The following definitions from RFC 2828 (Internet Security Glossary) are relevant to our discussion:

Security Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection : A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intrusion Detection Systems (IDSs)

- **host-based IDS**
  - monitors the characteristics of a single host for suspicious activity
- **network-based IDS**
  - monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity

comprises three logical components:

- sensors - collect data
- analyzers - determine if intrusion has occurred
- user interface - view output or control system behavior

IDS Principles

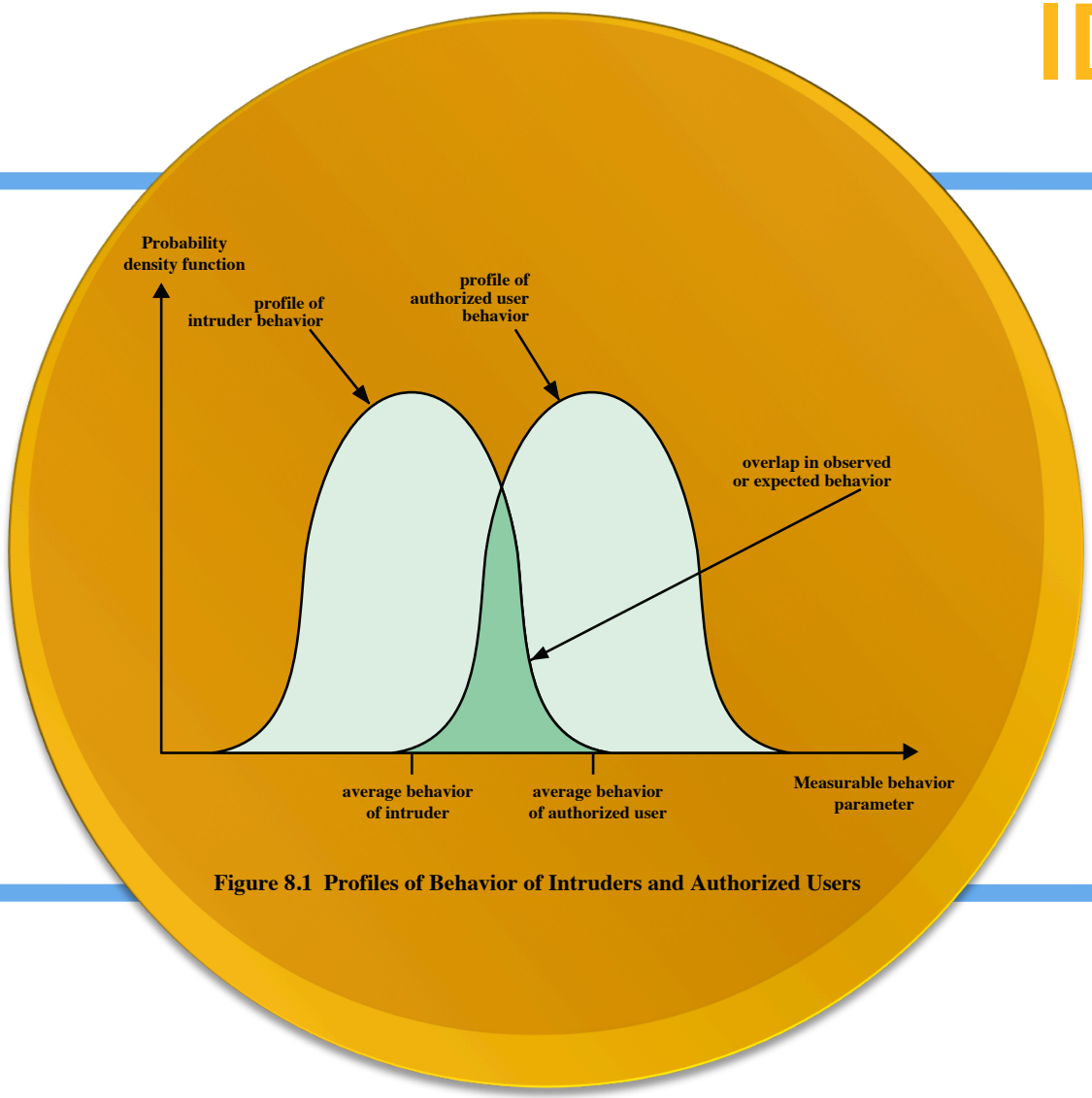


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

- assume intruder behavior differs from legitimate users
- overlap in behaviors causes problems
  - false positives
  - false negatives

Host-Based IDS

- adds a specialized layer of security software to vulnerable or sensitive systems
