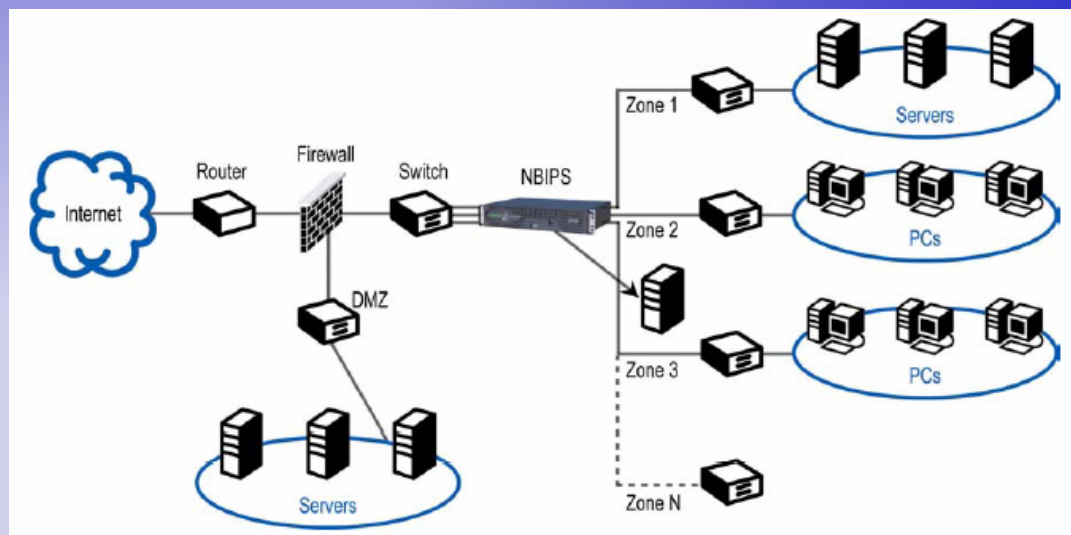


Network-based Intrusion Prevention TippingPoint UnityOne

Matthew R. Alderman, CISSP
Alderman Consulting, LLC
October 1, 2003

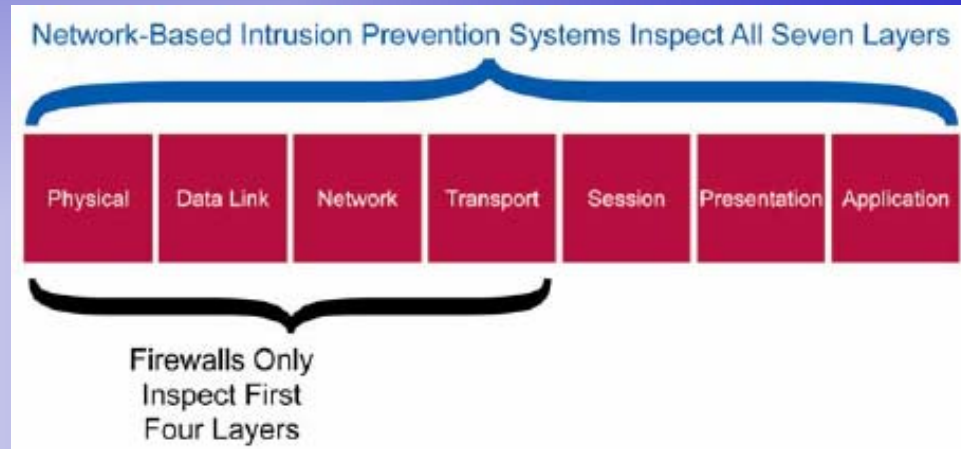
Network-based Intrusion Prevention A Primer

- ◆ An NBIPS installs in the network and is used to create physical security zones.



Network-based Intrusion Prevention A Primer (cont.)

- ◆ Network-Based Intrusion Prevention Systems are an extension of today's Firewall technologies.
- ◆ Today's Firewalls inspect only the first four layers of any packet of information flow.
- ◆ NBIPS inspect all 7 Layers, making it impossible to hide anything in the last four layers of a packet.



Network-based Intrusion Prevention Bilateral Peer-to-Peer Protection

- ◆ Peer-to-peer applications like Limewire, Grokster, Morpheus, Kazaa, represent a tremendous threat to all organizations.
- ◆ Protect your bandwidth by rate limiting or blocking illegitimate use of file-sharing applications.
- ◆ Limit your exposure to copyright infringement suits and royalties (from your employees or students breaking copyright laws).
- ◆ Protect your intellectual property from file sharing theft.

Network-based Intrusion Prevention

Basic Requirements

◆ Low Latency

- must have average latencies of less than 3 ms. regardless of frame size, traffic mix, line rate or number of attack filters/signature installed.

◆ Backbone Speeds and Large Session Counts

- must be scaleable to multi-gigabit speeds.
- must support 500,000 simultaneous sessions and 10,000 new sessions per second to be deployable.

