IntruVert
NETWORKS

Intrusion Prevention Through Innovation™

Network Intrusion Detection and Prevention

March 15, 2003

Ramesh Gupta
Vice President of Engineering

ramesh@intruvert.com
408-434-8302

3200-A North First Street
San Jose, CA 95134

Key Security Components

- **For Large Enterprises and Government Customers**
  - Authentication
  - Authorization
  - Access Control
  - Directory Services
  - Host and Application Security
  - Network Security
  - Security Management

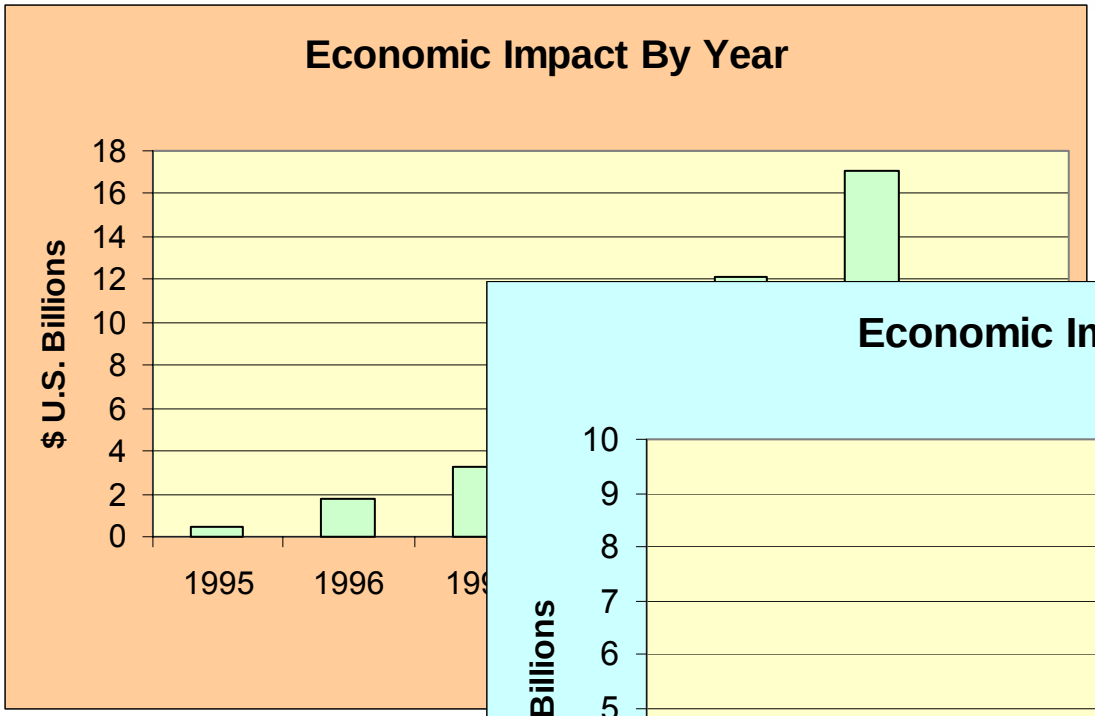
Key Network Security Components

- **Secure Network Transport**
  - VPNs
- **Network Access Control**
  - Firewalls
- **Network Intrusion Detection Systems**
  - Intrusion Detection Systems
  - Intrusion Detection and Prevention Systems

