

Information Security - Introduction to Intrusion Detection & Prevention

morgan alexander
Northrop-Grumman
xz13@cdc.gov

Intrusion Detection System (IDS)

(What It Is - Part 1)

Intrusion Detection Systems provide warnings when certain types of events or anomalies are recognized



Intrusion Prevention Systems (IPS)

(What It Is – Part 2)

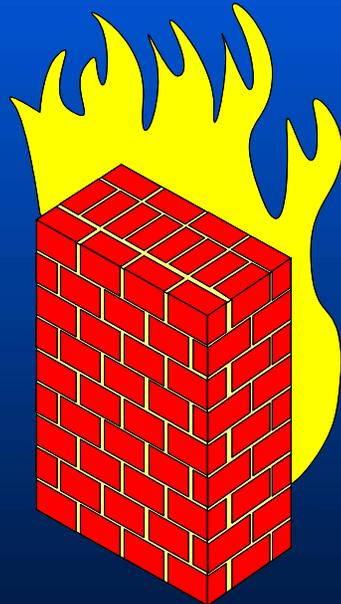
Intrusion Prevention Systems take steps to prevent actions when certain types of events or anomalies are recognized



Firewalls and IDS

(What It Isn't)

- Sit in the traffic flow
- Allow or deny traffic based on rules
- Focus on protocol, source / destination, etc.



- May or may not sit in the traffic flow
- May or may not interfere with traffic
- Focus is on the packet and/or the behavior



Anomaly vs. Signature

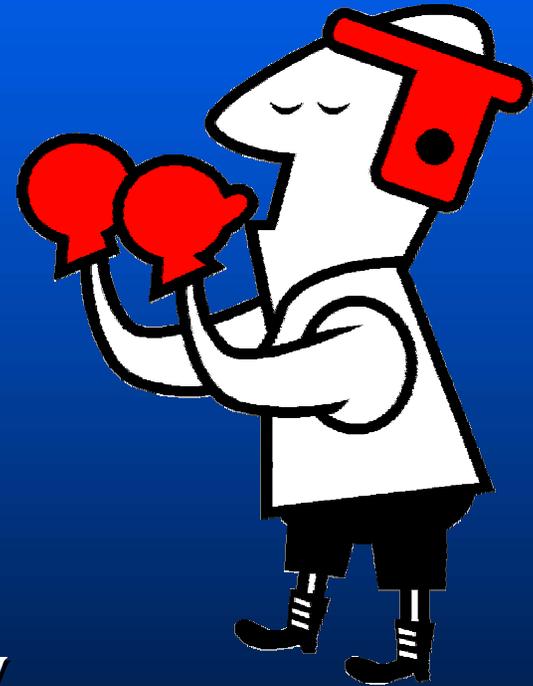
(How It Works)

- Signature-based systems:

$\langle sig \rangle = ".ida?"$

- Anomaly-based systems:

- Host-Based Actions
- Unusual Network Activity
- Non-Spec Packets (Protocol Analysis)



IDS Responses

(What It Does)

- **Quiet:** Logs and Console Alerts
- **Loud:** Pager, Email, Interactive
- **Active:** Session Sniping, Blocking