- monitors activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions

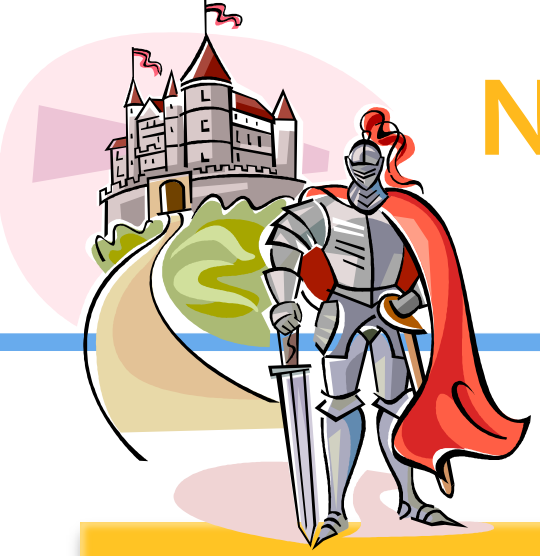
Host-Based IDS Approaches to Intrusion Detection

anomaly detection

- threshold detection
  - involves counting the number of occurrences of a specific event type over an interval of time
- profile based
  - profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts

signature detection

- involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder



Network-Based IDS (NIDS)

monitors traffic at selected points on a network

examines traffic packet by packet in real or close to real time

may examine network, transport, and/or application-level protocol activity

comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface

analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

NIDS Sensor Deployment

- inline sensor
  - inserted into a network segment so that the traffic that it is monitoring must pass through the sensor
- passive sensors
  - monitors a copy of network traffic

