Intrusion & Anomaly Detection

Intrusion Detection Systems

Lisa Frye, Instructor
frye@kutztown.edu
Kutztown University

Intrusion Detection

- Intrusion
- Intrusion Detection
- Intrusion Detection System (IDS)

Intrusion Detection System

- Monitor network traffic
- Defense in Depth

- True positives
- True negatives
- False positives
- False negatives

IDS Components

- Network sensors
- Alert systems
- Command console
- Response system
- Database

IDS Categorizations

- Active vs. Passive
- Signature-based / Misuse Detection / Rule-based
  - Anomaly detection
  - Penetration identification
- Anomaly-based / Anomaly Detection
  - Threshold detection
  - Profile based

Table 7-1 Advantages and disadvantages of IDS triggering mechanisms

Trigger	Advantages	Disadvantages
Anomaly detection	Because an anomaly detection system is based on profiles that the administrator creates, an attacker cannot test the IDS beforehand and cannot anticipate what will trigger an alarm.	A substantial amount of time is required to configure the IDS to use profiles of network users and groups.
	As new users and groups are created, IDS profiles can be changed to keep up with the new arrangements.	As new users and groups are created, profiles available to the IDS must be updated to remain effective.
	Because an anomaly detection system does not rely on published signatures, it can detect new attacks.	The definition of what constitutes "normal" traffic changes constantly; the IDS must be reconfigured continually to keep up.
	The system can effectively detect attacks from inside the network by employees or attackers who have stolen employee accounts.	After installation, the IDS must be "trained" for days or weeks at a time to recognize normal traffic.
Misuse detection	This approach makes use of signatures of well-known attacks.	The database of signatures must be updated to maintain the effectiveness of the IDS.
	The IDS can begin working immediately after installation.	New types of attacks might not be included in the database.
	The IDS is easy to understand and is less difficult to configure than an anomaly-based system.	By making minor alterations to the attack, attackers can avoid matching one of the signatures in the database.
	Each signature in the database is assigned a number and name so that the administrator can identify the attacks that need to set off an alarm.	Because a misuse-based system makes use of a database, a considerable amount of disk storage space might be needed.

