Advanced Network Security Testing

Avalanche Unified Security Testing

Michael Jack

Inspired Innovation

Agenda

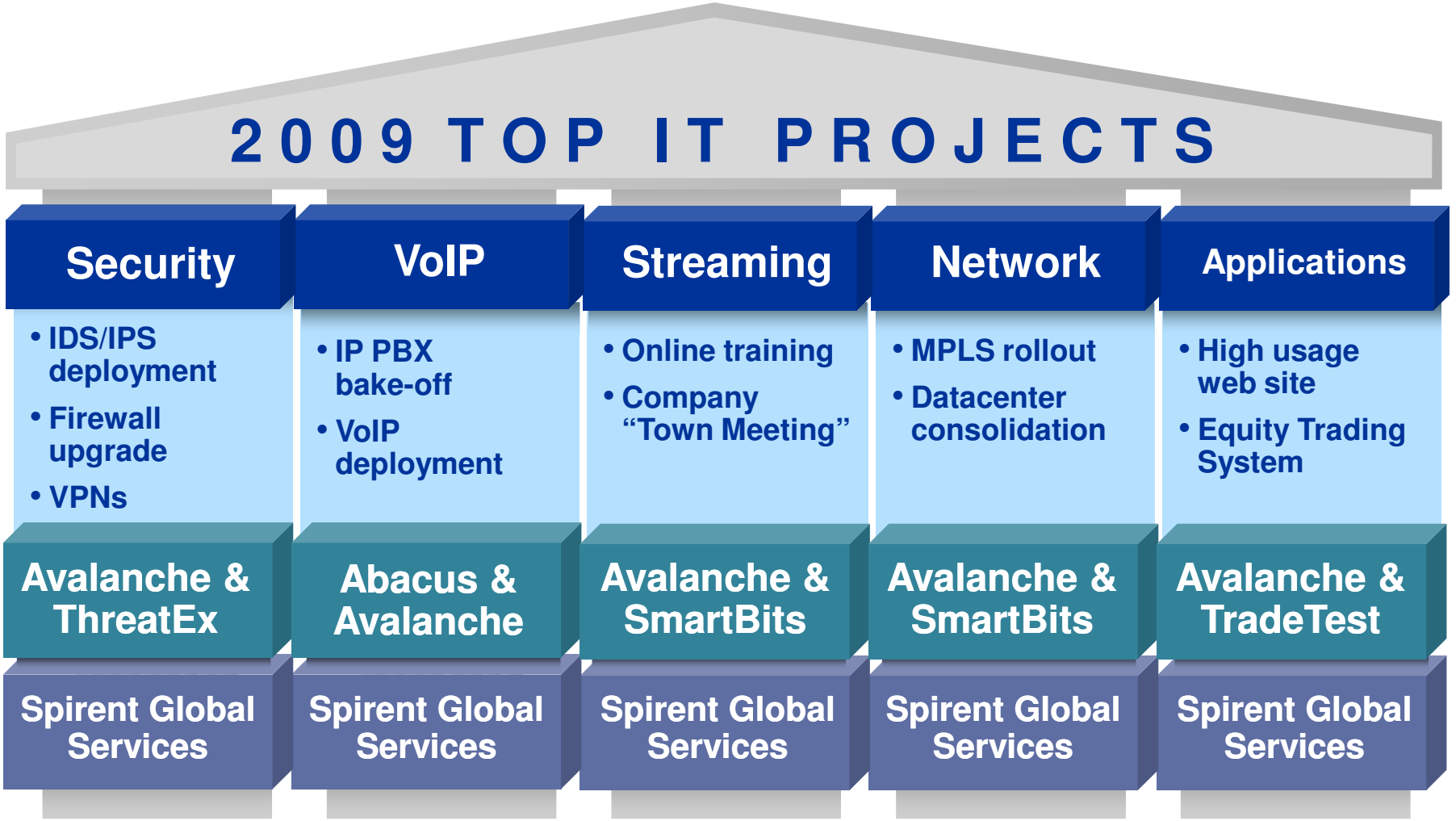
- The need for Defense In-depth
- Security Performance Issues
- Unified Testing
- Spirent User Quality of Experience Products
- Summary

Top IT Goals

- Improve availability
  - Deliver 24x7x365 application availability
  - Meet or exceed user performance requirements
- Increase security
  - Device-level: firewall, IDP, router, server, switch, etc.
  - End-to-end: user to application
- Save money
  - Buy right: select the right devices for the network and traffic mix
  - Reduce capital & operating costs: exact-size the network

Availability AND Security AND Savings

Spirent's Testing Solutions Ensure Success of Top IT Projects

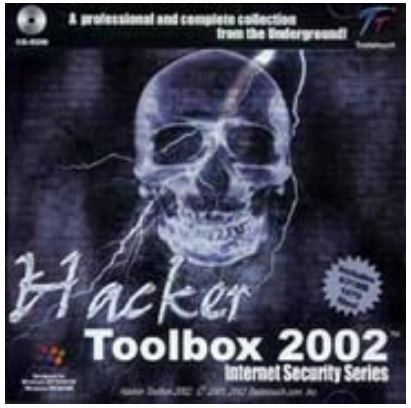


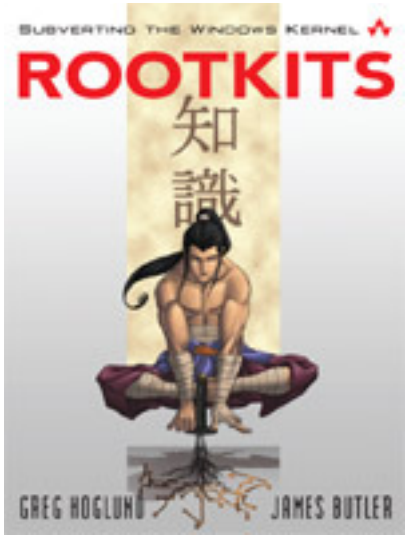
SPIRENT Communications

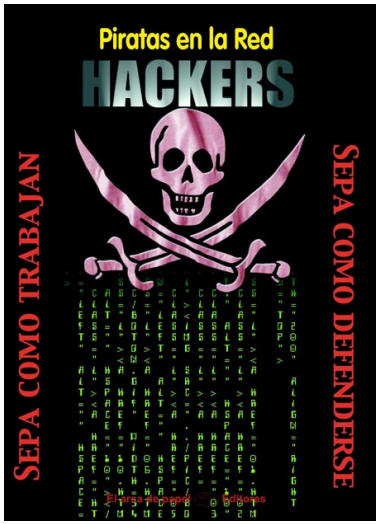
Inspired Innovation

Modern day Security Challenge

- Vulnerable code
- Hackers - > Exploits
- Increased Attack sophistication
- Attack automation
- Frequency of attacks
- Faster rate of vulnerability – 0 day
- Telecommunication companies and service providers are at greater risk with the addition of application services
  - Network Vulnerability
  - Application Vulnerability