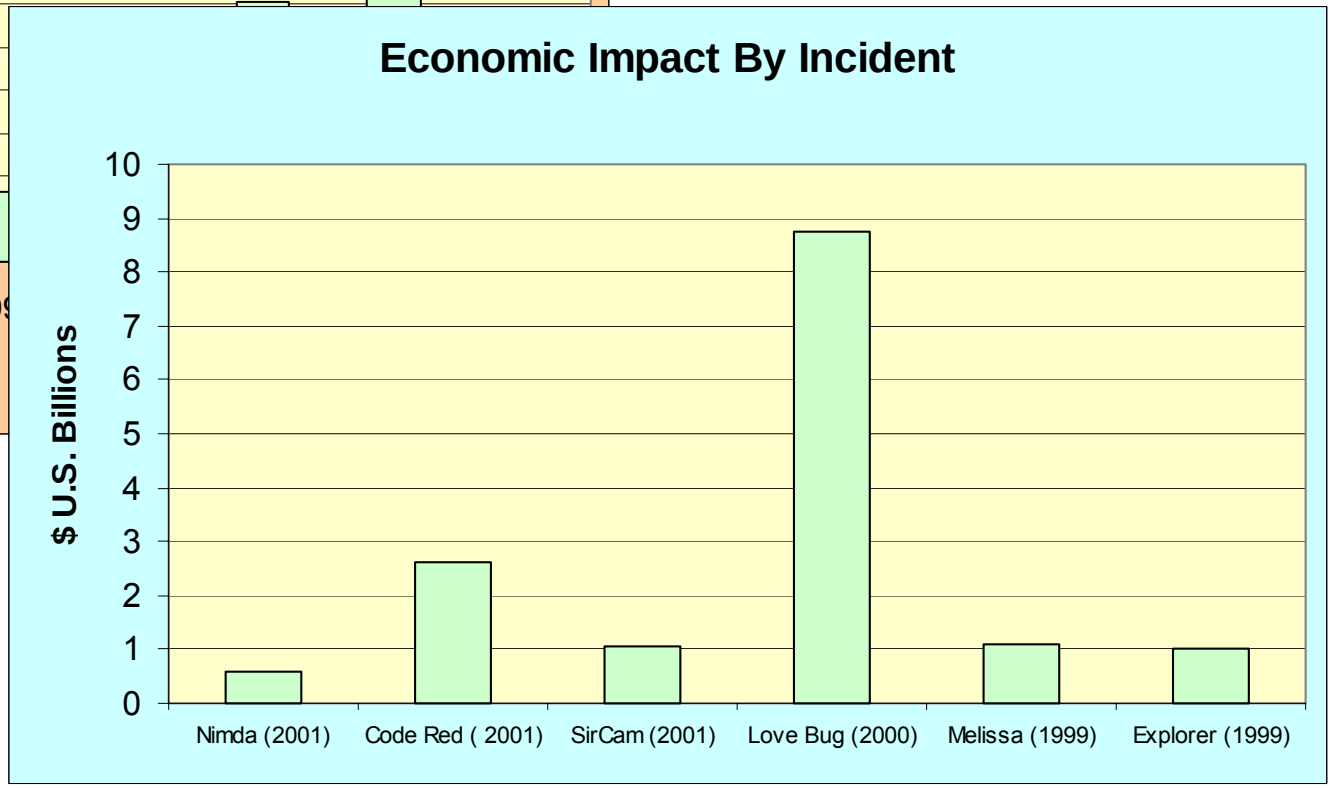
What is IDS

- **Monitor network traffic to detect malicious activity**
- **Malicious activity can include:**
  - Reconnaissance activity
  - System exploitation
  - Denial-of-service and
  - Policy violations
- **Apply countermeasures when malicious activity is detected**
  - Passive response actions
    - Generate Alerts and packet logs
    - Alert notification through e-mail and pagers
  - Active response actions
    - Terminate malicious flow with a TCP reset
    - Send ICMP Host Unreachable messages for UDP attacks
    - Reconfigure a firewall to block malicious traffic
    - Block malicious traffic

