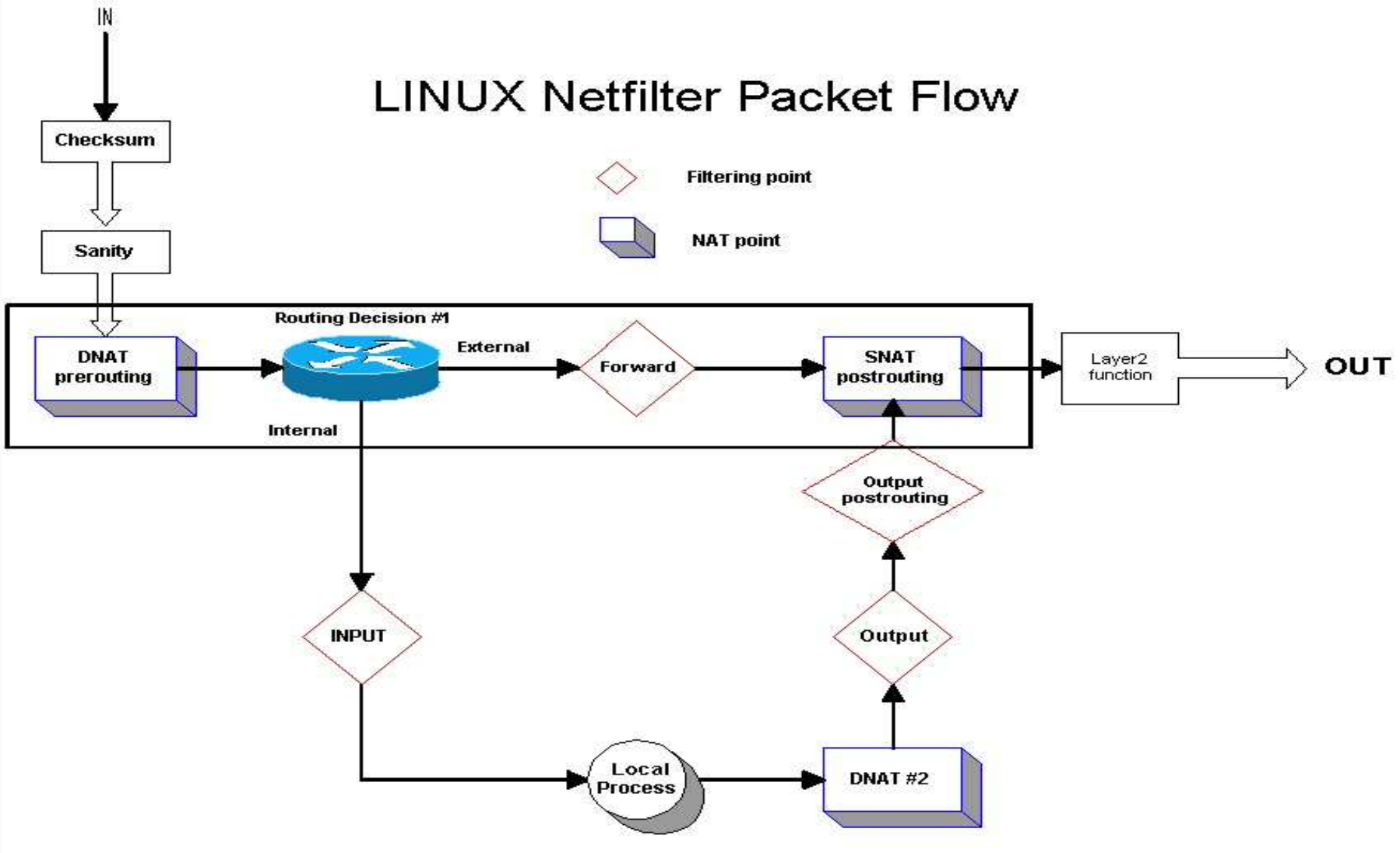
iptables

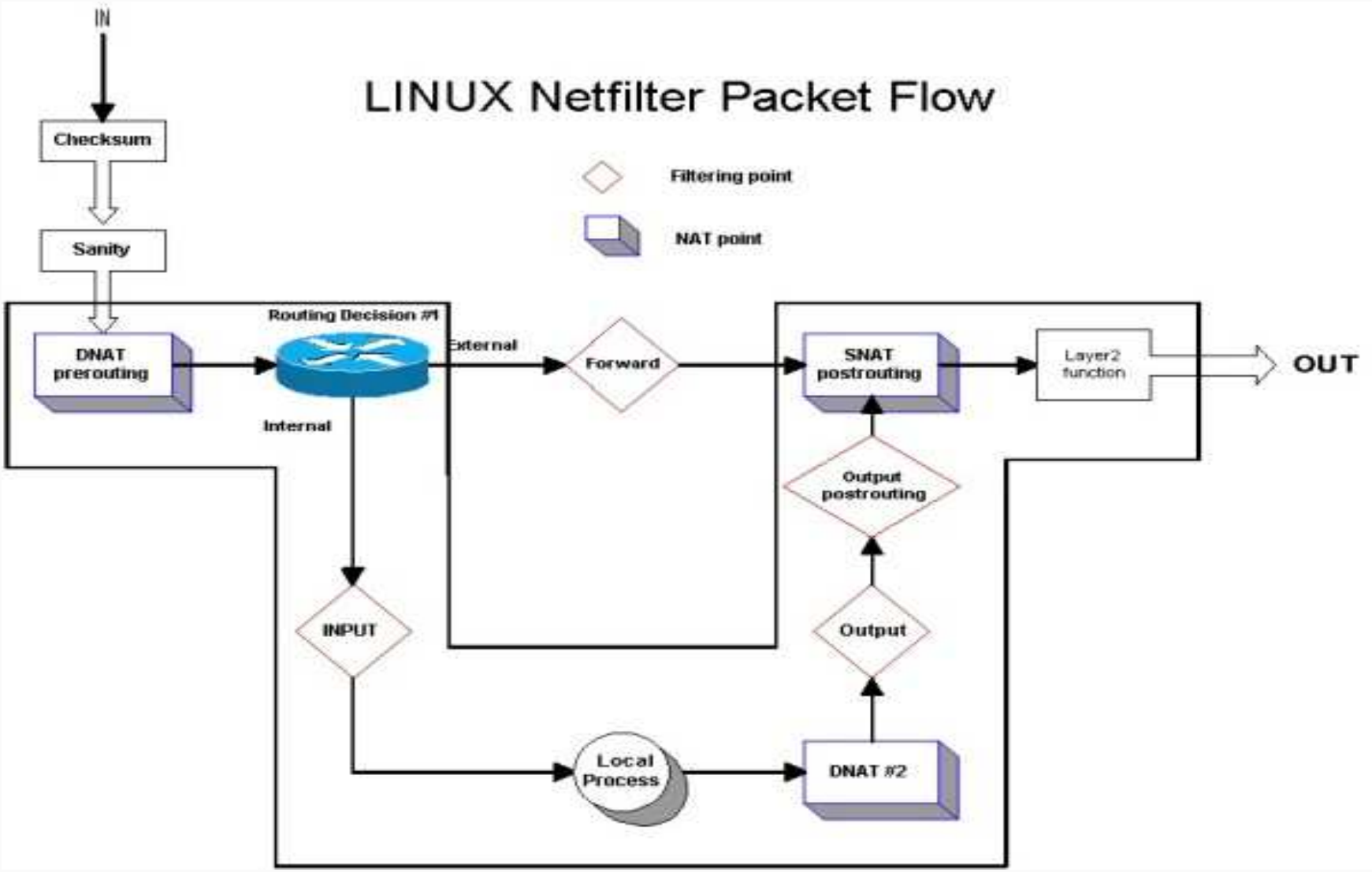
- **iptables** is a user space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall.

- Iptables requires elevated privileges to operate and must be executed by user root.

- On most Linux systems, iptables is installed as /usr/sbin/iptables.


LINUX Netfilter Packet Flow
IN
Checksum
Sanity
DNAT
prerouting
Routing Decision #1
External
Internal
Forward
SNAT
postrouting
Layer2
function
OUT
Filtering point
NAT point
Output
postrouting
INPUT
Output
Local
Process
DNAT #2


LINUX Netfilter Packet Flow
IN
Checksum
Sanity
Filtering point
NAT point
Routing Decision #1
DNAT prerouting
External
Forward
SNAT postrouting
Layer2 function
OUT
Internal
Output postrouting
INPUT
Output
Local Process
DNAT #2


LINUX Netfilter Packet Flow
IN
Checksum
Sanity
Filtering point
NAT point
Routing Decision #1
DNAT prerouting
External
Forward
SNAT postrouting
Layer2 function
OUT
Internal
Output postrouting
INPUT
Output
Local Process
DNAT #2

Iptables commands

- iptables –t filter –A INPUT –s 192.168.0.1 –j DROP

- iptables –t filter –A INPUT –s !192.168.0.1 –j DROP

- Example: Default Policy Deny everything that is not explicitly permitted

  #iptables -P INPUT DROP

  #iptables -P FORWARD DROP

  #iptables -P OUTPUT DROP

- Permit everything that is not explicitly denied.

  #iptables –P INPUT ACCEPT

  #iptables –P FORWARD ACCEPT

  #iptables –P OUTPUT ACCEPT