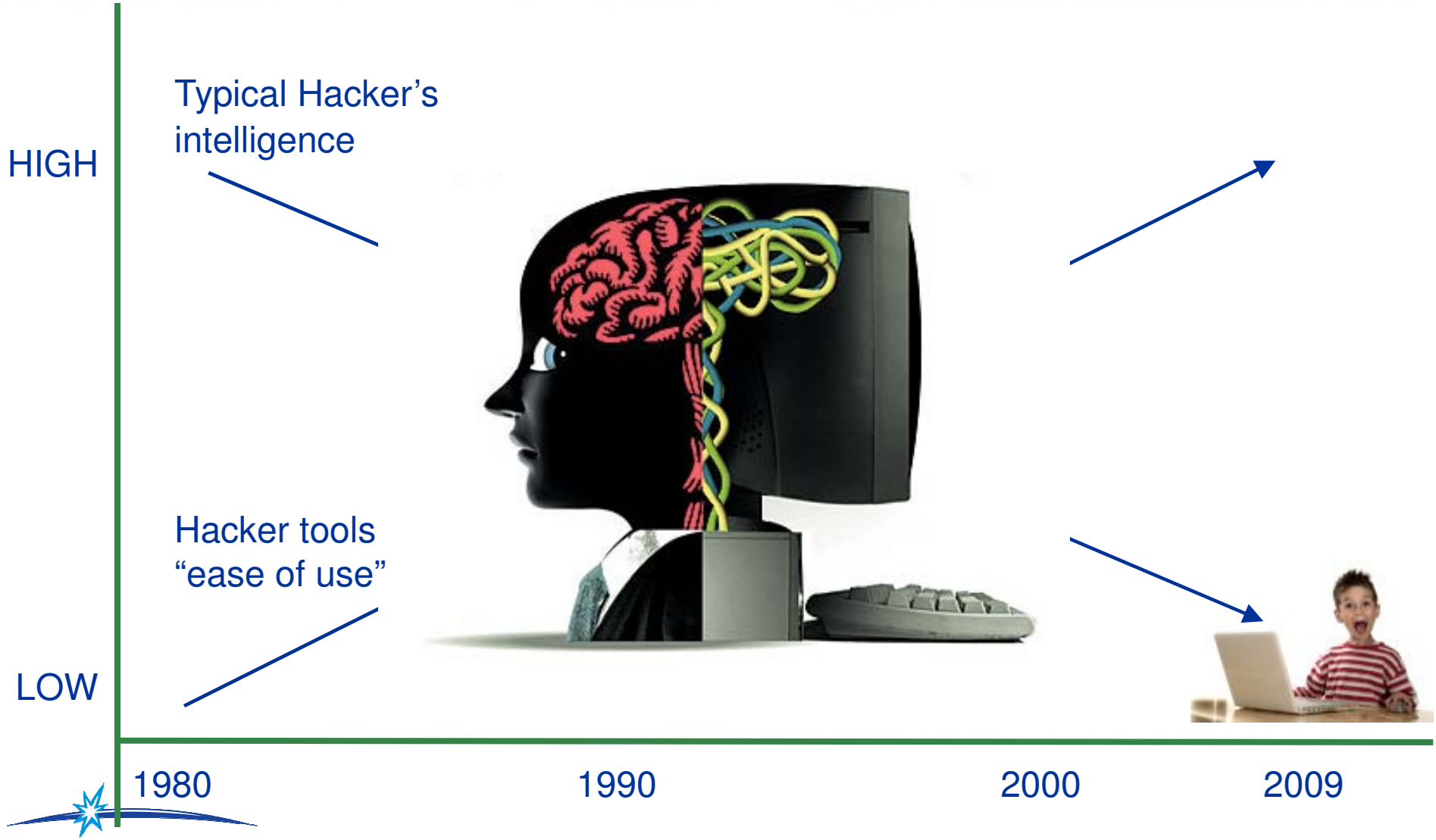




SPIRENT Communications

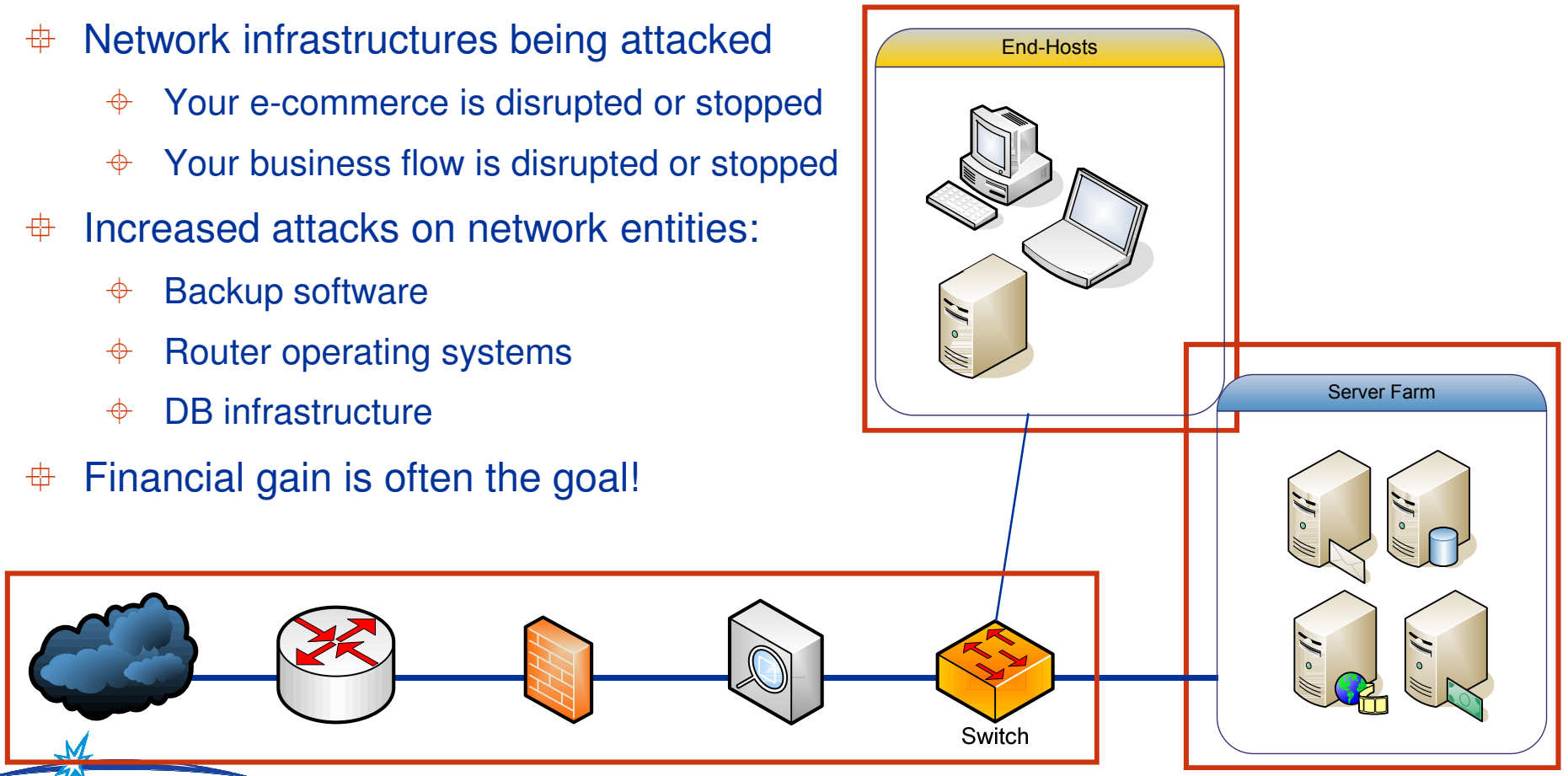
Inspired Innovation

Hacker Profile



The Shift Towards Network Attacks

- End hosts and Servers are no longer the only targets!
- Network infrastructures being attacked
  - Your e-commerce is disrupted or stopped
  - Your business flow is disrupted or stopped
- Increased attacks on network entities:
  - Backup software
  - Router operating systems
  - DB infrastructure
- Financial gain is often the goal!



