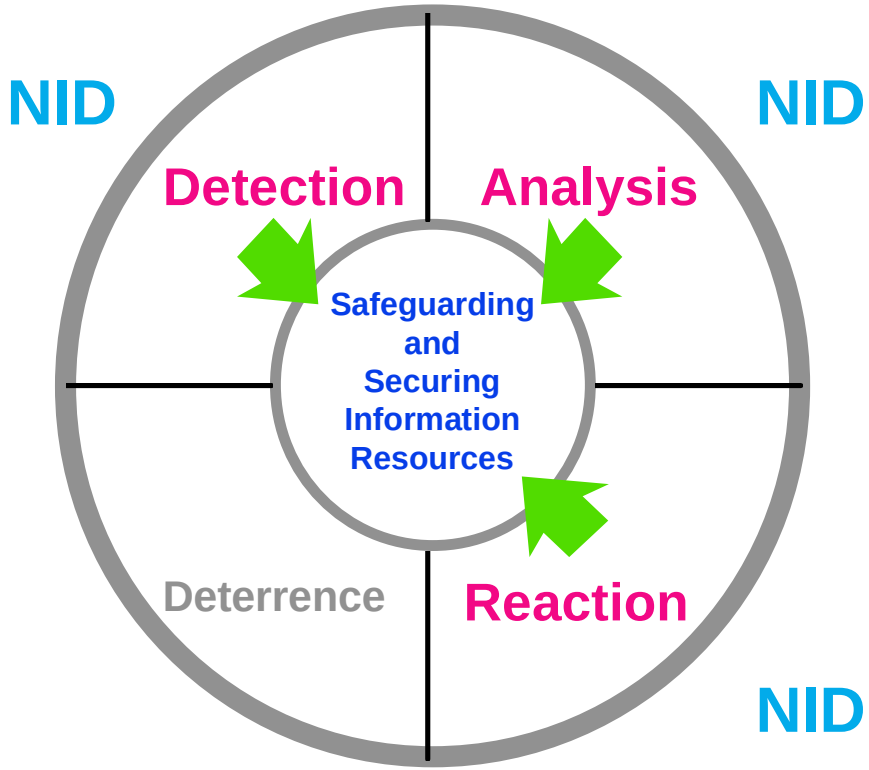
Computer Security Technology Center

Lawrence Livermore National Laboratory



Network Intrusion Detector

John Donetti
Scott Elko

http://ciac.llnl.gov/cstc

UCRL-MI-116536

This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48.

Network Intrusion Detector Origins

Problem: Computers connected to networks are subject to unauthorized or malicious use. There is a need to detect, analyze and respond to such abuse.