- Allow ssh login to firewall host from outside

```
#iptables –A INPUT    –i eth0 –p tcp -–dport ssh –j ACCEPT
#iptables –A OUTPUT –o eth0 –p tcp -–sport ssh –j ACCEPT
```

- Allow pings from all interfaces

```
#iptables –A INPUT      –p icmp –-icmp-type echo-request –j ACCEPT
#iptables –A OUTPUT –p icmp –-icmp-type echo-reply       –j ACCEPT
```

Stateful Inspection with Linux Netfilter

- Allow replies on outbound TCP packets

  #iptables -A OUTPUT –o eth0 -p tcp -m state --state NEW, ESTABLISHED, RELATED - j ACCEPT

  #iptables -A INPUT -i eth0 -p tcp -m state --state ESTABLISHED, RELATED -j ACCEPT

- Allow replies on outbound UDP packets

  #iptables -A OUTPUT –o eth0 -p udp -m state --state NEW, ESTABLISHED, RELATED –j ACCEPT

  #iptables -A INPUT -i eth0 -p udp -m state –state ESTABLISHED, RELATED -j ACCEPT

DNAT/SNAT Example

- INBOUND

  iptables –t nat –A PREROUTING –p tcp –dport 80 –j DNAT --to-dest 192.168.0.20

- OUTBOUND

  iptables –t nat –A OUTPUT –p tcp –dport 80 –j DNAT – -to-dest 192.168.0.200:3128

  MASQUERADE

  iptables –t nat –A POSTRUTING –o eth0 –j MASQUERADE

  SNAT:

  iptables –t nat -A POSTROUTING –j SNAT –to-source 1.2.3.45

References

- http://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-of-firewalls
- http://en.wikipedia.org/wiki/Application_firewall
- http://security.hsr.ch/lectures/IntSec1-Firewalls.pdf
- http://www.csh.rit.edu/~mattw/proj/nf/

Question &Answer