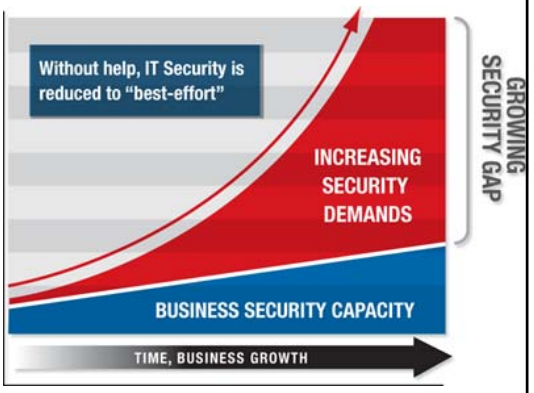
IPS evolution..

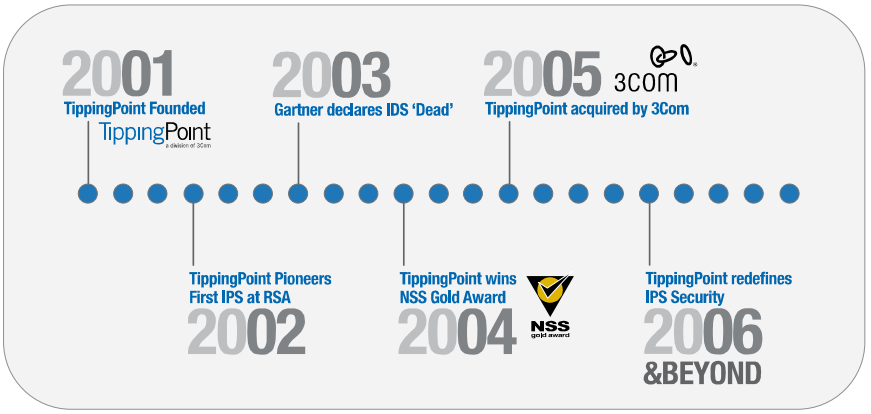
The Growing Security Gap

Security Demands Exceed Businesses Security Capacity

- Increasing rate of new vulnerabilities and decreasing time to patch
- IT complexity hinders security practice implementation
- Increasing number of attacks and attackers
- Walk-in worms, e-mail attacks, spyware
- More connected end points on the network
- Increasing number of applications
- VoIP Deployment
- Lack of IT resources



TippingPoint Intrusion Prevention System Evolution



TippingPoint
a division of 3Com

1st : Understanding the IPS

TippingPoint Perceptions..

Auditor : Do you have security for your network..?

CEO : yes, we have multiple firewall and anti-virus gateways

Auditor : do you have IPS..?

CEO : Yes we have IDS, we are secure.

Firewall : A network policy device. Through tough policy some security is yielded.

IDS : Intrusion Detection System. A forensic device. No real time business value.

IDS // IPS..??

TippingPoint What is an IPS..?

>IT IS : A network centric flow based classification engine, which acts.

>IT DOES : Block malicious traffic

>IT DOES : Block or Rate Limit undesirable traffic

>IT DOES NOT : Impact the network

>IT IS : Not known of; neither by the network team, nor the end users.

>IT DOES : only block the offending flow(s).

>IT IS : easy to install and administer

>IT IS NOT : a firewall

>IT IS NOT : an anti virus gateway

>IT CANNOT : be addressed, therefore not targeted.

>IT MUST : step up to the challenge, or step off.

>IT MUST : provide immediate protection and business value

>IT IS : A simple concept, but a real engineering challenge

TippingPoint Why not take an IDS, and call it an IPS..?

- IDS and IPS engineering teams have vastly different design goals -

IDS	IPS
>False Positive : OK, Accepted	>False Positive : Impact, Fear, Removal
>False Negative : OK, Accepted	>False Negative : Questions, Anger, Impact
>Unable to handle traffic load: no problem.	>Unable to handle traffic load: Impact
>System Crash : No problem	>System Crash : Impact
>Excessive Tuning : False Dangers, Time to install	>Excessive Tuning : Not Acceptable, Install time
>Protocol Decoders : Understood, Accepted	>Protocol Decoders : False Positives, Impact
>Exploit Signatures : OK, Easily obfuscated	>Exploit Signatures : Vulnerability Filters instead