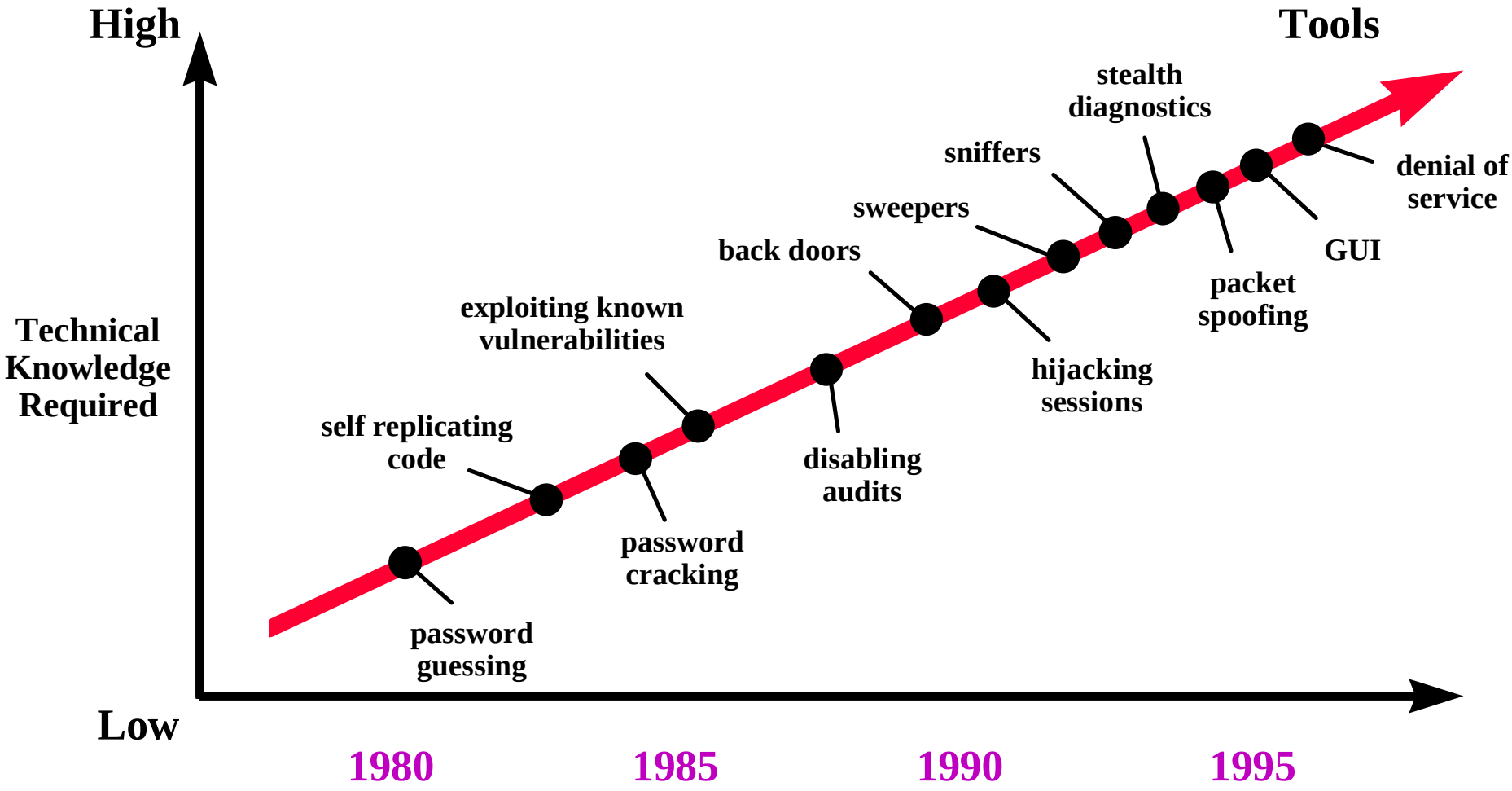
Feature: Multiple access network technology (such as Ethernet and FDDI) allows monitoring without any changes to existing hosts or routers.

Goals: Identify unauthorized individuals.
Identify unauthorized activities.
Analyze suspicious activities.

Network Intrusion Detector Statistics

- Internet opens doors to hackers
- Problem
  - Some system administrators connect new machines to internet during setup BEFORE a root password has been established.

Network Intrusion Detector Intruder Techniques Gain Sophistication



Network Intrusion Detector
Recent Trends And Observations

- **Many known vulnerabilities still being exploited even though patches available**
- **Password cracking <u>still</u> produces results**
- **UNIX is still the OS of choice to exploit**
- **One new vulnerability discovered per week**
  - ***Scriptors of Doom*** **targeting HP regularly**
- **PC viruses abound - *macro* virus spreading**
  - ***http://ciac.llnl.gov/ciac/CIACVirusDatabase.html***

Network Intrusion Detector
Recent Trends And Observations

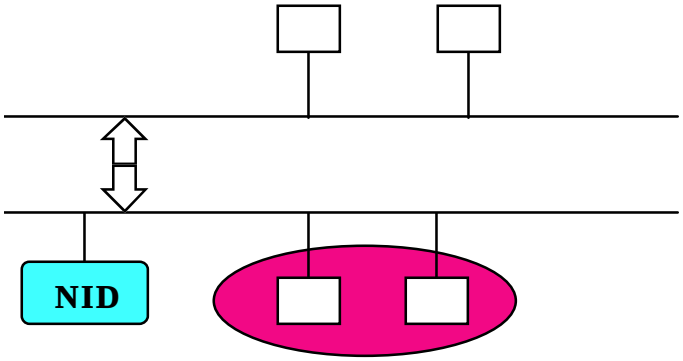
- **Trojan programs actively used - *rootkit***
- **Sniffers actively used and effective**
  - **Sniffers are readily available on the web for most OSs**
  - **Sniffer detectors are available for several OSs**
  - ***ftp://ciac.llnl.gov/pub/ciac/sectools/unix/sniffdetect***

Network Intrusion Detector Recent Trends And Observations

- **Web Home Pages being altered**
  - **DOJ, CIA, USAF**
  - **Mirror Site - *http://www.skeeve.net/cia***
- ***"Internet is now the fastest growing means for foreign governments and firms to gather information about U.S. businesses."***
  - **Source: National Counterintelligence Center**

Network Intrusion Detector Functional Overview

- A collection of tools that help detect, analyze, and gather evidence of intrusions.
- Operates on a dedicated host attached to the security domain you wish to protect.