Economic Impact of Malicious Code Attacks



Source: Computer Economics



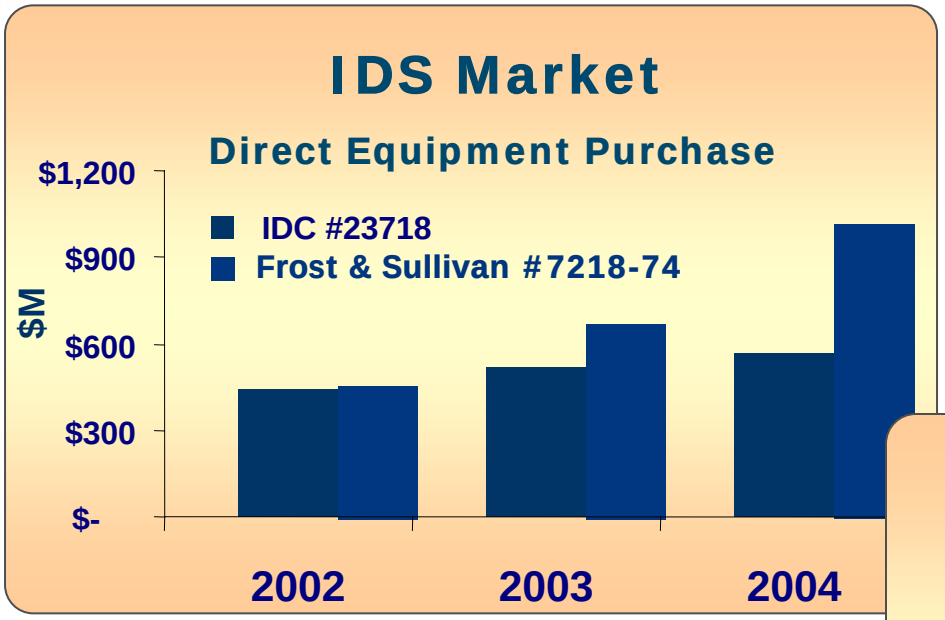
Why do we need IDS?

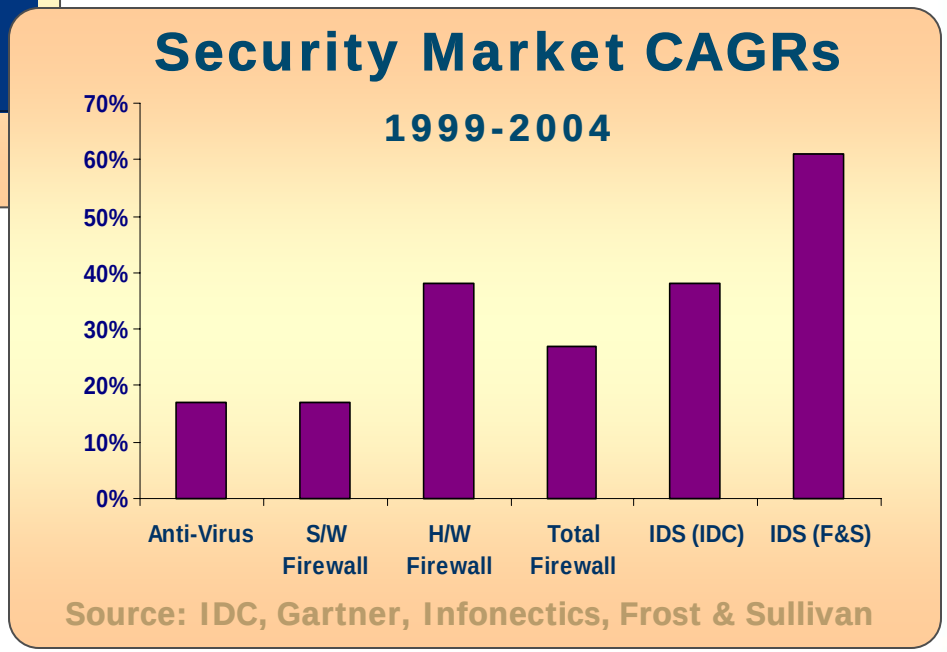
- Firewalls, while necessary, are not sufficient
- Firewalls are an access control device and do not inspect the traffic they permit
  - Vulnerable to Web attacks if HTTP is permitted
- IDS is required to monitor the actual traffic
- Very efficient for monitoring inside the network perimeter as well
- Complementary to Firewalls and VPNs and necessary for Defense-in-Depth strategy

Why is IDS a growth market?