Contrast : TippingPoint IPS // SNORT IDS

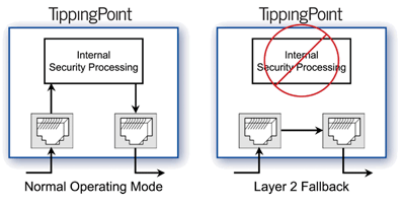
"It takes less engineering effort to design a IPS from ground up than to convert an IDS"

TippingPoint Design Priorities for IPS

1. ZERO NETWORK IMPACT
2. NO FALSE POSITIVES
3. **NO FALSE NEGATIVES**

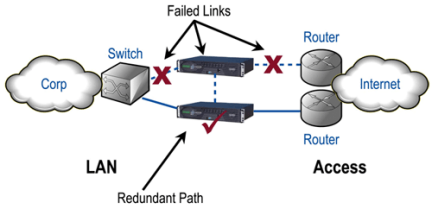
TippingPoint High Availability and Stateful Network Redundancy

Intrinsic High Availability



> Dual Hot-Swappable Power Supplies
> Self-Monitoring Watchdog Timers
—Security and Management Engines
—L2 switch fallback
> 99.999% Network Reliability
> Underlying OS - VxWorks

Stateful Network Redundancy



> Stateful Redundancy
—Active-Active
—Active-Passive
> No IP Address or MAC Address
> Transparent to Router Protocols
—HSRP, VRRP, OSPF
> Zero Power HA

TippingPoint Closing the Gap with an Intrusion Prevention System

PROTECTS:
- Microsoft Applications & Operating Systems
- Oracle Applications
- Linux O/S
- VoIP

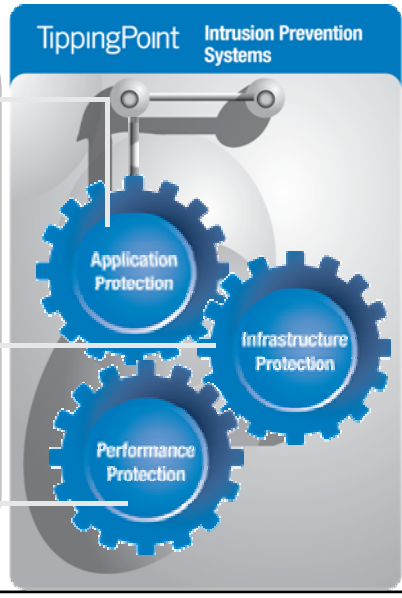
FROM:
- Worms/Walk-in Worms
- Viruses
- Trojans
- DDoS Attacks
- Internal Attacks
- Spyware

PROTECTS:
- Routers (e.g. Cisco IOS)
- Switches
- Firewalls (e.g. Netscreen, CheckPoint FW1)
- VoIP

FROM:
- Worms/Walk-in Worms
- Viruses
- Trojans
- DDoS Attacks
- SYN Floods
- Traffic Anomalies

PROTECTS:
- Bandwidth
- Server Capacity
- Missions-Critical Traffic

FROM:
- Peer-to-Peer Apps
- Unauthorized Instant Messaging
- Unauthorized Applications
- DDoS Attacks

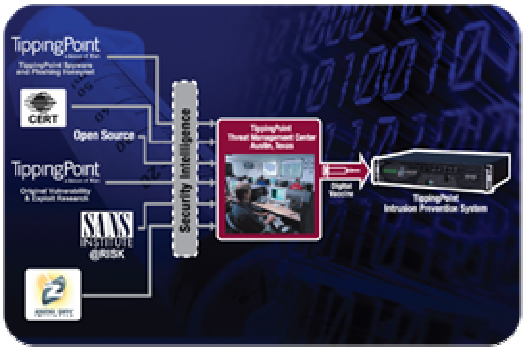


TippingPoint Management - Key in day to day operations

> Deployment must be simple, straight out of the box
> IPS & MGMT should be appliances
> What is the underlying OS used, any issues arising from these..?
> Scalability
> Filter Control must be simple, not requiring extensive tuning
> Category Control, with Filter level control if desired
> There should be a 'Recommended' set of filters which are enabled
> A need to create trust rules and exceptions - nmap etc.
> Change an entire ORG policy with one operation - fast responses.
> The IPS must be complemented by the MGMT system, not rely on it
> Reporting should be comprehensive & flexible but also 100% open