Network Attacks Are Costly…

Facts:

- *85% of Fortune 1000 companies annually experience network attacks*

- *The net average cost PER attack is $2M*
  - *A spate of DDoS attacks against Amazon, Yahoo, eBay, and other major sites in February 2008 caused an estimated cumulative loss of US$1.2 billion*

    Source Yankee Group

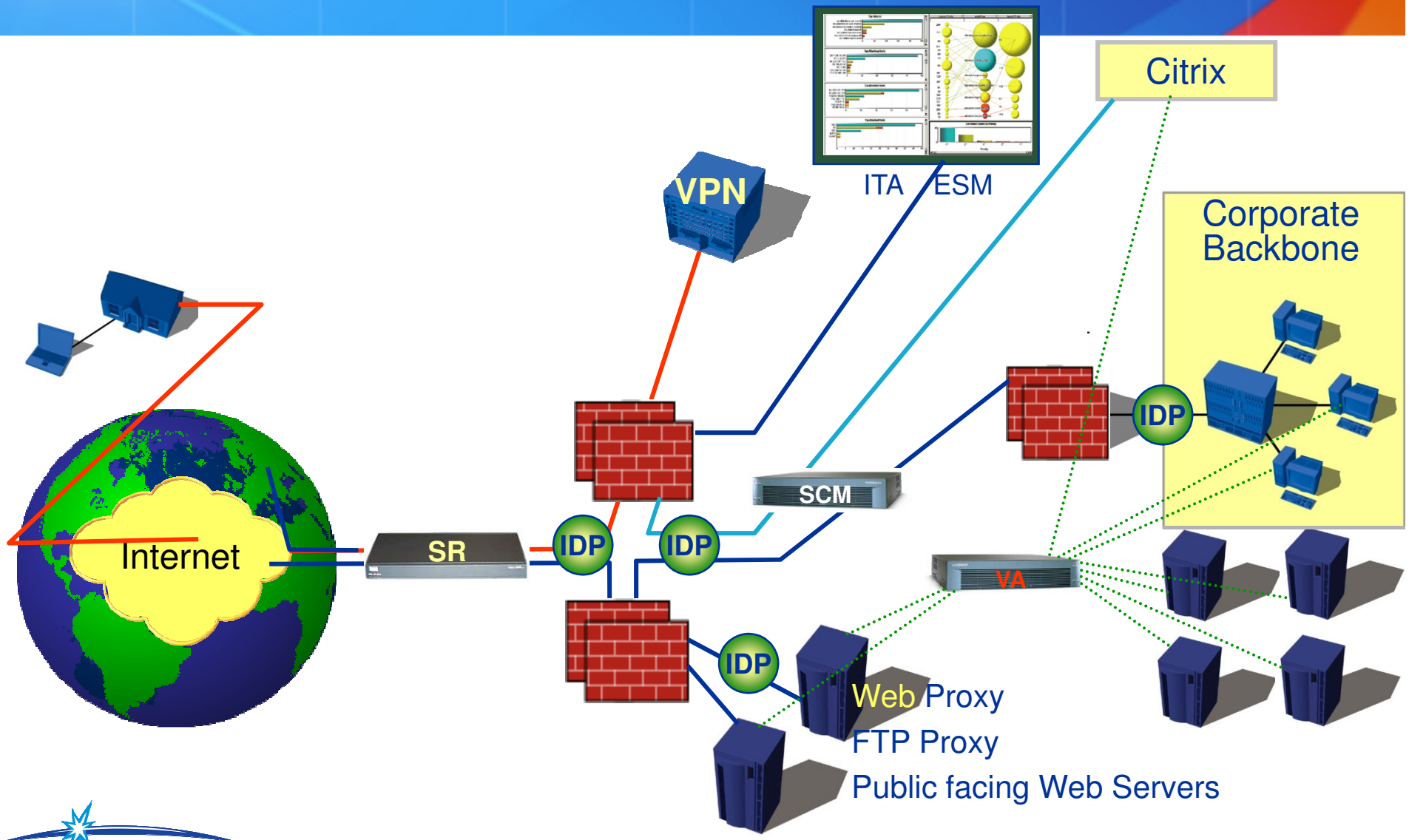
  - Microsoft lost approximately US$500 million over the course of a few days from a DDoS attack on its site.
- *Your customers have a very short acceptance of network vulnerabilities. They move elsewhere.*

SPIRENT Communications

Inspired Innovation

"How secure are you? Can you *prove* it?"

Typical Perimeter Defense Tools



SPIRENT Communications

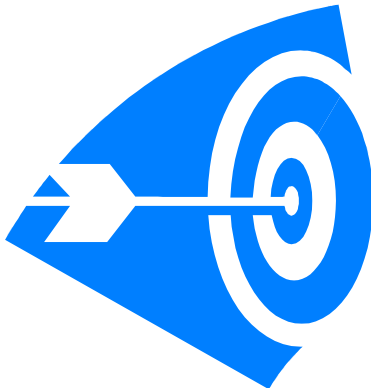
Inspired Innovation


SPIRENT
Communications
Security Performance Issues
Inspired Innovation

Security Performance issues impact user experience

- Security is merely a specialized application
- Often, security is the weak link in application processing
  - Security devices are now in-line
  - Nearly every end station runs its own security component
  - Any security infrastructure change affects application performance
    - E.g. added policies, IDP pattern matching, virus scanning, etc.
- Security processing can be considered a form of impairment
  - Adds application latency
  - May cause packet loss
  - Applications that worked may time out when a configuration changes
  - Customers may see longer delays if security is not carefully applied
    - So, security must be deployed with minimum application impact