Network Intrusion Detector Unique Capabilities

- **NID is passive—an intruder does not know NID is active.**
- **NID can recreate connections between computers.**
- **NID can perform threat analysis during or after data collection.**
- **NID requires no modifications to the hosts it protects.**
- **NID can begin data collection upon detection of intrusive behavior.**

Network Intrusion Detector User Community

- NID has been used to detect, identify or track network intrusions at a number of installations.

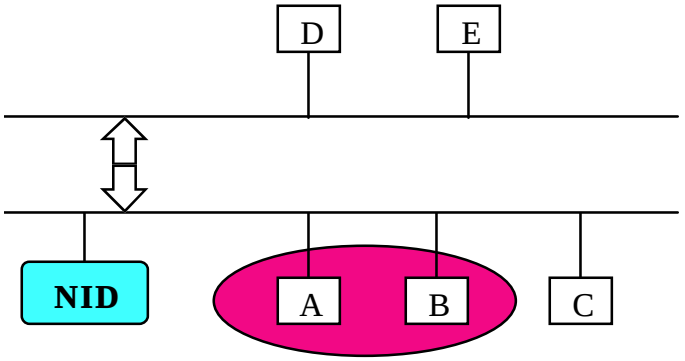
ANL	BNL	DISA
INEL	LANL	LLNL
ORNL	SNL	Navy
FBI	Army	Pantex

Network Intrusion Detector Security Domain

- A security boundary sets the delineation between inside and outside for hosts and networks
- A security domain is the region defined in relation to the security boundary
  - Crosses
  - Completely inside or completely outside
  - Destination inside, source outside

Network Intrusion Detector
Sample Security Domain

- **In this example, a security boundary is drawn around the A and B computers and NID is set to monitor crossing packets**
  - **Packets initiated by or sent to C, D, or E are checked**
  - **Packets between A and B are ignored**

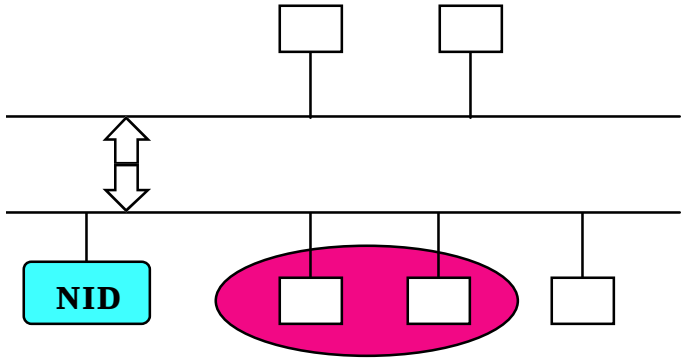


Network Intrusion Detector Operating Modes

Mode	Description
❖ Retrospective Analysis	Capture all packets
❖ Real-time Detection	Capture, analyze & notify
❖ Evidence Gathering	Minimize sessions captured
❖ Statistics Gathering	Analyze IP traffic headers

Network Intrusion Detector Retrospective Analysis

- **Goals**
  - Detect past intrusions
  - Discover new intrusion methods
- **Steps**
  - Collect packets
  - Analyze packets
  - View packets



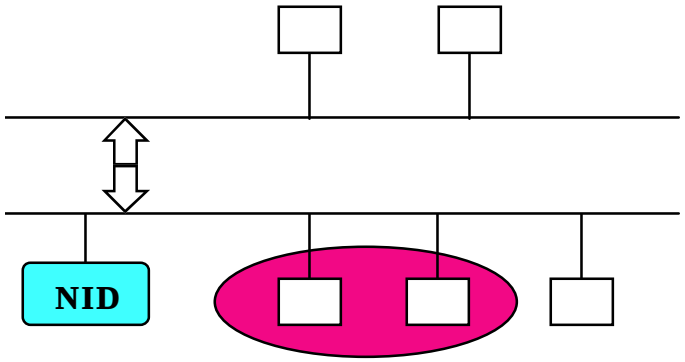
Security Domain	Crosses
Service Used	Selected

Network Intrusion Detector Retrospective Analysis

- **Data collection**
  - **Raw unsegregated packets**
- **Data analysis**
  - **Threat scoring**
- **Stream re–creation**
  - **Extractions from raw data**
- **Stream display**
  - **Replay of original interactions**

Network Intrusion Detector
Real-time Detection

- **Goals**
  - Detect intrusions in progress
  - Provide alarms
- **Steps**
  - Collect packets
  - Analyze packets
  - Issue alarms



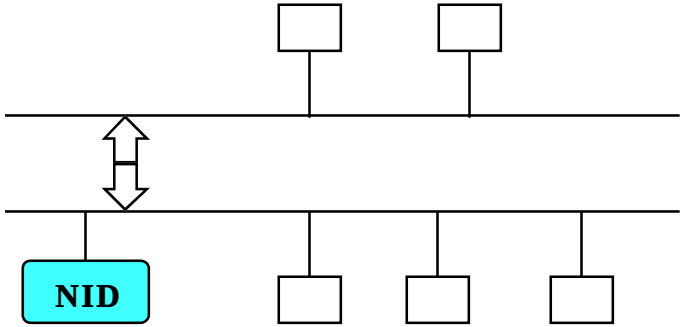
Security Domain	Crosses or Inside
Service Used	Selected or All

Network Intrusion Detector
Real-time Detection

- **Capture each packet**
- *If the packet crosses the security domain and is one of the desired services*
- **Write packet to disk**
- **Look for signatures**
- *If a signature is found*
- **Evaluate the threat**
- *If the threat is above our threshold*
- **Signal a threat has been detected**

Network Intrusion Detector Evidence Gathering

- **Goals**
  - Confirm suspicion of intrusion
  - Obtain proof of intrusion
- **Steps**
  - Watch for patterns
  - Collect packets
  - View packets



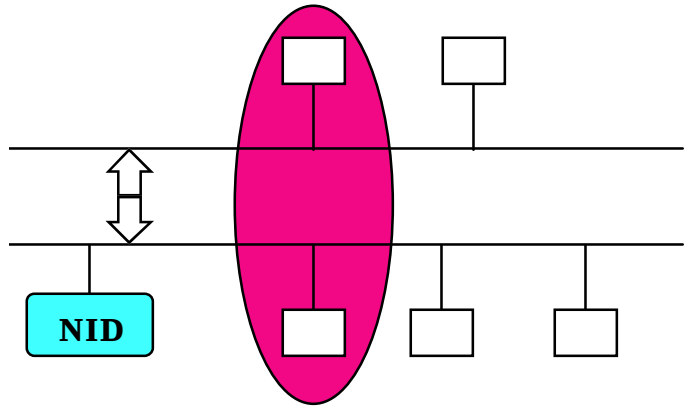
Security Domain	—
Service Used	Selected

Network Intrusion Detector Evidence Gathering

- **Obtaining *grounds* for data stream capture**
  - **Pattern recognition**
  - **View context**
  - **Obtain permission**
- **Obtaining evidence *(proof)***
  - **Pattern recognition & capture**
- **Presenting evidence**
  - **Packet script**

Network Intrusion Detector Statistics Gathering

- **Goals**
  - Understand network traffic
  - Discover unusual activities
- **Steps**
  - Collect packet statistics or headers



Security Domain	Source in Dest out
Service Used	Selected or All

May also collect statistics with no security domain

Network Intrusion Detector Statistics Gathering

- **Traffic statistics**
  - Collected by all data capture programs
  - Blocked-time traffic analysis
  - Evidence gathering to obtain permission for “wire-taps”
- **Server statistics**
  - Correlated by service
  - Day-night traffic analysis
- **Network headers**
  - Continuous-time traffic analysis

Network Intrusion Detector Monitoring Capabilities

	Retrospective Analysis	Real-time Detection			Evidence Gathering		Statistics Gathering	
	Retro	**Threat**	**Domain**	**Suspect**	**Grounds**	**Proof**	**Server**	**Header**
Security Domain	Crosses	Crosses	Inside	Outside	None / Crosses	None / Crosses	Dest In Src Out	None / Crosses
Service Used	Selected	Selected	All	All	Selected	Selected	Selected or All	All
Data Served	Packets	Packets / None	Packets / None	Statistics	Context	Packets Context	Statistics	Headers
Live Actions	—	Alarm Context	Alarm	Alarm	Alarm	Alarm	—	—