- Growing cyber-terrorism threat especially post 9-11-01
- Cost of events like Code Red/Nimda (estimated at $3.2B by Computer Economics)
- Skills required to attack systems are readily available
- Growing recognition that IDS is necessary
- IDS can be deployed where firewalls can't
- Component of "best security practices"

IDS Market Forecasts





How are Intrusions Detected?

IntruVert NETWORKS

1 Known Attacks

Signature Detection

- Requires frequent updates
- Subscription service

2 Unknown / new Attacks

Anomaly Detection

- Not as precise as signature detection, requires human intervention
- E.g. Code Red reported as buffer overflow

3 DoS Attacks

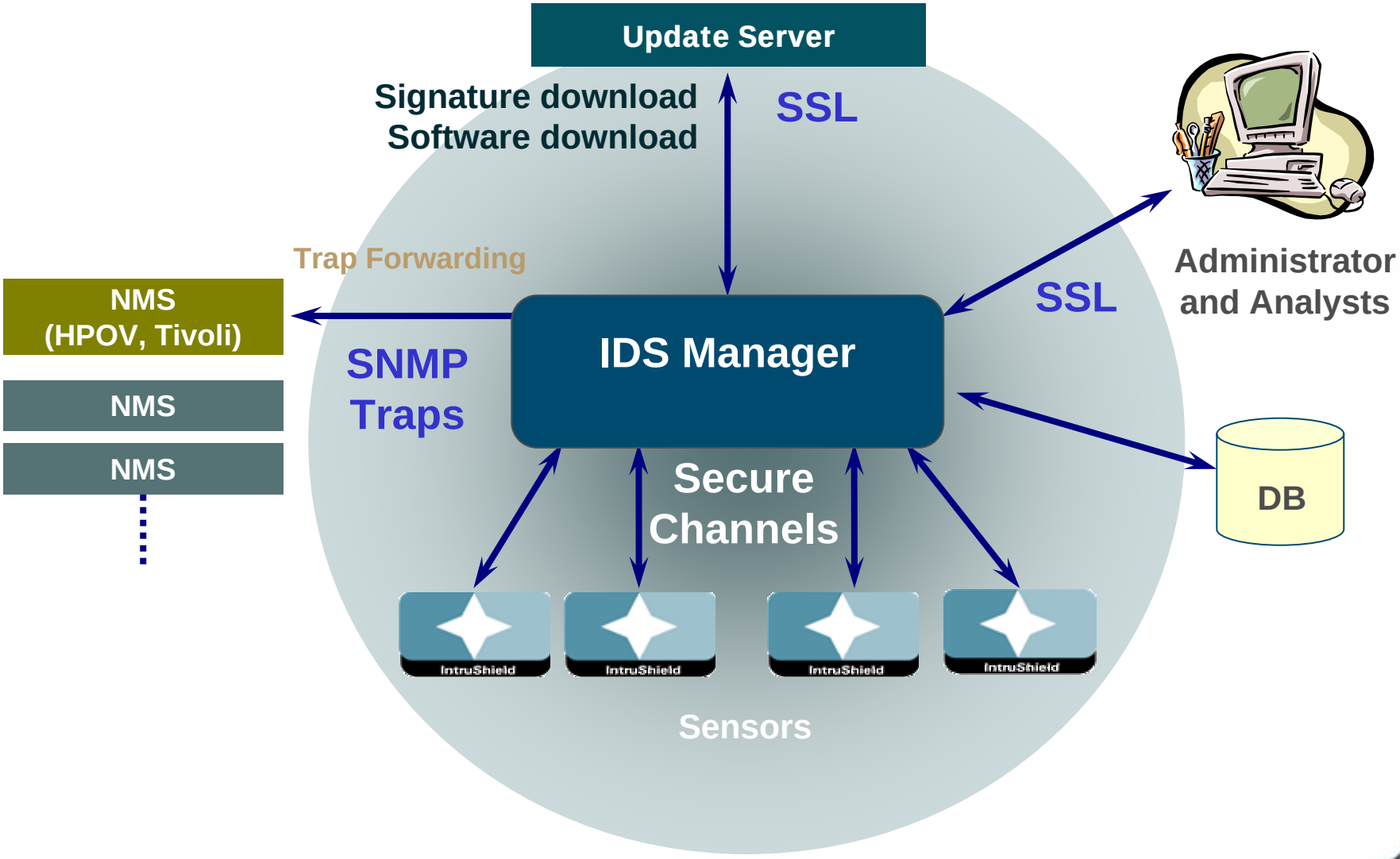