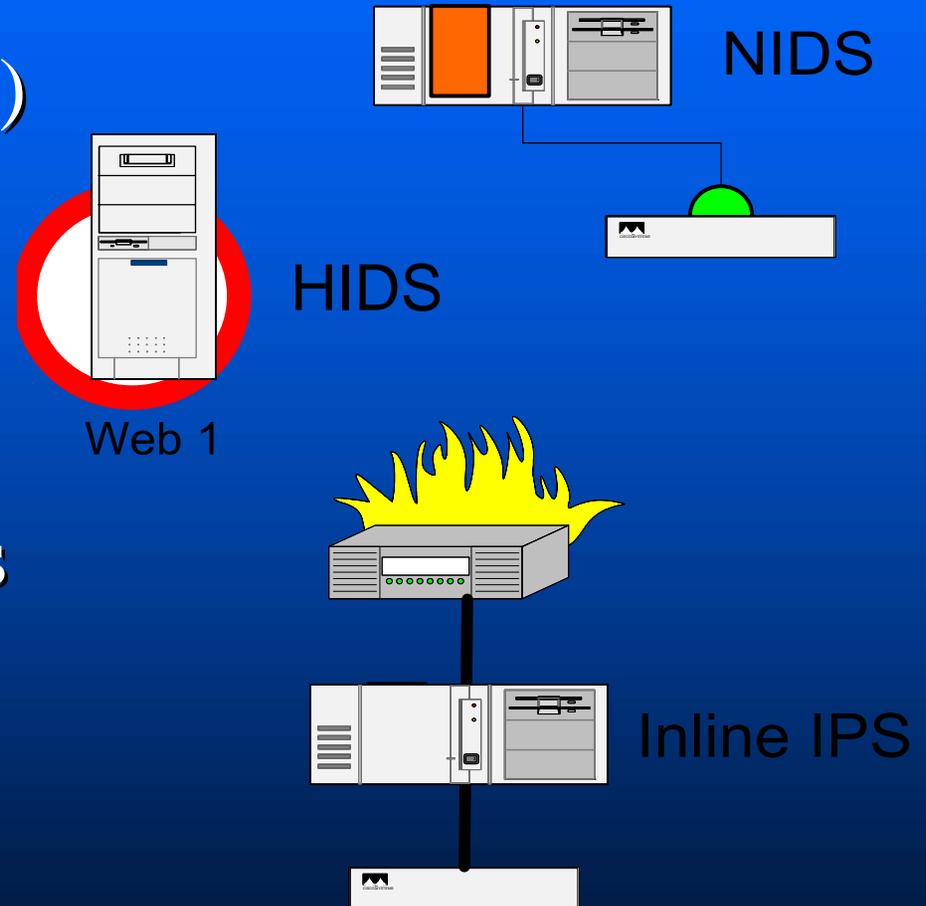


Take great care
when choosing
Active Response!