Other Types of Detection

- Traffic rate monitoring
- Protocol state tracking
- IP packet reassembly

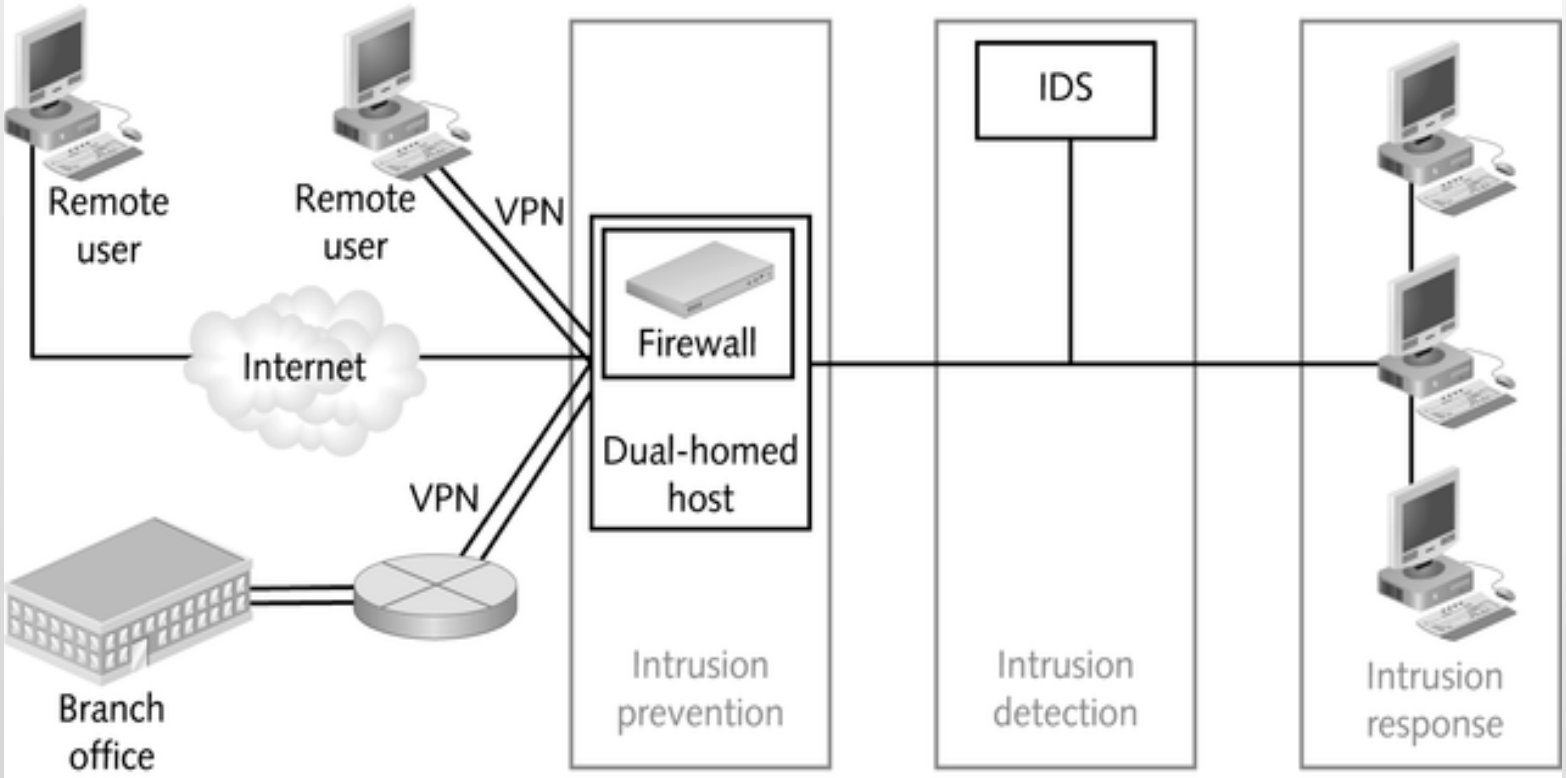

Figure 8-1 The role of intrusion detection in an overall network defense configuration

Network-Based IDS Placement

- Just inside Firewall
- DMZ
- Server farm segment
- Segment with mainframe

- Why are each of these good locations?

