Data Flow Description

# Revision:

|  |  |  |  |
| --- | --- | --- | --- |
| Author | Description | Version | Date |
| Thang Duong Chi | Add this document | 1.0 | 4/12/2010 |

# ID

# Name

**Alert Rules**

# Description

Contains alert rules for NIDS and HIDS to make alerts

# Source

D3

# Destination

Process 1

# Type of Data Flow

File Screen Report Form Internal

# Data Structure Traveling with the Flow

Alert Rule = [NIDS\_Rule HIDS\_Rule]

NIDS\_Rule = Action + Protocol + SrcIPList + SrcPortList + Direction + DestIPList + DestPortList + (Rule\_options)

SrcIPList= {Src\_IP}

SrcPortList={Src\_port}

DestIPList={Dst\_IP}

DestPortList={Dst\_port}

HIDS\_Rule =

# Volume/Time

1/day

# Comments

# Unresolved Issue

The volume/time may not be correct

HIDS\_Rule data structure