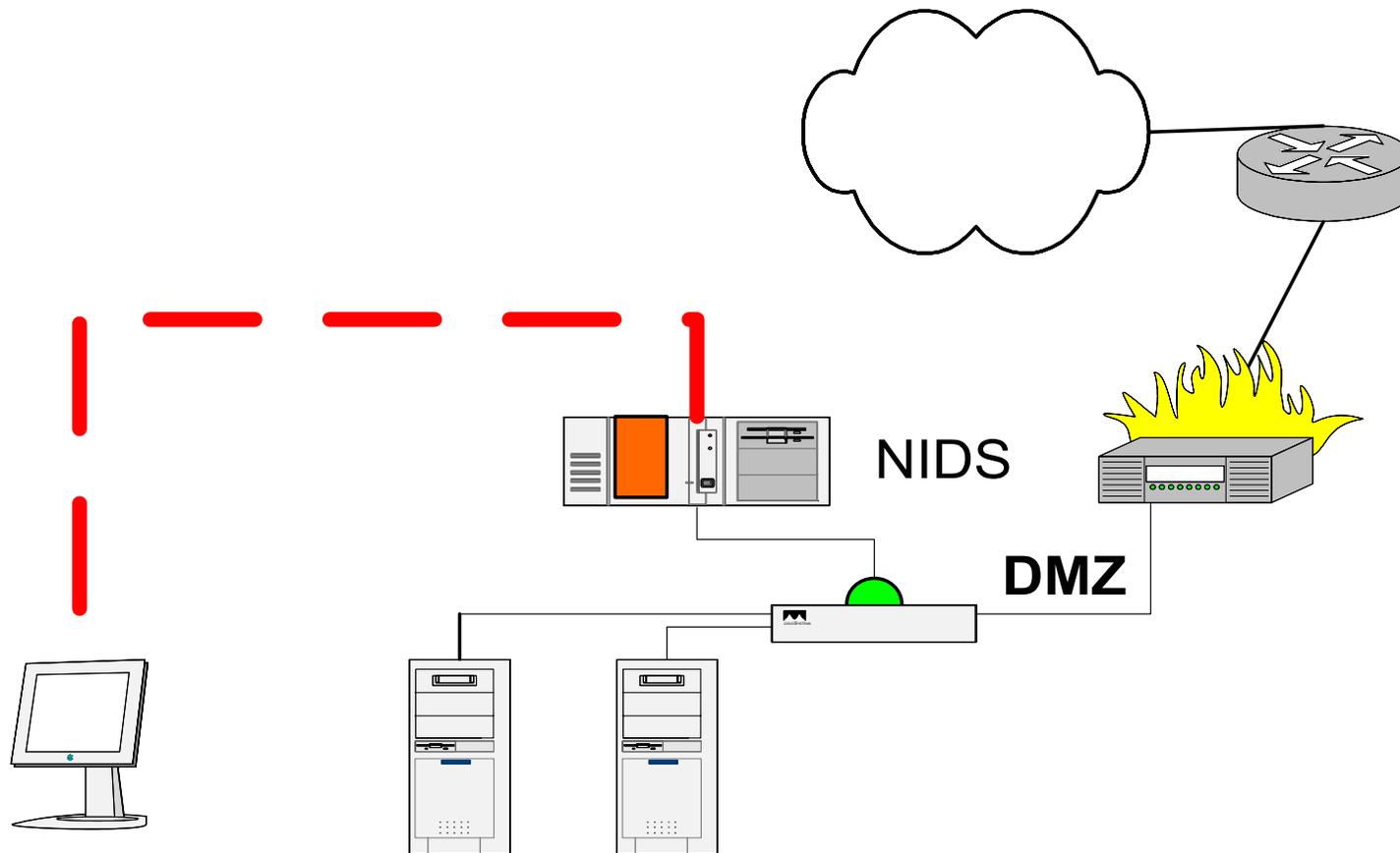
Some IDS Deployment Options

- Network IDS (NIDS)
- Host-Based (HIDS)
- In-Line IPS

-
- Other IPS Variations
 - Other relations:
 - Honey Pots
 - Network Recorders



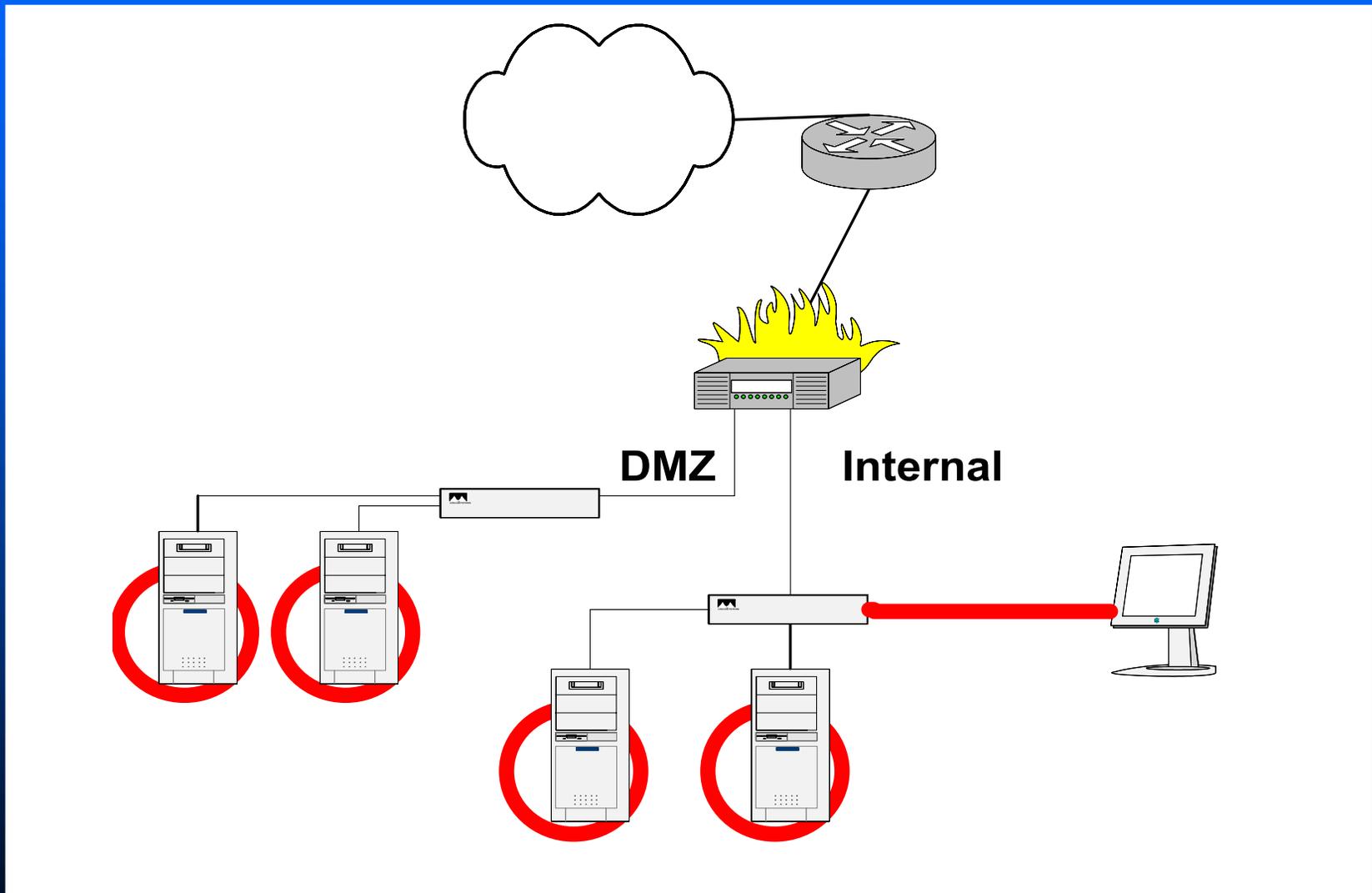
Example Network IDS