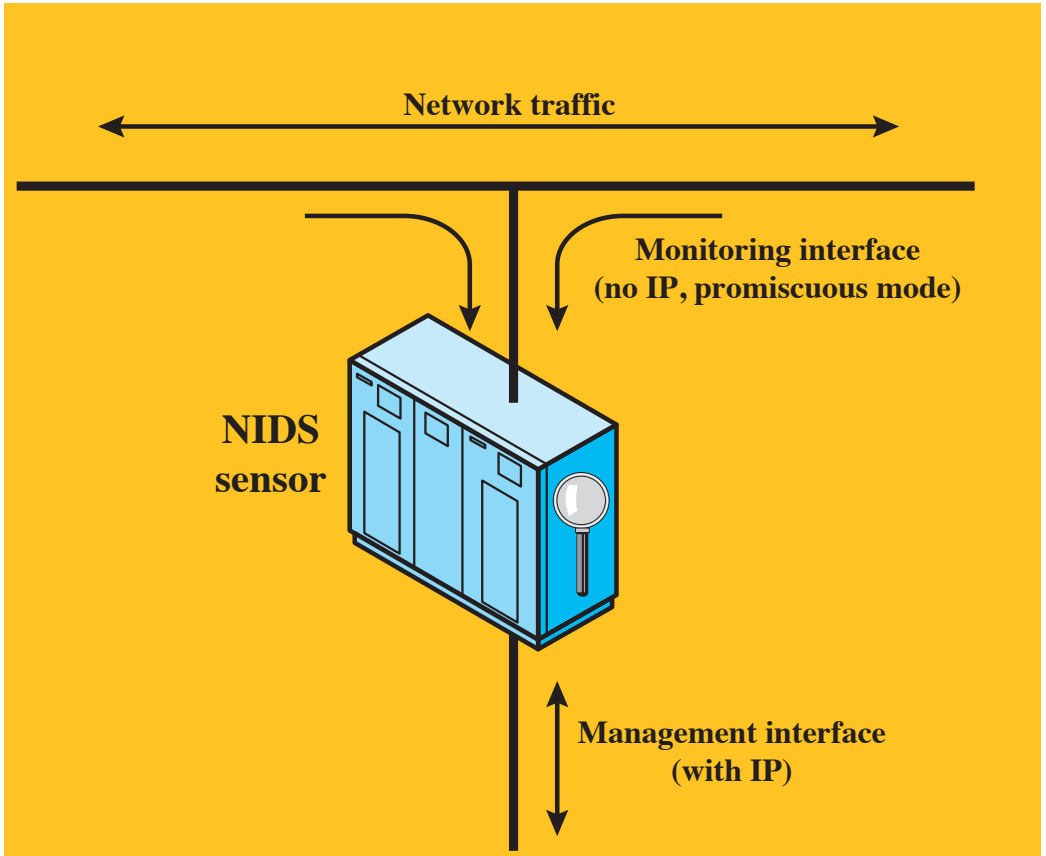


Figure 8.4 Passive NIDS Sensor (based on [CREM06])