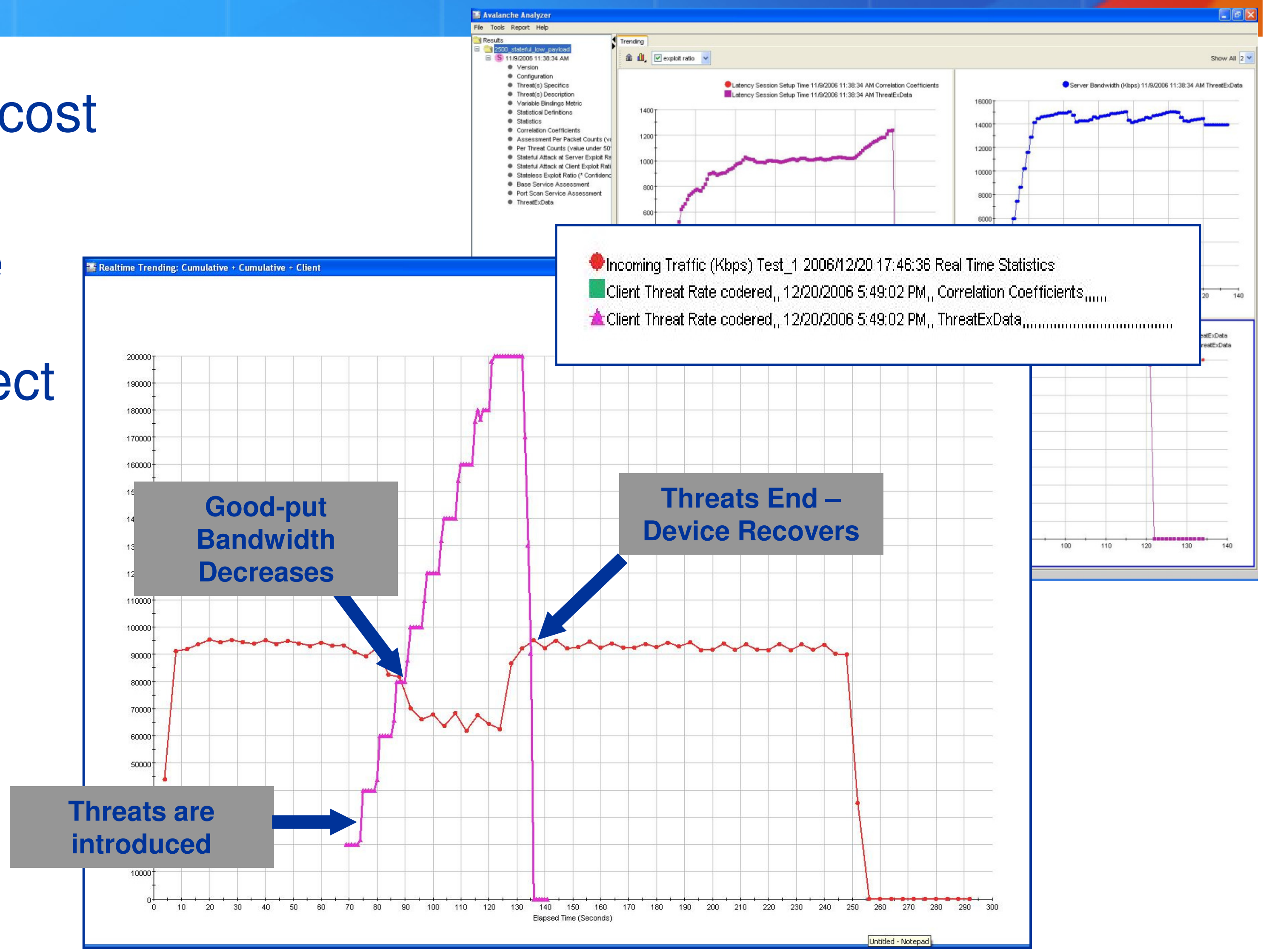
Key Security Questions



- End-to-end Security
  - Is bad traffic stopped during an attack?
  - Does layering of devices jeopardize overall security?
- Availability
  - Is good traffic throughput sustained while under attack?
- Adaptability
  - Is it easy to reconfigure and block new attacks?
- Accuracy
  - Are attacks actually detected and blocked? False positives?
- Visibility
  - Can you isolate device-level faults in an end-to-end network?
  - Can you manage real-time threat identification, analysis and mitigation?

Action / Reaction

- What is the cost of access
- Are defense mechanism able to protect normailzed access

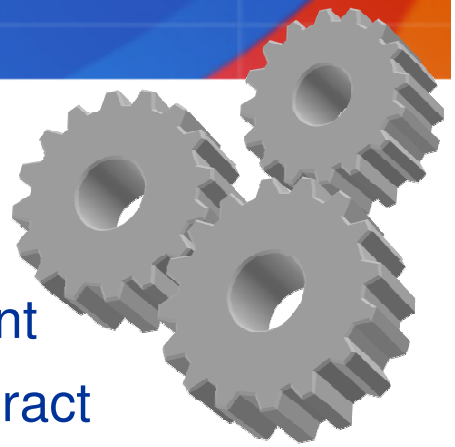


Avalanche Analyzer

SPIRENT Communications

Inspired Innovation

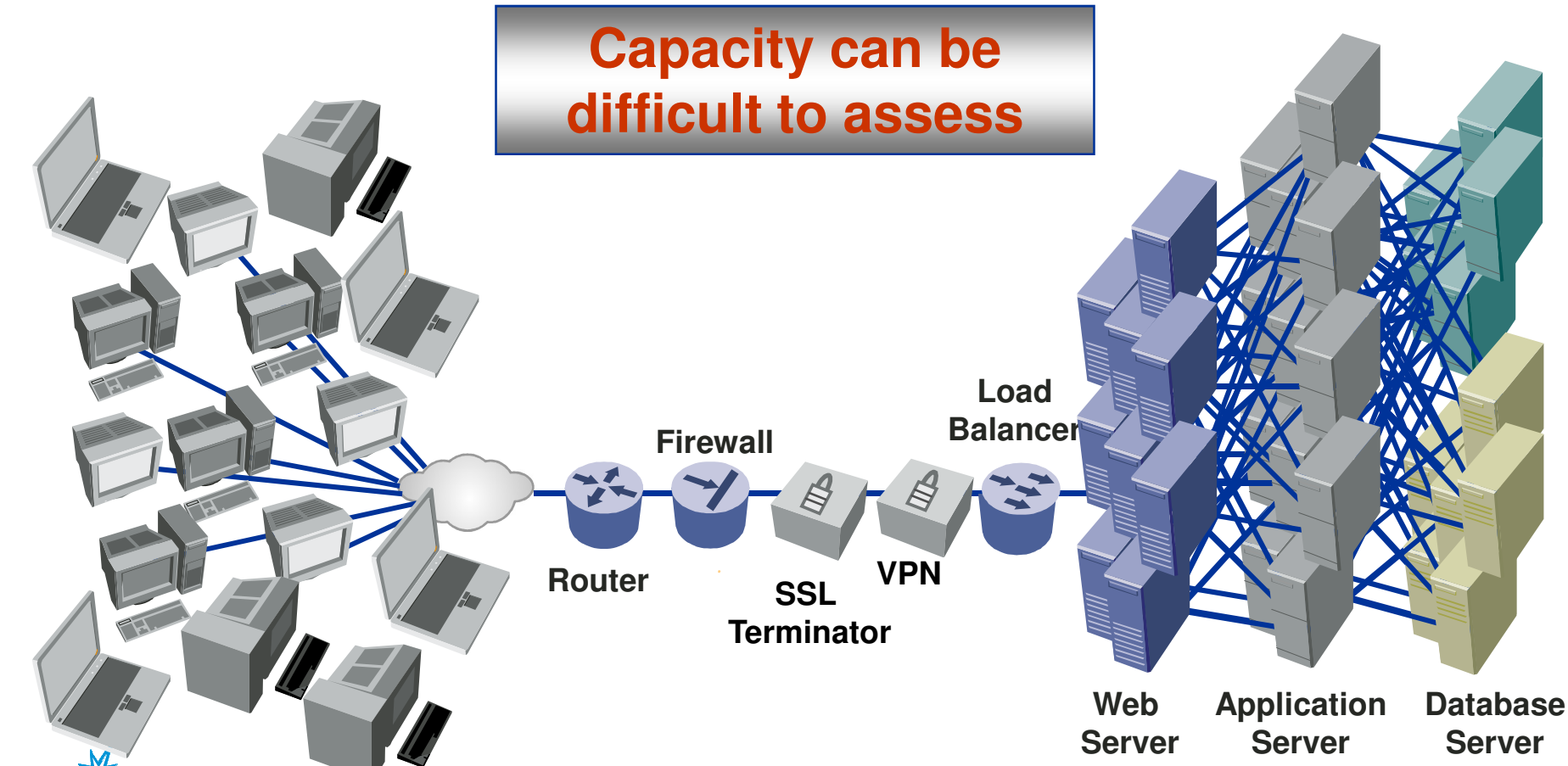
Why Should We Test?