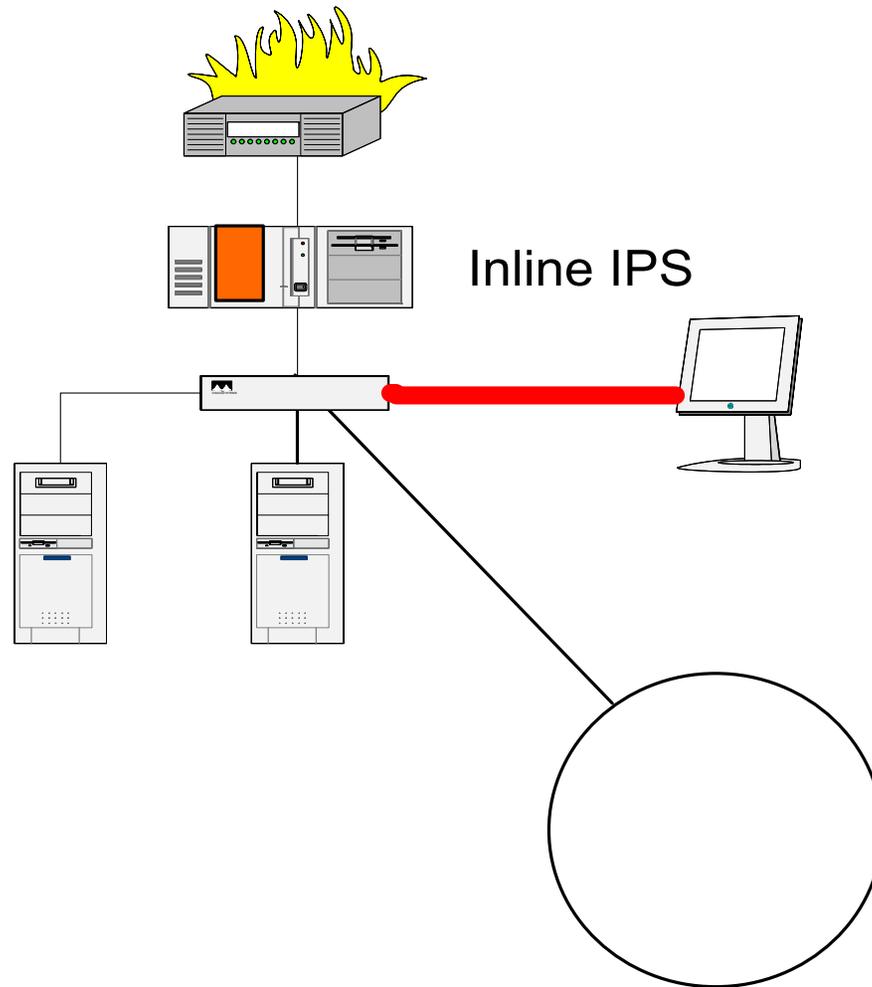
Some Things to Know About NIDS

- NIDS and Switched Environments
 - Mirror / Span Ports
 - Network Taps
- NIDS see only 1 network at a time
- NIDS and Encryption
- NIDS can see an attack attempt but not the end result