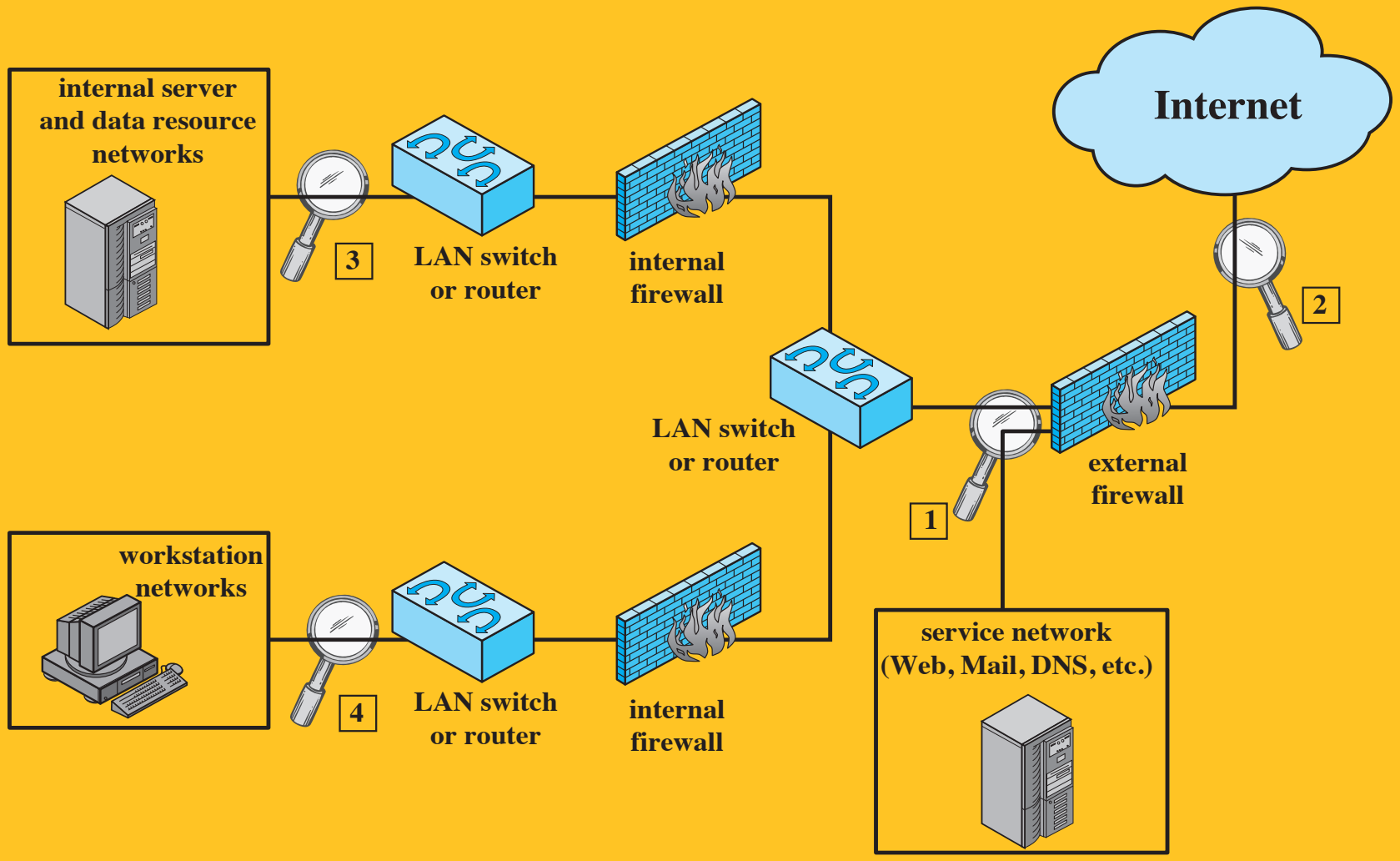


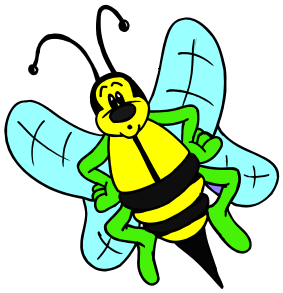
Figure 8.5 Example of NIDS Sensor Deployment

Intrusion Detection Techniques

- signature detection
  - at application, transport, network layers; unexpected application services, policy violations
- anomaly detection
  - denial of service attacks, scanning, worms
- when a sensor detects a potential violation it sends an alert and logs information related to the event
  - used by analysis module to refine intrusion detection parameters and algorithms
  - security administration can use this information to design prevention techniques

Honeypot

- decoy systems designed to:
  - lure a potential attacker away from critical systems
  - collect information about the attacker's activity
  - encourage the attacker to stay on the system long enough for administrators to respond
- filled with fabricated information that a legitimate user of the system wouldn't access
- resource that has no production value
  - incoming communication is most likely a probe, scan, or attack
  - outbound communication suggests that the system has probably been compromised
- once hackers are within the network, administrators can observe their behavior to figure out defenses



Honeypot Deployment

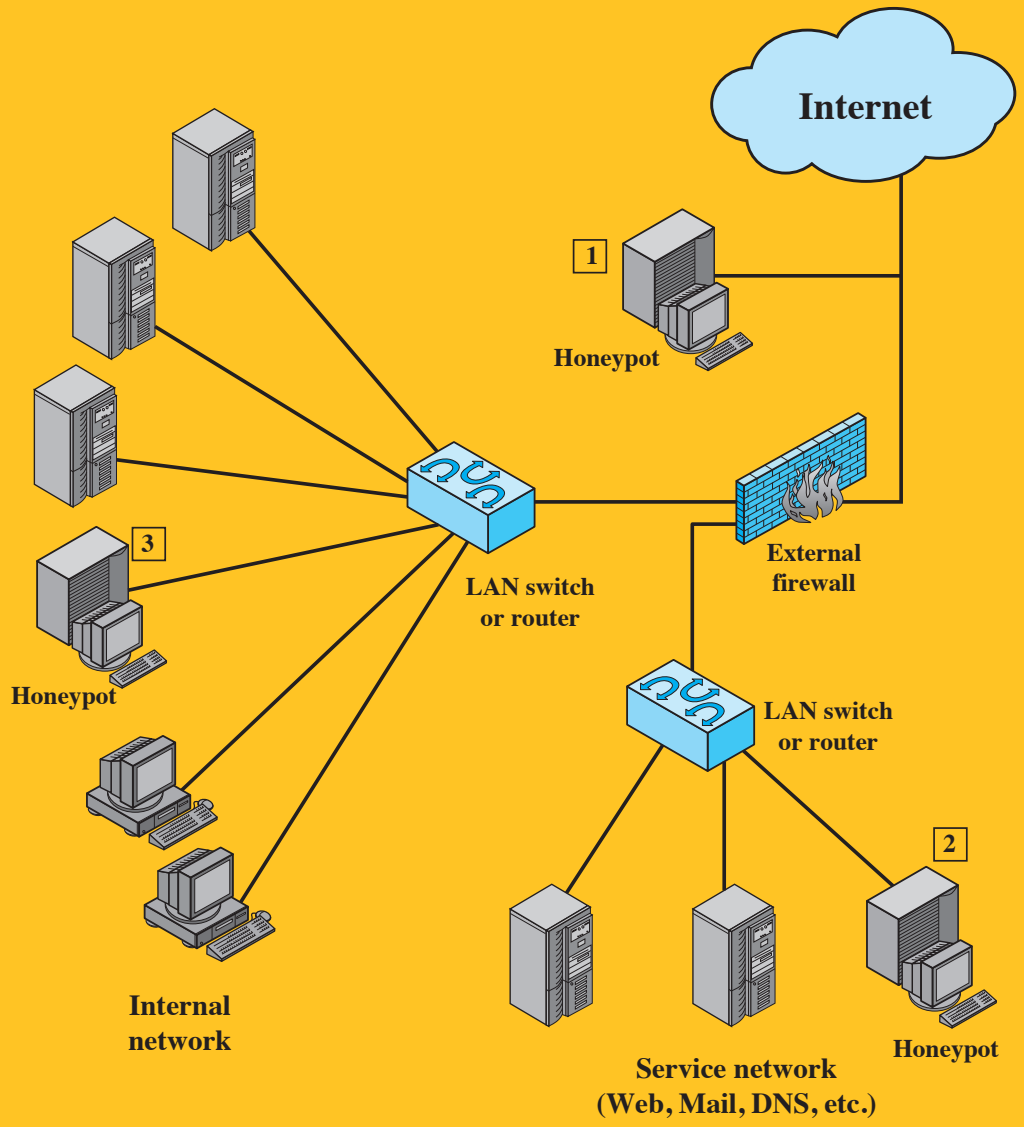


Figure 8.8 Example of Honeypot Deployment

SNORT

- lightweight IDS
  - real-time packet capture and rule analysis
  - easily deployed on nodes
  - uses small amount of memory and processor time
  - easily configured