- Testing is an insurance policy
  - Shows how applications perform before deployment
  - Shows how applications, network and security interact
  - Helps determine capacity and failure scenarios
- Testing should be performed before you deploy:
- New application software or software upgrade
  - A new network device or device software upgrade
  - Any network topology change or new service provider

- "Plug and Pray", Where should you find your issues? Production or Test??

Problem : Application & Network Infrastructure is Complex

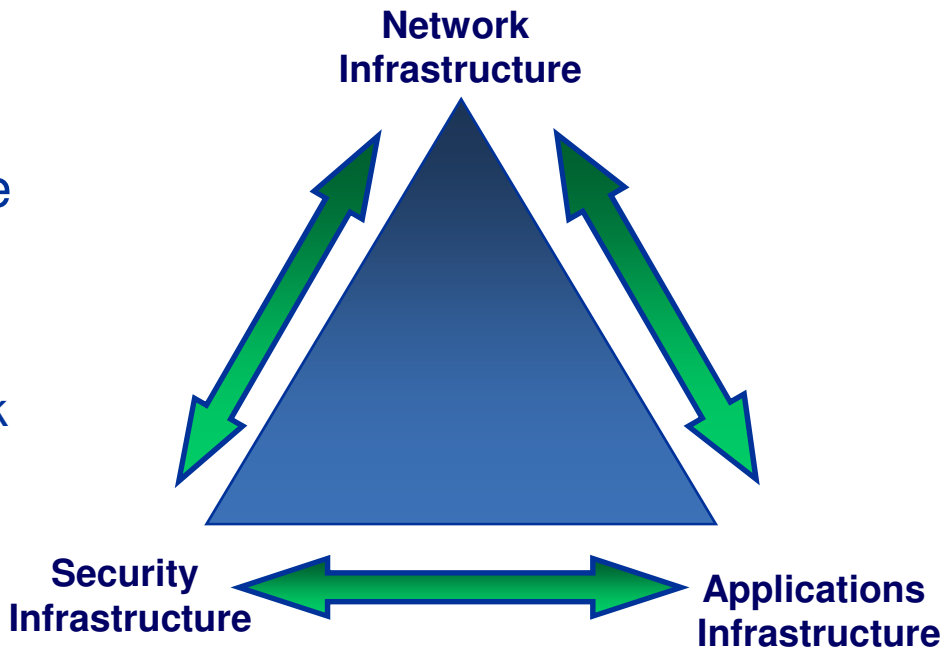


SPIRENT Communications

Inspired Innovation

A Better Approach - Unified Testing

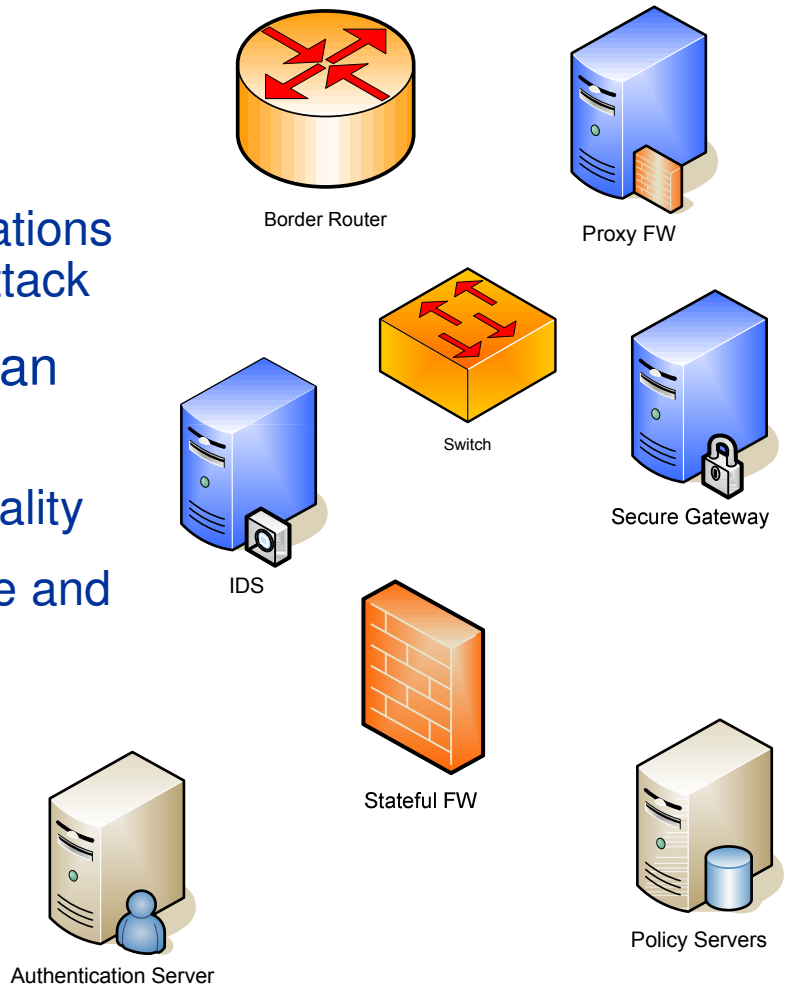
- Unified Testing: Testing your applications, security and network infrastructure together
- Unified Testing enables testing the User Experience
  - Enables you to correlate user experience to your own mix of applications, security and network infrastructure
  - Enables device verification in a realistic environment
  - Simulates actual users to show system-level operation
  - Enables SLA success verification
  - Interactive testing *ensures* success before deployment



SPIRENT Communications Inspired Innovation

Why Test Layer 4 through Layer 7?