DoS / DDoS Detection

- Significant threat to eBusiness
- Must be detected accurately
- Can be misinterpreted as network outage or host malfunction

Benefits of combining three techniques

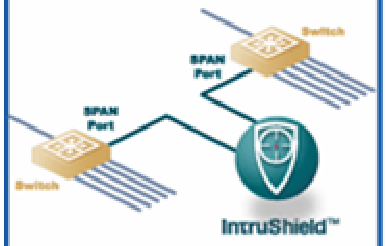
- ✓ **Create complete solution to detect ALL malicious activities**
- ✓ **Significant processing & accuracy efficiencies**
- ✓ **Single management infrastructure**
- ✓ **Lowest possible TCO**

Typical IDS System Architecture



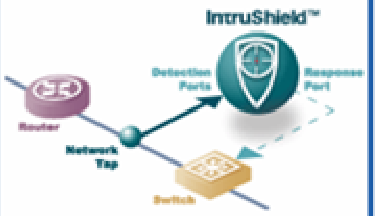
Typical IDS Deployment modes

SPAN Mode



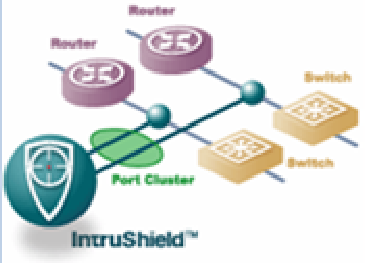
Packet "sniffing" from switch port.

Tap Mode



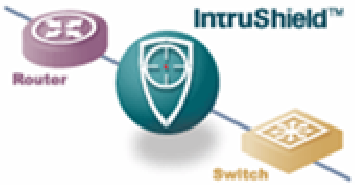
Full copy of TX and RX traffic from network wire