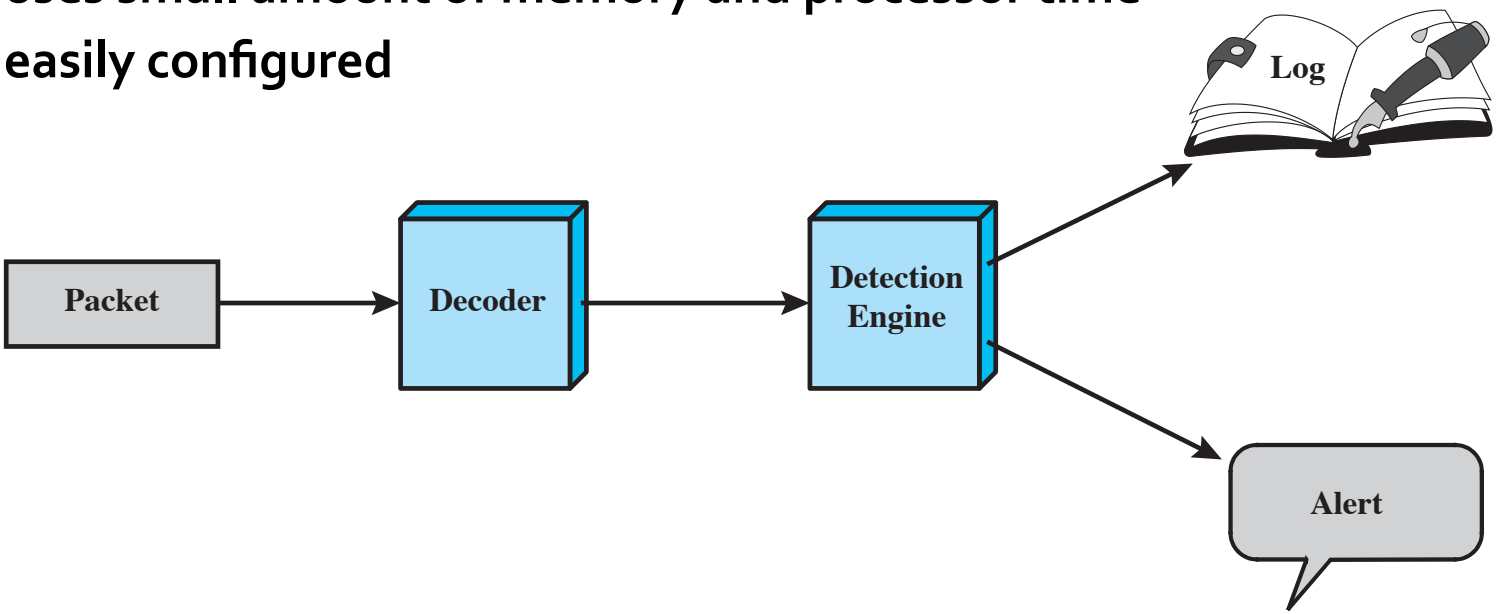


Figure 8.9 Snort Architecture

SNORT Rules

- **use a simple, flexible rule definition language**
- **each rule consists of a fixed header and zero or more options**

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
activate	Alert and then turn on another dynamic rule.
dynamic	Remain idle until activated by an activate rule , then act as a log rule.
drop	Make iptables drop the packet and log the packet.
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Make iptables drop the packet but does not log it.

Examples of SNORT Rule Options

meta-data

msg Defines the message to be sent when a packet generates an event.

reference Defines a link to an external attack identification system, which provides additional information.

classtype Indicates what type of attack the packet attempted.

payload

content Enables Snort to perform a case-sensitive search for specific content (text and/or binary) in the packet payload.

depth Specifies how far into a packet Snort should search for the specified pattern. Depth modifies the previous content keyword in the rule.

offset Specifies where to start searching for a pattern within a packet. Offset modifies the previous content keyword in the rule**.**

nocase Snort should look for the specific pattern, ignoring case. Nocase modifies the previous content keyword in the rule.

non-payload

ttl Check the IP time-to-live value. This option was intended for use in the detection of traceroute attempts.

id Check the IP ID field for a specific value. Some tools (exploits, scanners and other odd programs) set this field specifically for various purposes, for example, the value 31337 is very popular with some hackers.

dsize Test the packet payload size. This may be used to check for abnormally sized packets. In many cases, it is useful for detecting buffer overflows.

flags Test the TCP flags for specified settings.

seq Look for a specific TCP header sequence number.

icmp-id Check for a specific ICMP ID value. This is useful because some covert channel programs use static ICMP fields when they communicate. This option was developed to detect the stacheldraht DDoS agent.

post-detection

logto Log packets matching the rule to the specified filename.

session Extract user data from TCP Sessions. There are many cases where seeing what users are typing in telnet, rlogin, ftp, or even web sessions is very useful.