Connect NIDS to Network

- Switch Port Analyzer (SPAN)
- Hubs with switches
- Taps with switches

SPAN

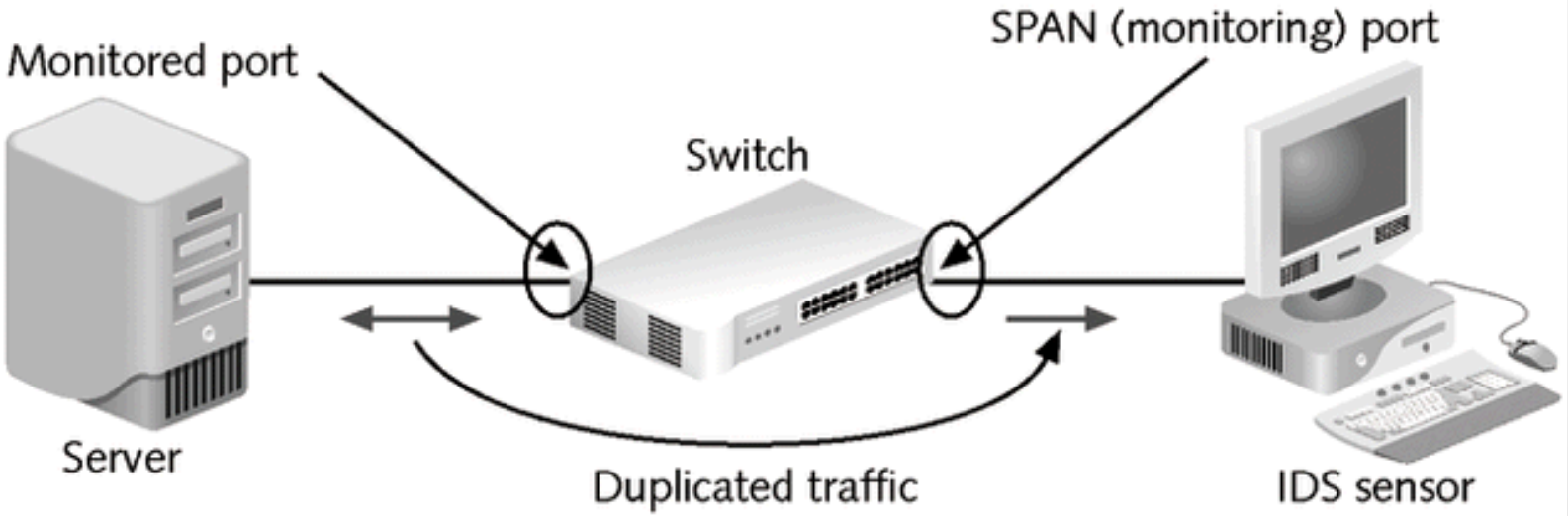

Figure 12-2 Basic SPAN port operation

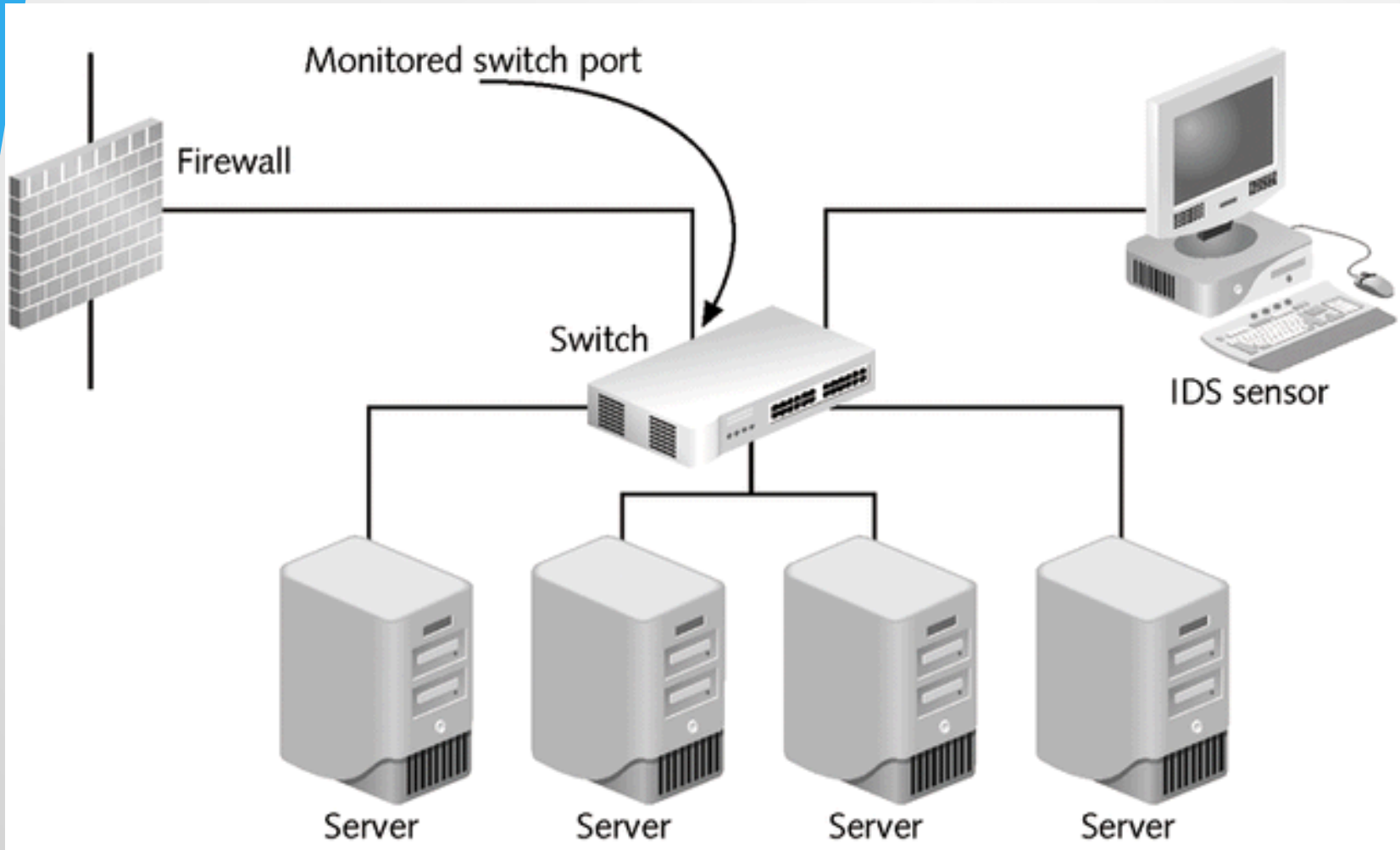

Figure 12-3 Using a SPAN to monitor an entire segment

IDS using a Hub

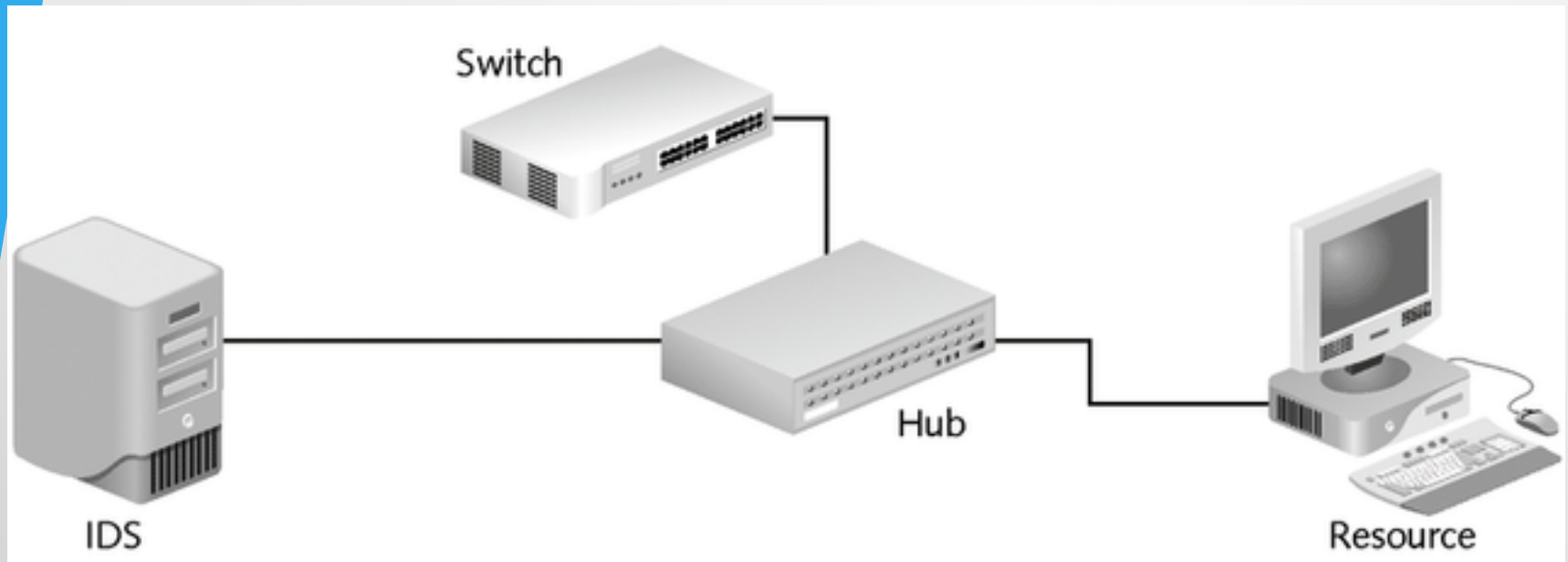

Figure 12-4 Using a hub in a switched infrastructure

Types of NIDS

- Signature databases
- Port signature
- Header signature

NIDS Responses

- TCP resets
- IP session logging
- Shunning / blocking

Host-based IDS

- Audit log files
- Monitor file checksums
- Elementary NW-based signature techniques
- Intercept and evaluate requests for resources
- Monitor system processes

Hybrid IDS

- Combine NIDS and HIDS
- Combine sensor locations
- Combine detection methods

- Distributed IDS (DIDS)

Distributed IDS: Challenges

- Audit record formats
- Transmission of data among IDS nodes
- Centralized architecture
- Distributed architecture