- L4-L7 testing is required to show:
  - How L2-L3 devices operate in a production environment
  - How the user experience and applications varies under load, impairment and attack
- *Only* actual payloads *and* protocols can test security and applications
  - Integrity, Authentication & Confidentiality
  - Stateful devices and proxies examine and act based on payload contents:
    - Firewalls & IDS/IDP Devices
    - Application Gateways (proxies)
    - Secure Gateways & VPNs
    - Unified Threat Management



System Test Problems

Complexity

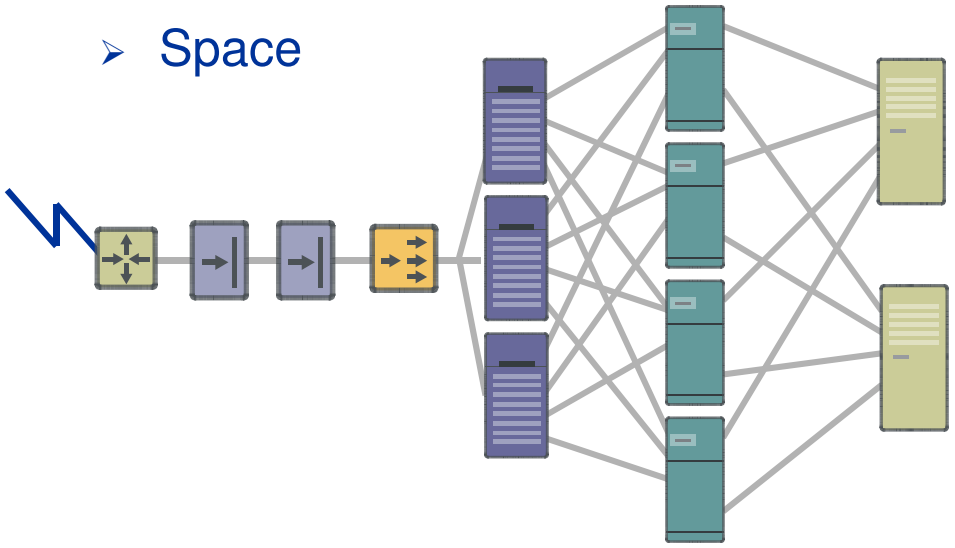
- Complex interactions under load
- Capacity Assessment requires stressing
- Scalability problems
- Unconfirmed vendor performance claims
- Failure prone

Cost

- Hardware and software
- Administration
- Personnel
- Space

Time

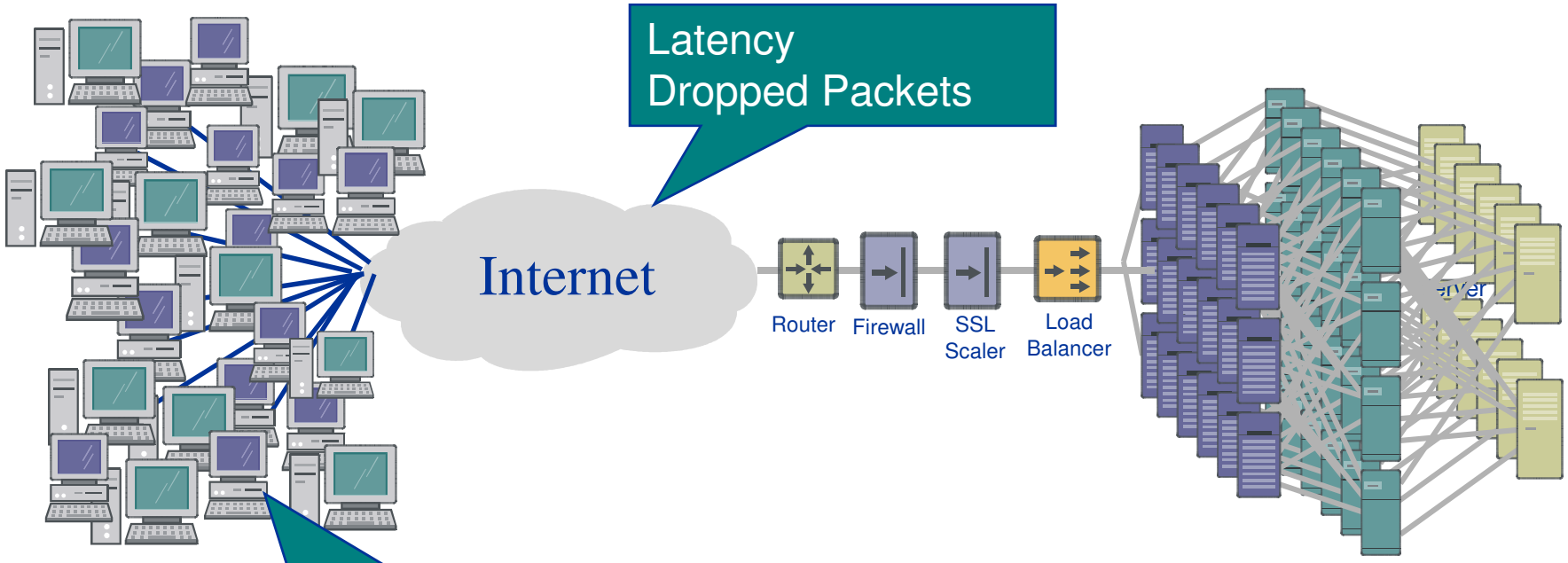
- Test setup and execution is time-consuming



SPIRENT Communications

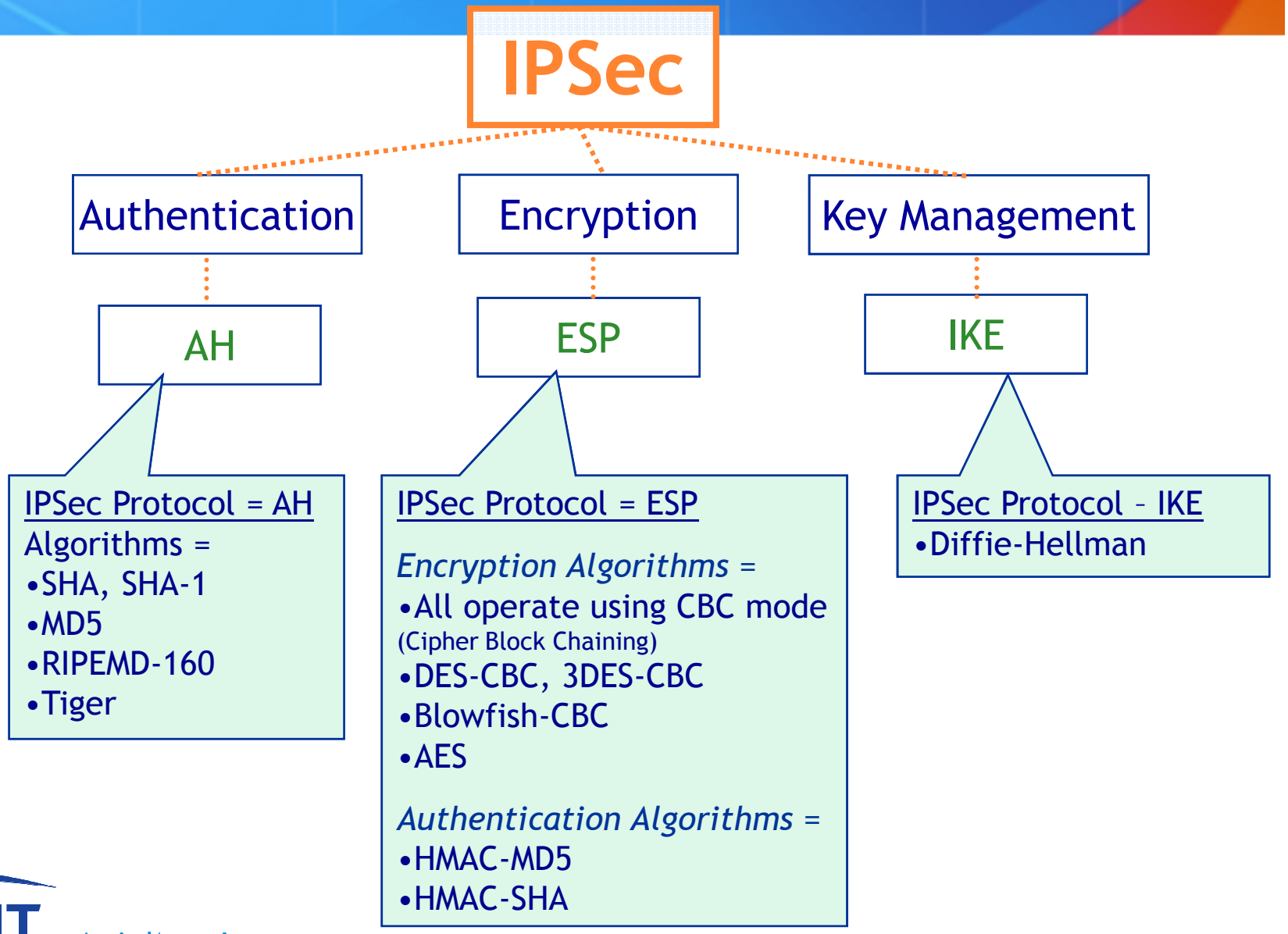
Inspired Innovation

Capacity Assessment requires simulating Clients and the Internet

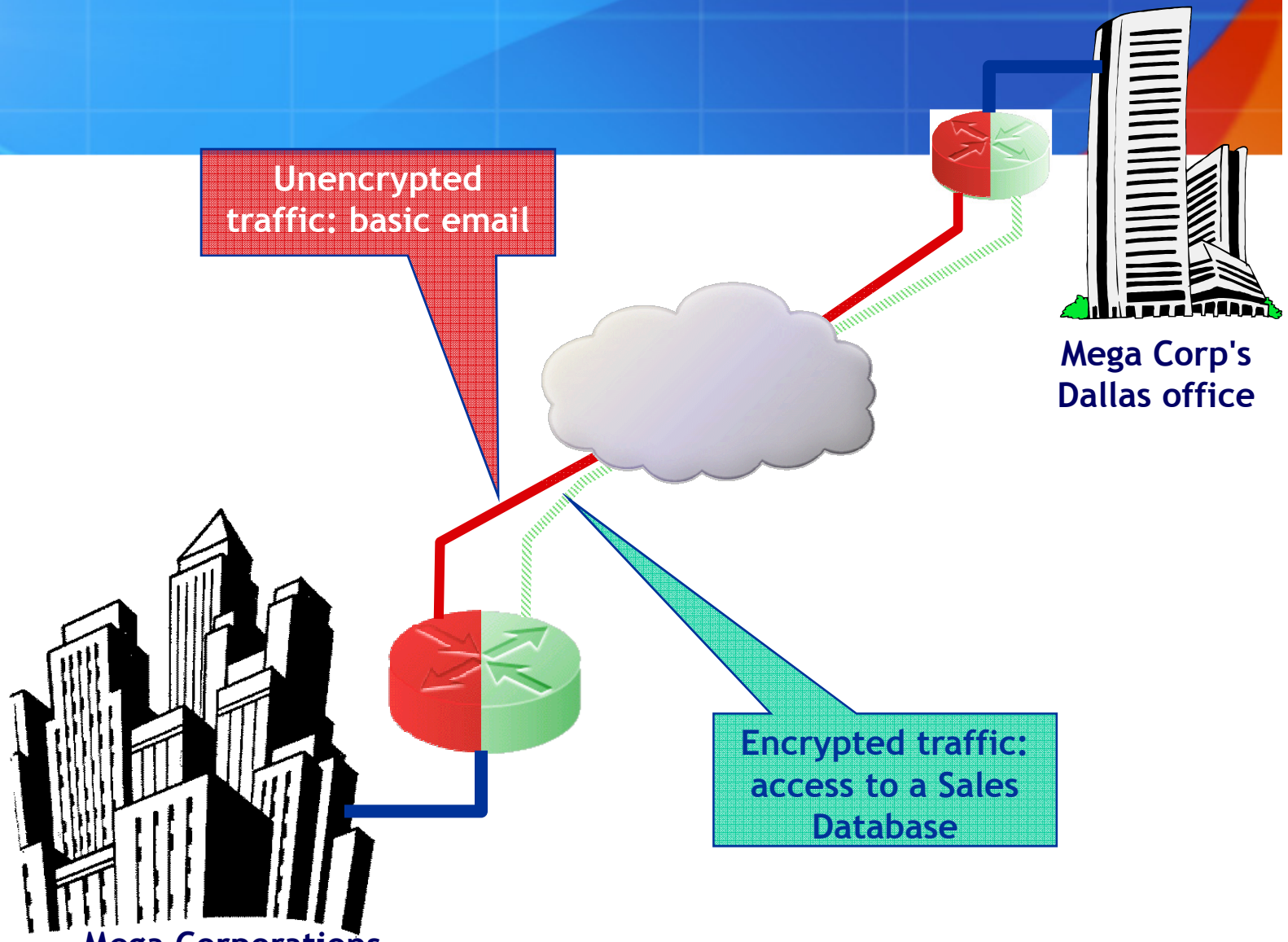


SPIRENT Communications
Inspired Innovation

IPSec at 5000 feet

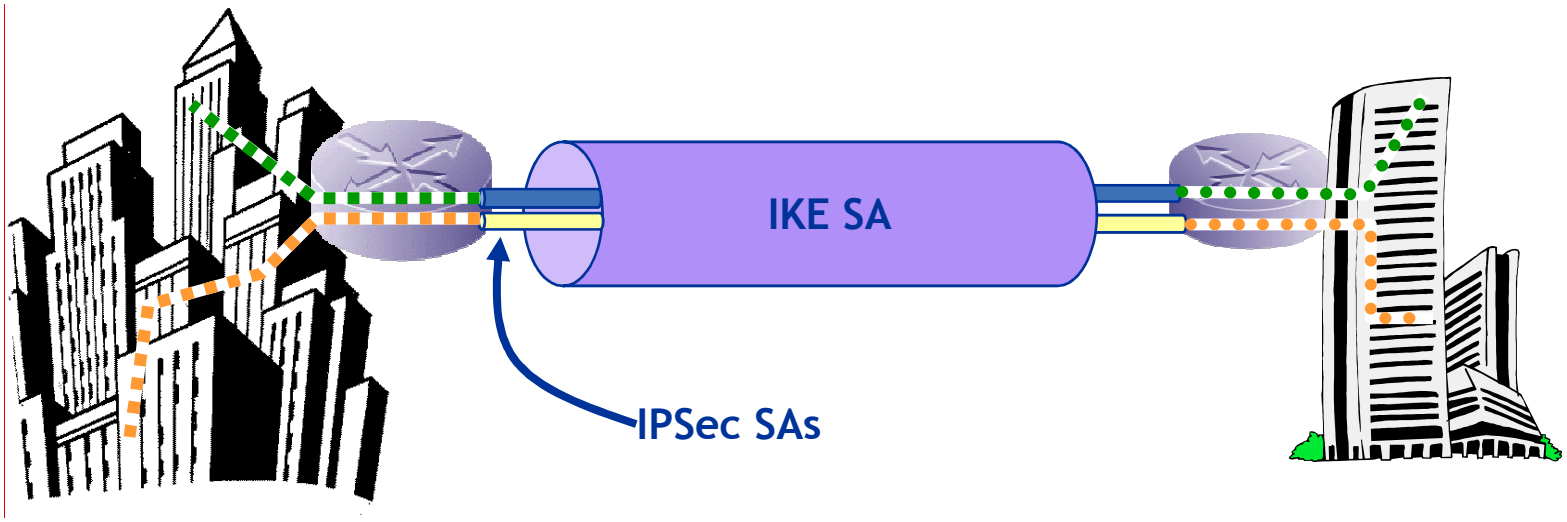


IPSec


Unencrypted traffic: basic email
Mega Corp's Dallas office
Encrypted traffic: access to a Sales Database
Mega Corporations Head Office in San Jose

How did that path (SA) get there?