Port Clustering



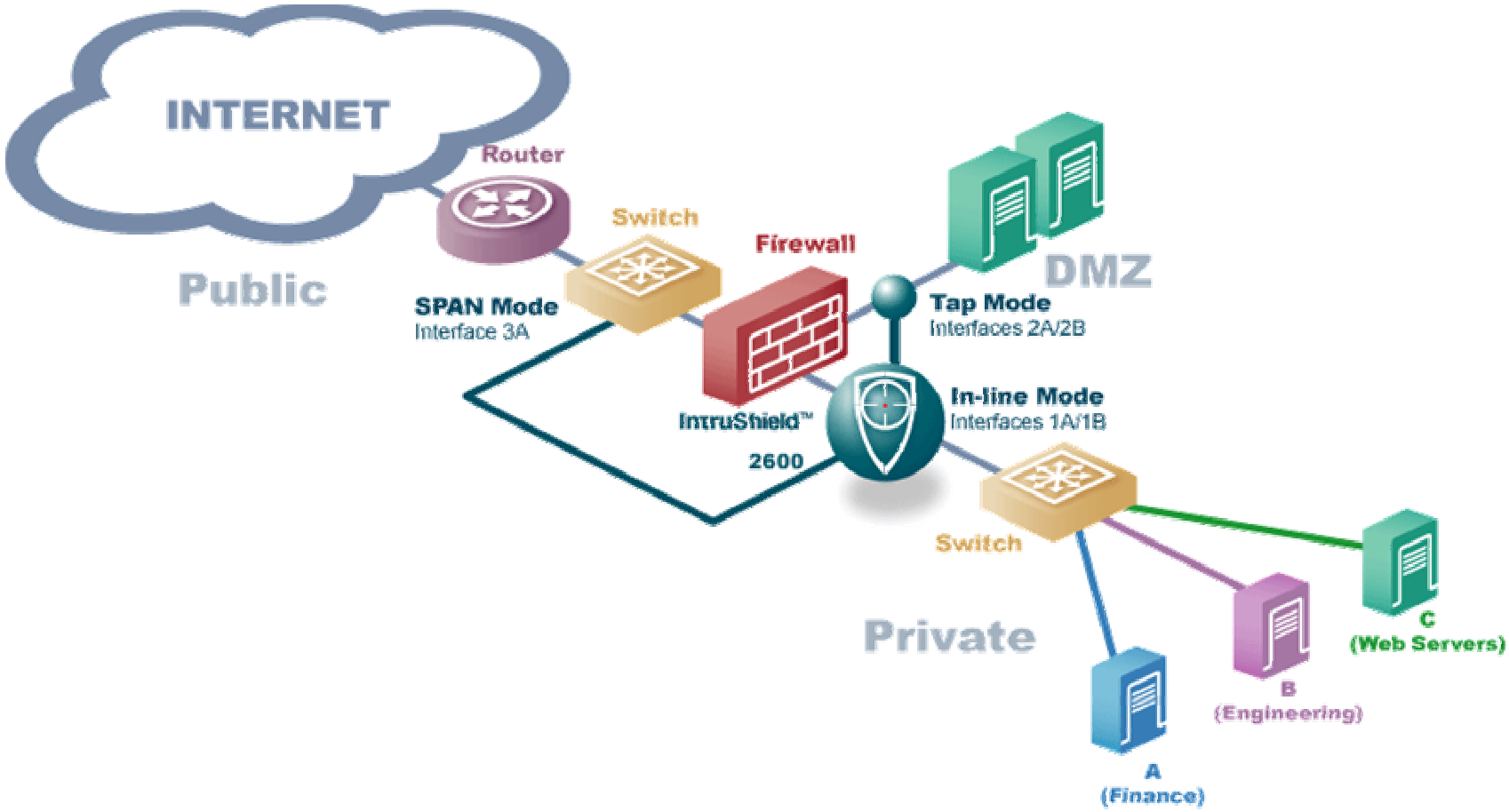
Aggregate into one traffic stream for analysis

In-line Mode

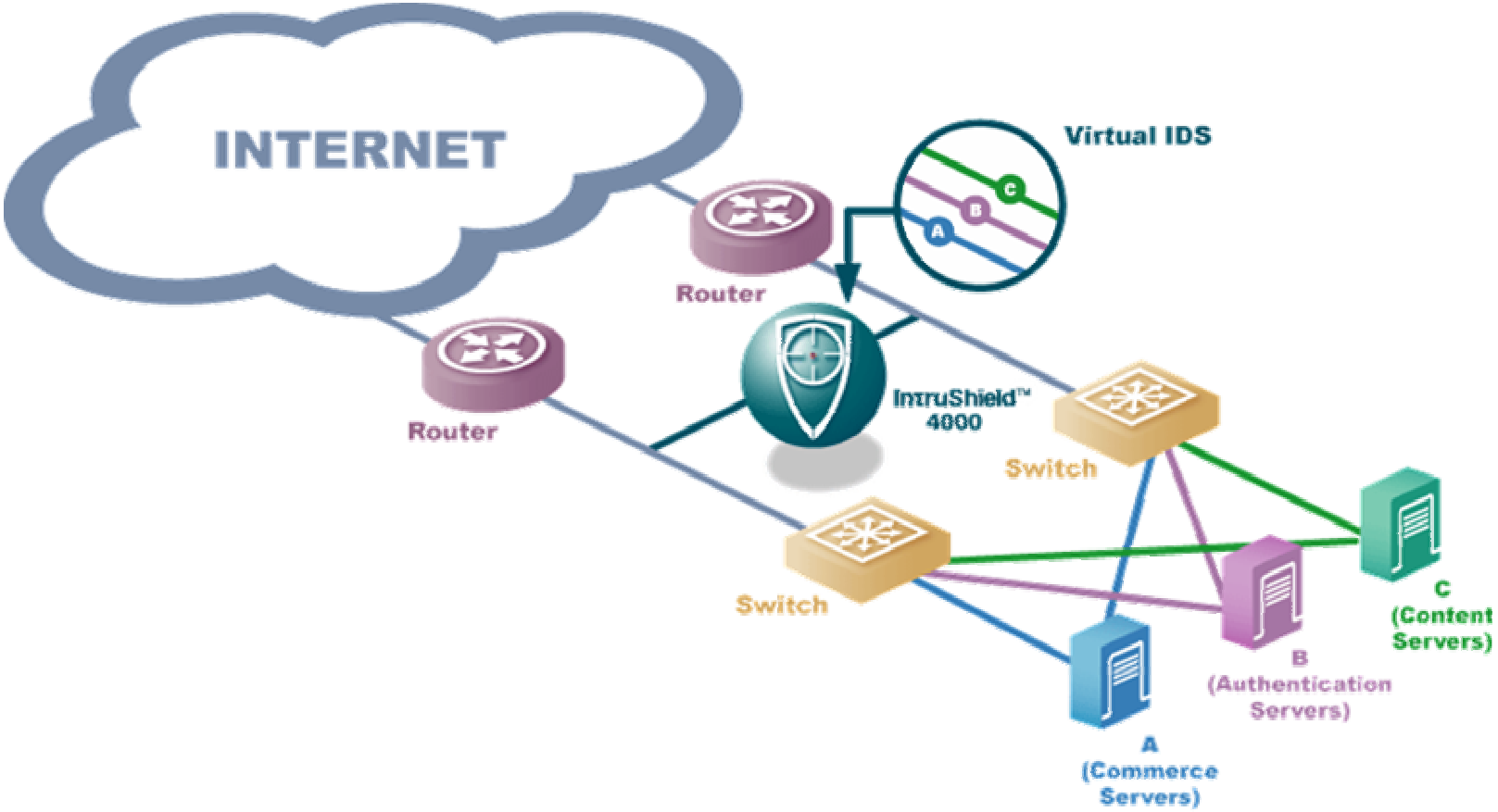


Sit in data path with active traffic

Perimeter Deployment



Enterprise Data Center / Core IDS Deployment



Key Network IDS Challenges

- **Business Challenges**
  - Comprehensive Protection
  - Total Cost of Ownership (TCO)

- **Technology Challenges**
  - Detection
    - Comprehensive Protection
  - Data Management and Analysis
    - TCO
  - Prevention
    - TCO
    - Comprehensive Protection

Detection

- **Requirements**
  - Broad Detection Coverage
    - Known, unknown and DoS attacks
  - Scalability to support growing number of Protocols and Signatures
  - High Accuracy of Detection
    - Comprehensive Protocol Analysis
    - Multiple triggers in Multiple Fields
  - Flexible deployment options to capture/process all relevant traffic
    - SPAN, TAP, In-line, Active-Passive, Active-Active, Asymmetrically routed Networks
  - Multi-Gigabit Performance with real-world traffic

Detection Challenges

- **Stealthy attacks**
  - Increasingly complex Evasion techniques
    - Quoting in protocols such as HTTP, FTP, Telnet
    - Layer 7 data fragmentation such as RPC record fragmentation
    - Ambiguous encoding mechanisms such as SNMP ASN.1 BER

- **Protocol Tunneling**
  - P2P Traffic tunneled over well known services such as HTTP
  - Instant Messaging traffic tunneled over well known services
  - Backdoors
    - Unencrypted backdoors
      - Protocol Tunneling
      - Command shell on a high port
    - Encrypted backdoors
      - Using SSH
      - Using SSL
      - Using proprietary encryption

Detection Challenges (contd.)

