Process Specification

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Thang Duong Chi | Add this document | 1.0 | 28/11/2010 |

# Number:

1

# Name:

Process Packet

# Description:

Captured packets will be checked with rules. Packets that don’t conform to the rules will be dropped. The rest will be checked with alert rules to make alerts. Server data will be used to make alerts from HIDS rules. These alerts will be normalized.

# Input Data Flow:

Rules

Server Data

Packet

Alert Rules

# Output Data Flow:

Processed Packet

Packet to drop

Normalized Alert

# Type of Process:

Online Batch Manual

# Subprogram/Function Name:

# Process Logic:

IF packet\_against\_rule THEN drop\_packets ELSE make\_processed\_packet

IF process\_packet\_against\_alert\_rule AND server\_data\_against\_HDIS\_rule

THEN emit\_alert; normalize\_alert

# Unresolved Issues: