COMNET: The State of Intrusion Detection

Martin Roesch,
CTO and Founder

SOURCEfire network SECURITY

Agenda

- Background
- A Day in the Life of…
- The Complexities of an IDS
- Effective Intrusion Detection
- The Future of IDS

Background on Intrusion Detection

SOURCEfire network SECURITY

What is NIDS?

A network intrusion detection system monitors traffic in real time and alerts when suspicious activity is detected

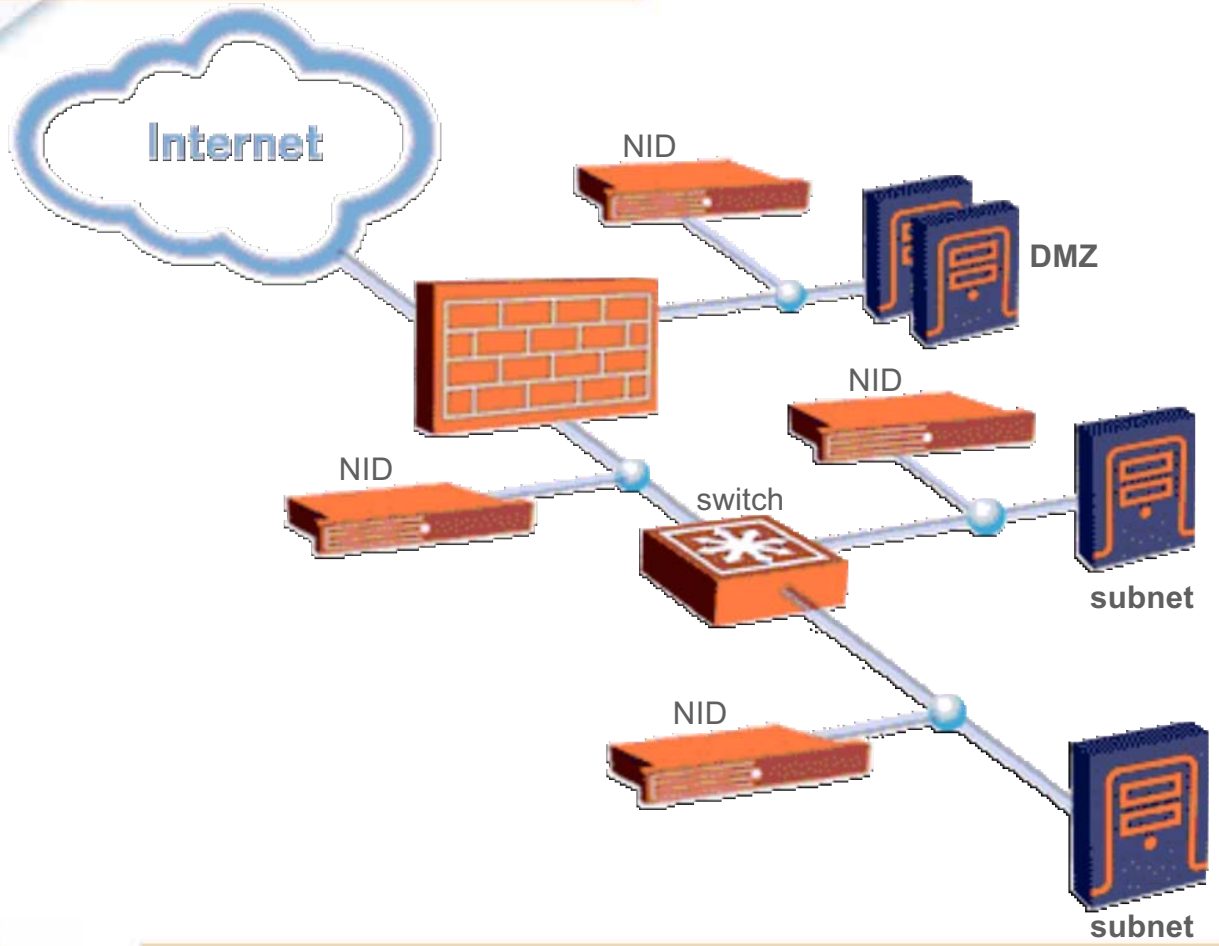
Why is NIDS Important?

Access control (firewalling) is only part of the security solution, you need network monitoring technology to secure your enterprise effectively

Complementary Security Measures

- Network IDS complements and augments firewalls
  - Provides “assurance” in case firewall is bypassed or misconfigured
  - Protects against insider threats
  - Affords forensic analysis against changing environments and threat vectors

“Defense in Depth”



A Day in the Life of…

Administrator

- Responsible for day to day administration of the IDS
- Often overworked and understaffed
- Typically lacks experience with underlying operating systems
- Struggles to stay up to date on latest vulnerabilities, threats, patches, etc.

Administrator
Specific IDS Requirements

- Ease of deployment and use
  - No third party components
  - No operating system to install or update
- Elimination of false positives
- Automatic response to new vulnerabilities

Analyst

- Responsible for maintaining corporate network security and enforcing security policies
- Has to make near real-time decisions based on information from various sources
- Must be able to quickly decide what damage has been done

Analyst
Specific IDS Requirements

- Ability to aggregate and correlate event information in near real time
- Easy access to detailed forensic information
- Ability to modify rules language to enforce security policy

Executive

- Responsible for purchasing decisions
- Oversees entire security team
- Limited exposure to actual system

Executive
Specific IDS Requirements

- Low Total Cost of Ownership
  - End-to-end solution
- Comprehensive support and maintenance
- Advanced reporting mechanisms to easily show ROI

The Complexities of IDS

SOURCEfire network SECURITY

Deficiencies of Current Systems

- Unmanageable amounts of data
- Slow response to new vulnerabilities
- Un-scalable infrastructure
- Inflexible detection methodologies

Deficiencies of Current Systems
cont'd

- Lack of ability to do policy enforcement
- Limited forensic capabilities
- High total cost of ownership
  - Require 3rd party components

Why IDS Deployments Fail

SOURCEfire network SECURITY

Why IDS Deployments Fail*

- Organizations do not understand the administrative and technical commitment the technology requires
- Auditors require NIDS and organizations deploy the technology reactively to audit reports without understanding how to manage it

*__Michael Rasmussen__, Senior Security Analyst, Giga

SOURCEfire network SECURITY

Why IDS Deployments Fail*
cont'd

- NIDS has a high amount of false alarms that frustrate the untrained user that does not have the appropriate expectations
- The technology has often been easy to bypass and often misses significant security events

*__Michael Rasmussen__, Senior Security Analyst, Giga

SOURCEfire network SECURITY

Why IDS Deployments Fail*
cont'd

- It is difficult to implement in high bandwidth, in switched environments or where communication is encrypted
- Organizations are deploying it without any intention of doing incident response — why detect an attack if you don't plan on doing anything about it?

*__Michael Rasmussen__, Senior Security Analyst, Giga

SOURCEfire network SECURITY

Effective Intrusion Detection

SOURCEfire network SECURITY

Requirements of an Effective IDS

- Installs quickly and easily
  - No hardware to source or support
  - No third party components
- Offers precise attack detection
  - Utilize multiple detection methodologies
  - Stay up to date on the latest vulnerabilities
  - Allow detection of organization specific threats

SOURCEfire network SECURITY

Requirements
cont'd

- Provides detailed forensic information
- Offers flexible deployment options
- Ensures low total cost of ownership
- Employs strong self-preservation methods for enhanced stability and uptime

"Characteristics of a Good IDS*"

- Runs continually without human supervision
- Not a "black box" - internal workings should be examinable
- Fault tolerant
- Impose minimal overhead on the system
- Resistant to subversions
- Easily tailored
- Difficult to fool

*Based on a Purdue University study

SOURCEfire network SECURITY

"Characteristics of a Good IDS*" cont'd

- Timely signature updates
- Signature accuracy
- Capable, experienced support staff
- Proven installations in complex environments
- Integration with other monitoring frameworks and security devices

*Based on a Purdue University study

SOURCEfire network SECURITY

The Future of IDS

Beyond Intrusion Detection

- Sensing technologies are becoming standardized
- Increased network speeds are changing the focus of IDS
  - Need for more focused detection
  - Usability of the information is key

Intrusion Management is the Future!

SOURCEfire network SECURITY

Complete Intrusion Management Solution

Unparalleled performance with management capabilities that scale beyond true gigabit network speeds

SOURCEfire network SECURITY

Q & A

SOURCEfire network SECURITY