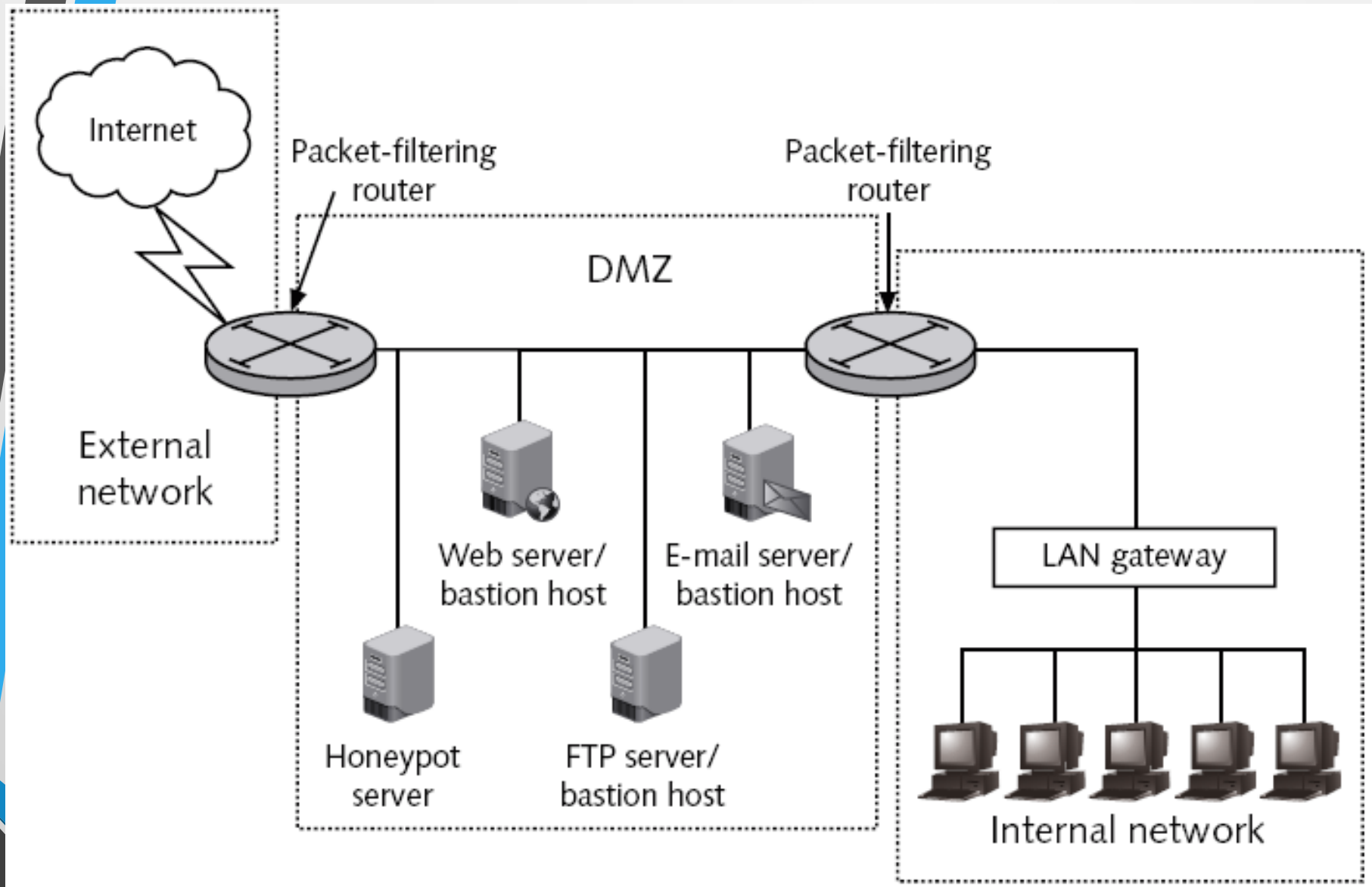

Figure 10-3 A honeypot in the DMZ

Incident Response

- IDS Monitoring Policy and Procedure
  - IDS Tuning
  - Monitor logs and alerts
- Incident Response Plan
  - Record necessary information
  - Report incident
  - Prosecution
  - Recover

Intrusion Prevention System

- Real-time
- BlackICE, 1998
- Snort