TippingPoint Filter Update Service

> Your IPS is good the day you buy it!
> Must be weekly at least
> Emergency Filter updates
> Check it for value:
  — Microsoft Tuesday
  — SANS Top 20
  — Your environment
  — False claims
> Must be zero downtime to update
> Accuracy is key - BLOCKING!
> Extensibility
  — Signatures, vulnerabilities, traffic and protocol anomalies
  — New Threats: P2P, Instant Messaging, Spyware, Phishing, VOIP



TippingPoint Trials // Bakeoffs

- The vendor must be comfortable to put the device straight inline & blocking
- Don't use the IDS mindset : All Filters on - Permit & Notify - you're buying IPS!
- Look for the fit in YOUR environment
- Use your OWN data to test the unit with - same data, for all vendors
- How easy is it to understand and drive the IPS..?
- Put the vendor to the test..:
  - Check claims made in tenders
  - Contact Support
  - Ease of 'out of box' experience… no vendor SE coaxing
- Test speed - lots of traffic, and attacks at the same time, measure results
- Look to understand the architecture - what is the underlying OS and hardware..?
- Check Filter accuracy and repeatability under load
- Police very closely what the vendor tells you..!
- If the SE has a hard time, you will also!

TippingPoint Testing methodologies

- Beware of '3rd' party independent test houses - Miercom etc
- Look for solid logic in testing, not vendor bias
- Don't use any PCAP's that you have not created yourself
- Let Vendors use their PCAP's only on THEIR equipment
- The circular debate : Compare results from one IPS to another..
- Look for external feedback - Secunia, Google, vendor reputation..
- When you don't have time or expertise look to the experts

NSS gold award

ICSA labs A DIVISION OF CYBERTRUST

TippingPoint a division of 3Com

3rd : Real world…

TippingPoint The IPS market : Today

- User education still showing to be low
- Network Giants power up the marketing engines and FUD
- Most every customer tries to turn the IPS into an IDS
- Every ‘security’ vendor has an IPS - even Novell..? - mixed messaging
- Many IPS’s deployed but offering literally no business value
- Corporate Governance dictating IPS installations
- Banks : closing branches, more online transactions
- Education : Default Open makes it hard to police with firewalls
- Mission Critical system protection : Car manufacturing etc
- An increasing mindset change : VPN Links / WAN Links etc.

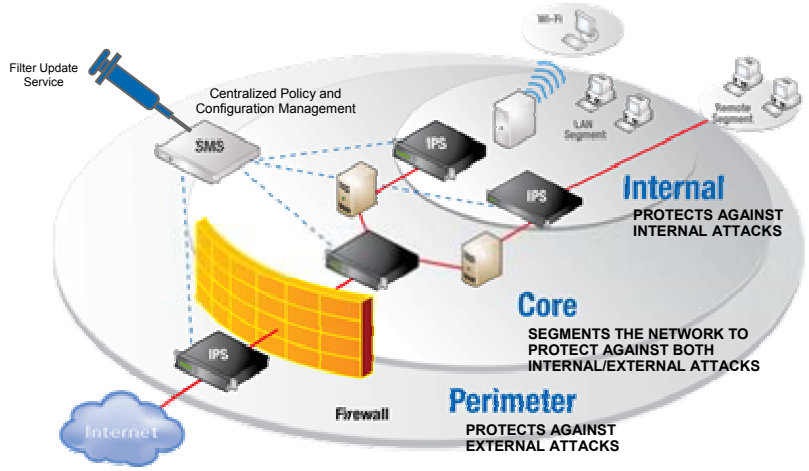
TippingPoint VoIP issues

- The issues with VoIP
  - Confidentiality
  - DoS
- Average IT life span is 3-5 years
- VoIP is experiencing wide deployments today, and increasing
- Vendors moving to deliver full feature set over SIP
- Many SIP vulnerabilities today, increasing..
- Call Servers should NOT be treated as just another server etc
- What is the impact to your business if your call server is DoS’d..?

VOIPSA
VoIP Security Alliance

www.voipsa.org

TippingPoint Flexible Deployment Core to Edge



TippingPoint
a division of 3Com

INLINE, BLOCKING RIGHT FROM THE WORD GO