Network Intrusion Detector Privacy

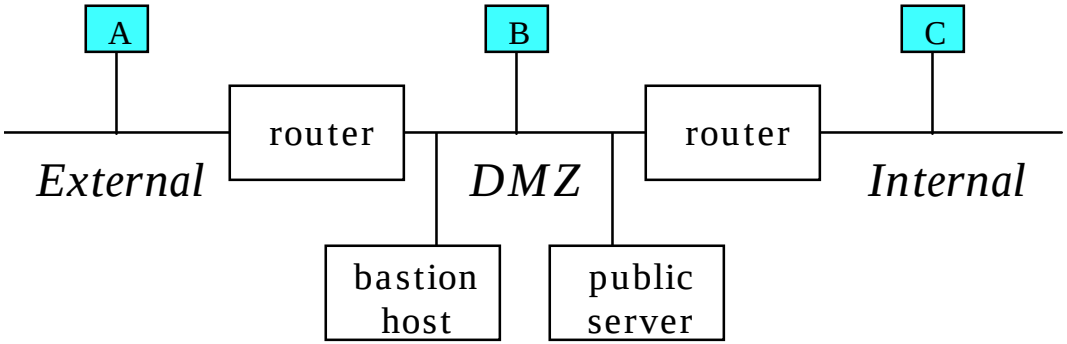
- **Information Protection vs. Privacy**
  - **Organizations have a right to protect investments**
  - **Individuals have a right to privacy**
- **Best balance: Evidence Gathering model**
  - **Search for specific patterns**
  - **Get permission to collect data**
  - **Collect only specific data**

Network Intrusion Detector
NID Placement

- **NID Developers**
  - **Provide NID as a tool**
  - **Show what data can be captured and analyzed**
    - **NID can be very invasive**
- **NID Users**
  - **Must determine policy for how to use NID**
    - **Legal ramifications to what data is captured and analyzed.**

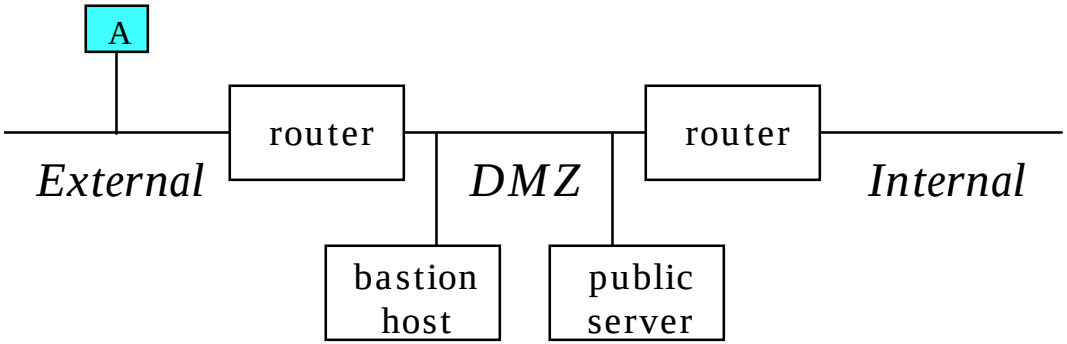
Network Intrusion Detector
NID Placement

- **With a two router firewall, NID can be placed in one of three regions**
  - **A External: directly outside the network**
  - **B DMZ: between the screening and filtering routers in the "demilitarized" zone; the bastion host or semi-public servers may be on the local segment or on another router port**
  - **C Internal: directly attached to the local network**