◆ Intrinsic Reliability

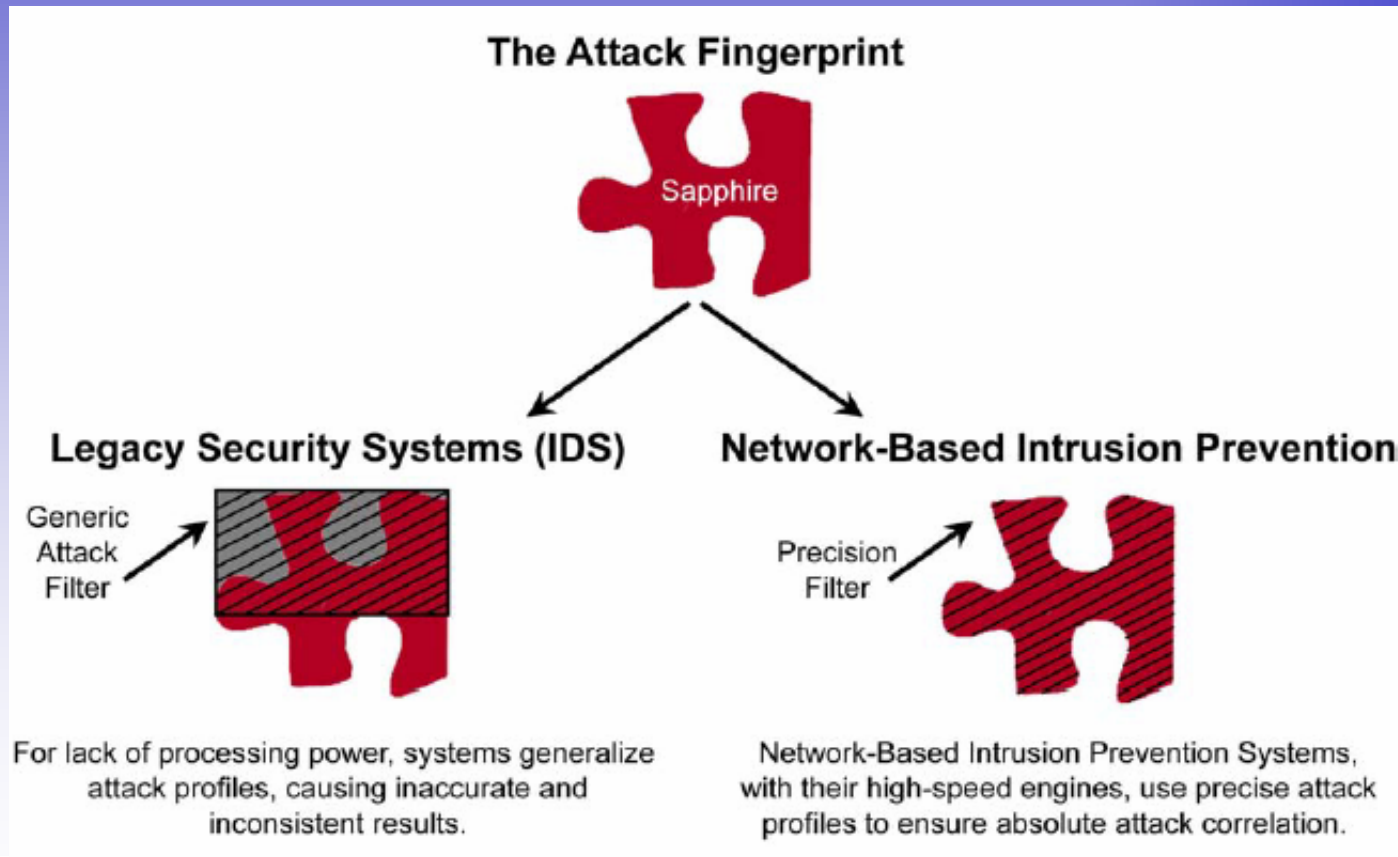
- must be able to automatically fall back to Layer 2 (transparent switch) in the case of internal failure.

◆ Absolute Precision

- a true NBIPS is designed much like a firewall and never blocks or drops good traffic.

Network-based Intrusion Prevention

Absolute Precision



TippingPoint UnityOne

◆ Intrusion Prevention Appliance

- UnityOne 200
 - 2 10/100 MB Segments (200 MB max)
- UnityOne 400
 - 4 10/100 MB Segments (400 MB max)
- UnityOne 1200
 - 4 10/100/1000 MB Segments (1.2 GB max)
- UnityOne 2400
 - 4 10/100/1000 MB Segments (2 GB max)

TippingPoint UnityOne (cont.)

◆ Intrusion Prevention System

- UnityOne 2000
 - Up to 20 10/100/1000 MB Segments (2 GB max)
- Security Management System
 - Centralized management

TippingPoint UnityOne Demo

Questions & Answers

- ◆ Is TippingPoint planning to support ATM modules in the UnityOne 2000?
 - ATM modules have been discussed and are on the road map. OC-3 and OC-12 compatible modules are at least 6 months away.
- ◆ What is in the next release of the UnityOne?
 - Two power supplies in all Intrusion Prevention Appliances.
 - Zero power failover allows Intrinsic High Availability in the event of a power failures. Requires an external patch panel (TPTI part number is available).
 - Rate shaping. The ability to inspect and prioritize traffic based on rules.

Thank You!

Matthew R. Alderman, CISSP

Alderman Consulting, LLC

5725 Deer Creek Drive

Willoughby, OH 44094

Phone: (216) 210-3243

E-mail: matthew@alderman-consulting.com