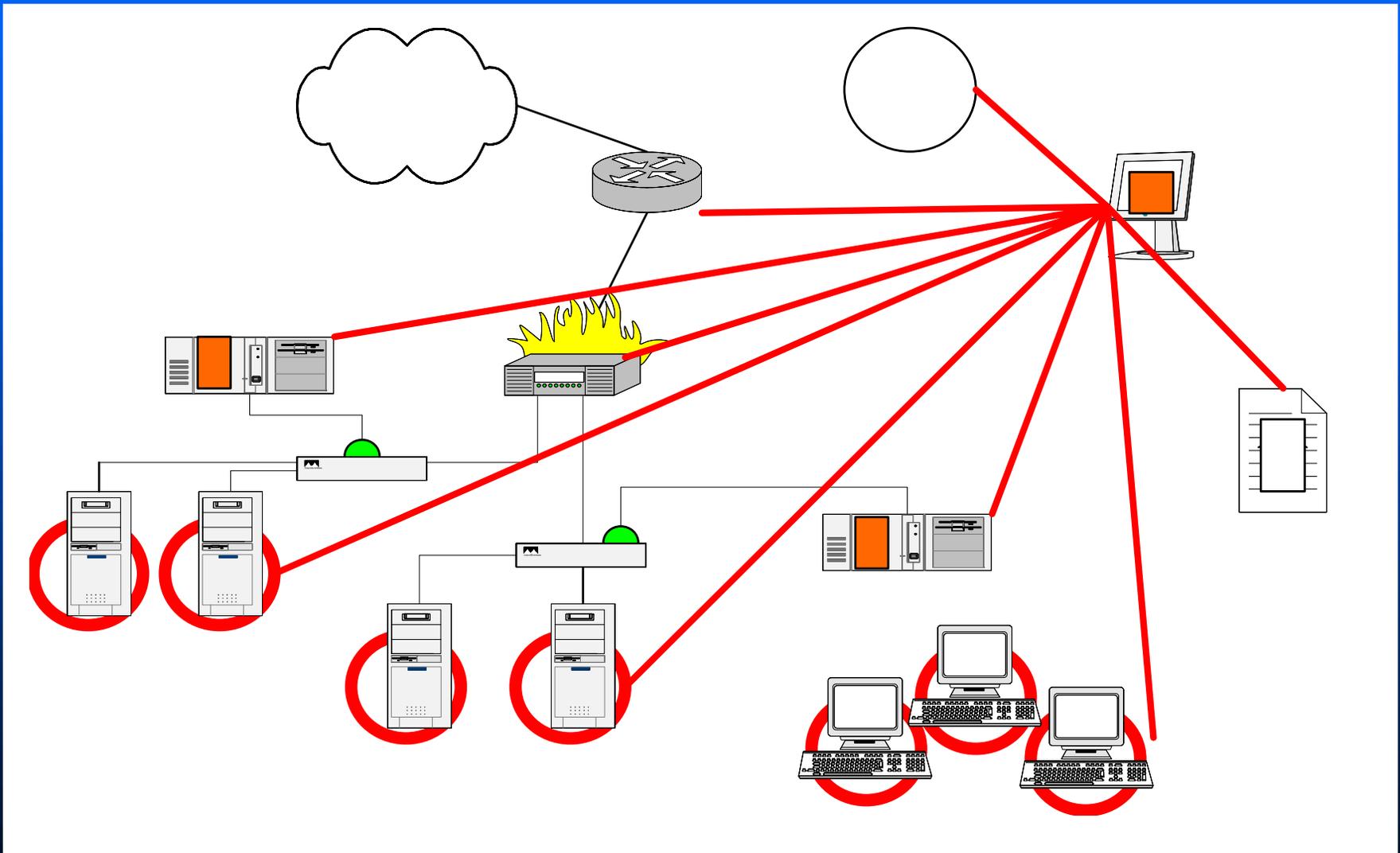
Example Host-Based IDS



Example IPS (In-Line)



Looking Toward the Future



Benefits of Implementing IDS / IPS

- Early warning of potential attacks (probes and reconnaissance)
- Alerts during an active attack (internal or external)
- Active response may reduce damage or prevent an attack from succeeding
- Assist to identify underlying network issues
- Useful during evidence gathering
- Compliment to any layered defense strategy

Hidden Costs of IDS / IPS

- Network Documentation
- Manpower to:
 - Learn and configure the system
 - Tune the system
 - Update the system
 - Monitor the system
 - Respond to alerts and investigate activities



Managed Solutions

A popular alternative or enhancement to in-house intrusion detection is a Managed Intrusion Detection System (MIDS)



Incident Response

Develop a plan for event investigation and incident response – Before you have to investigate the first event!



Deployment Tips

- Develop specific requirements
- Evaluate the best approach for your organization – **don't forget open source**
- Get senior management buy-in
- Ensure you have adequate policy in place
- Deploy slowly
- Allow time to tune before moving on
- Update frequently
- Note that IDS solutions are not infallible
- **KNOW YOUR NETWORK**

IDS Resources

- Topical reading online at:
www.securityfocus.com/infocus/ids
- Product-neutral intrusion detection and incident response training from SANS –
www.sans.org
- Network Intrusion Detection (3rd Edition)
by Stephen Northcutt and Judy Novak
www.amazon.com

Questions?