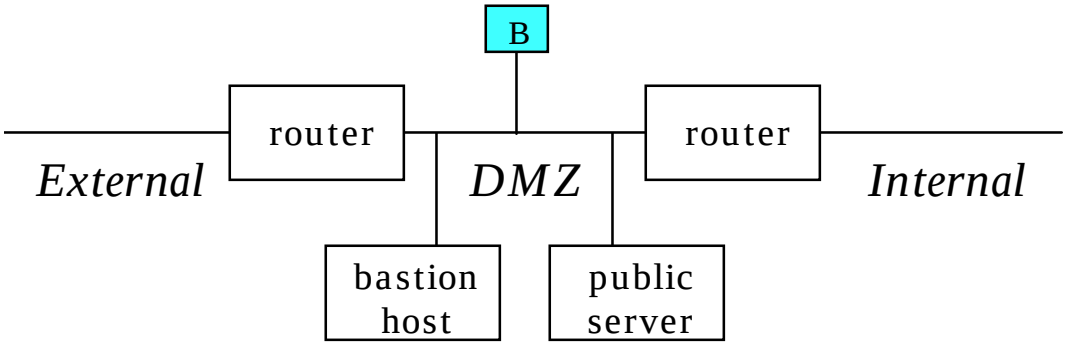
Network Intrusion Detector
External NID Placement

- ✔ All incoming and outgoing traffic may be monitored
- ✔ Internal network traffic is not monitored
- ✔ No hole need be opened through firewall for remote monitoring
- ✘ No DMZ or internal host-to-host traffic monitoring
- ✘ Completely open for external attack such as IP spoofing



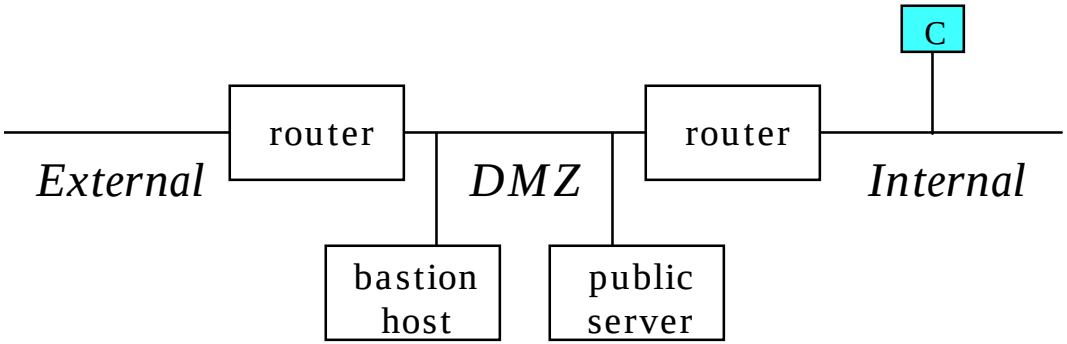
Network Intrusion Detector
DMZ NID Placement

- ✔ Most incoming and outgoing traffic may be monitored
- ❖ DMZ traffic only monitored if not on another router port
- ✔ Internal network traffic is not monitored
- ✘ Hole through first router in firewall for remote monitoring
- ✘ No internal host-to-host traffic monitoring
- ✔ Protected from external attack such as IP spoofing



Network Intrusion Detector
Internal NID Placement

- ✔ Most incoming and outgoing traffic may be monitored
- ✘ DMZ traffic is not monitored
- ❖ External network traffic is not monitored
- ✘ Hole through entire firewall for remote monitoring
- ✔ Internal host-to-host traffic monitoring
- ✔ Protected from external attack such as IP spoofing



Network Intrusion Detector New Enhancements

- **System-wide GUI interface**
  - **Reduces the learning curve for new users**
  - **Command line interface is still supported**
- **Supports FDDI networks**
  - **Monitor large backbones**
    - **Currently working on LLNL backbone**
    - **5-6 million packets / hour**
    - **Need fast machine with lots of disk**
      - **9 gig in 3 days**

Network Intrusion Detector New Enhancements

- **Have incorporated SSH as part of NID**
  - **SSH operated from GUI**
  - **Some minor setup required, this is GUI operated**
- **Portable NID**
  - **Completed port to LINUX**
    - **Red Hat**
    - **Currently Beta-testing**
    - **Full distribution by early May**

Network Intrusion Detector New Enhancements

- **NID Training Class**
  - **2-3 day class**
  - **Meant to be HANDS-ON learning**
  - **Covers everything from installing to running NID.**

Network Intrusion Detector New Enhancements

- **Ported to HP Platform**
  - **Supported on HP-UX 10.10 systems (TAC-4)**
- **Parentage Incorporated**
  - **NSA graphical tool suite**
  - **Create input files from NID data**
  - **Must have agreement with NSA to get Parentage**
    - **We cannot distribute Parentage.**