- **Well known Services on non-standard ports**
  - Examples
    - FTP on port 1234
    - HTTP on a high port such as 4600
    - SSH on a high port such as 8200

- **Accuracy of Detection**
  - Buffer Overflow attacks
    - Mutation using tools like ADMutate
    - Too many false positives with the following detection approaches
      - Simple Signature matching
      - Counting of NOPs
      - Counting of Binary characters
  - DoS detection using simple thresholds
    - Networks are highly dynamic and simple thresholds lead to too many false positives
  - Signature detection
    - Too many false positives with packet grepping IDSs

Detection Challenges (contd.)

- **Broad detection coverage**
  - All categories of Intrusions
    - Exploits
      - Known and Unknown or First-Strike Intrusions
    - Reconnaissance attempts
    - Denial of Service attacks
    - Policy Violations
  - Increasing number of protocols that are being targeted
  - Increasing number of Intrusions
    - The performance of most IDS systems degrades as the number of attacks increase due to the increasing number of attack patterns that the IDS has to analyze
  - Requires timely signature and protocol updates to keep pace with the vulnerabilities being discovered

Data Management and Analysis

- **Requirements**
  - Management of large number of Alerts
    - Intuitive and easy to use Alert Analysis tools
    - Attack Verification to focus on only relevant alerts
    - Alert Correlation to reduce many alerts to a few relevant Incidents
    - Work flow to manage Incidents
  - Management of large number of sensors
  - Forensic Analysis
    - Packet logs and powerful reports
  - Remote Management

Analysis Challenges

- **Increasing number of hosts and amount of traffic**
  - Increasingly diverse OSs, applications and services
- **Increasing number of attacks and thereby the number of alerts**
- **Cumbersome Alert Analysis tools**
- **Incident tracking and management**
- **Insufficient or incomprehensible forensic data**
- **Little visibility as to whether an intrusion succeeded or failed without significant time spent investigating each of the events reported by an IDS**
  - Is the intrusion relevant to the host and application
  - If relevant, is the host vulnerable to the intrusion
- **If an Intrusion Prevention System (In-line IDS) is deployed, need clear indication as to whether the intrusion was blocked or not blocked**

Intrusion Prevention

- **Growing trend towards deployment of Intrusion Prevention as opposed to just Intrusion Detection**
  - Growing interest from customers in this capability
  - Most customers wish to deploy the IDS in the Intrusion Detection Mode (sniffing mode) initially and then migrate to the Intrusion Prevention mode (in-line mode)
- **This trend has been confirmed by Industry Analysts such as Gartner**
- **Benefits of Intrusion Prevention**
  - Prevent the attack from reaching the target host and prevent the resulting compromise/loss of sensitive data
  - Avoid the costly post-attack incident analysis and clean-up
  - Turn on in-line blocking for a newly discovered attack giving the security staff enough time to patch the vulnerable hosts
    - Minimize down time for mission critical hosts and applications
  - Prevent IDS evasion and OS fingerprinting through Protocol Scrubbing (Protocol Normalization)

Intrusion Prevention Challenges

- **In-line Operation or Sniffing-mode Operation ??**
  - Passive monitoring IDS can "attempt" to block a TCP based attack using TCP resets
    - If the attack reaches the end host before the TCP reset from the IDS reaches the end host, this form of Prevention will not work
- **Reliability of the sensor**
- **Availability of the sensor (Up time)**
  - Requires timely signature and protocol updates that do not require rebooting or restarting of the sensor
- **Performance of the sensor**
- **Latency introduced by the sensor**
- **Ability to instruct the IDS as to which attacks should be blocked and which attacks should not be blocked**
- **Accuracy of detection**
  - Blocking benign traffic will result in customer dissatisfaction and affects network availability