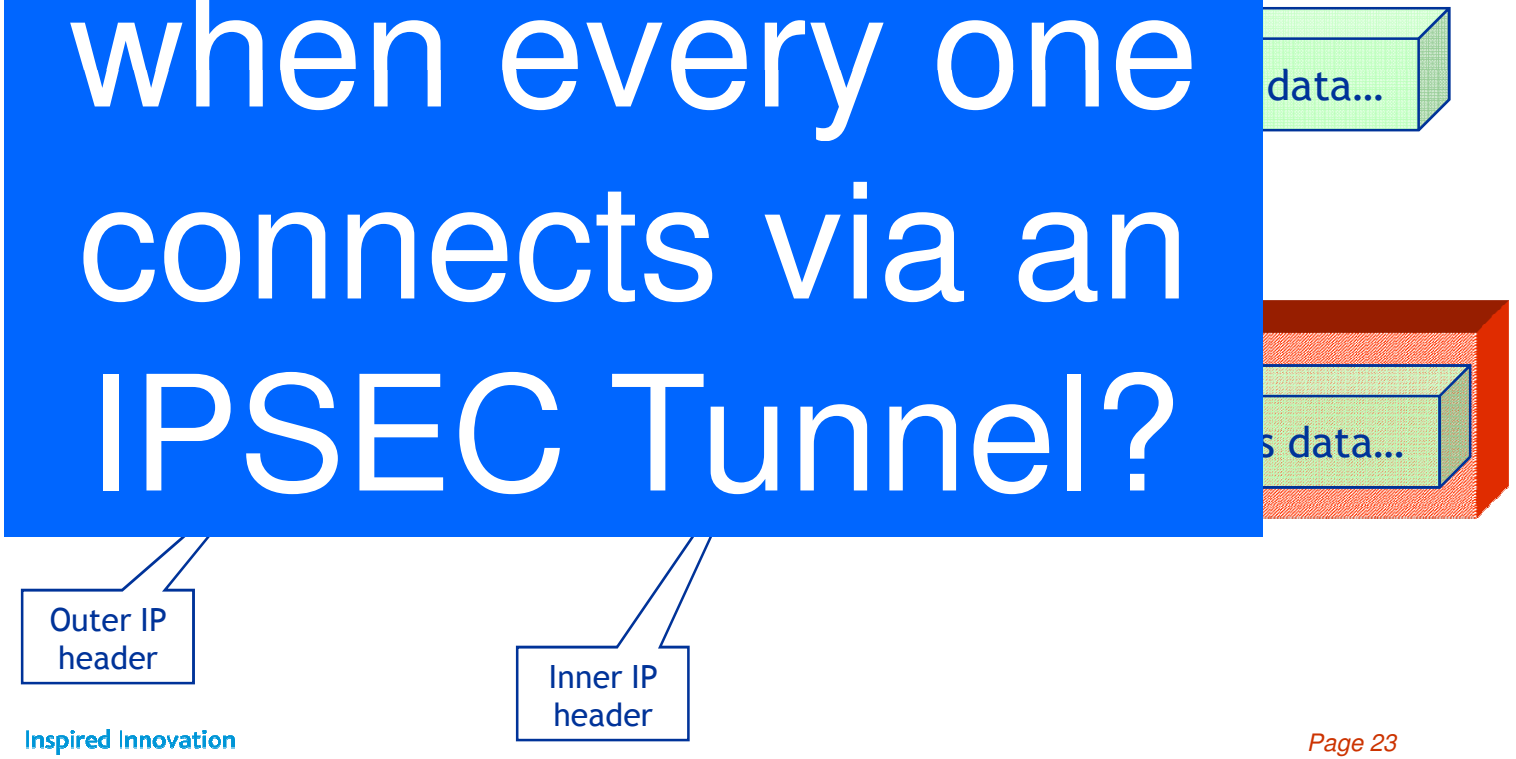
- It had to be created first
- There are two types of SAs:
  - IKE SAs
  - IPSec SAs



IPSec

- **Tunnel** Mode protects the *entire* IP datagram:
  - The communications endpoint is the encrypted inner IP header, and the ter IP

What Happens when every one connects via an IPSEC Tunnel?



Avalanche Security offering

- IPSEC
  - Brir
  - Full
    - ers
  - Cor
    - e
  - Sup
  - Use

Quickly setup 1000 new tunnels per second with full transactions

SPIRENT Communications

Inspired Innovation

Avalanche – Security / Web Apps / Triple Play

Appliance

Spirent TestCenter Hardware

2U

9U

- *Think*… Millions of Internet users and/or application servers in a single box
- Line rate L4-7 testing performance up to 10G
- Load tests Network Security devices and the Application Servers they protect
- Supports all major web applications including, web surfing, email, streaming video, file downloads, VoIP and more

HTTP, HTTPS, SOAP DNS, FTP, STMP, POP3, TELNET, STREAMING Unicast/Multicast, SIP, Capture and Replay, Radius, MM4, IPv4/IPv6 (DHCP,IPSEC/SSL VPN, PPPoE, 802.1x, VLAN), CIFS, RTMP, Video Quality

Avalanche Security offering

- SSL
  - Supports all 3 versions of SSL:
    - SSLv2, SSLv3, TLSv1 – Client and Server
  - Selectable cipher suites independently on Client and Server
    - Enables testing for correct cipher negotiation
  - Support for Unique **Certificates** – Client and Server
    - Loadable Client (User) and Server certificates
    - Loadable Certificate Authority (CA) certificates
    - Loadable Certificate Revocation List (CRL)
  - Support for **Session Id re-use**

*Under Development

Avalanche Security offering

- Integrated Threats
  - Library of 3300+ threats
  - Ability to send threats from the same port as good traffic
  - Single GUI and Hardware for better
  - Testing IDS/IPS appliances or Threat Mitigations
    - Cisco Guard XT (DDoS Guard)
    - Cisco Security Monitoring analysis and Response System (MARS)
- SAPEE – Application Protocol Emulation Environment
  - Advanced Playback engine to emulate complex P2P traffic like Bittorrent, Edonkey, Gnutella etc and other messenger traffic
  - Support for Non-Native Protocols
  - Playback your own protocols and captured traces.
  - Great solution for testing IDS/IPS appliances

Spirent Professional Services

- Spirent Test Services provide customers with test data and expert analysis to make business decisions
- Spirent Professional Services test expertise comes from:
  - Supporting all major network equipment manufacturers and operators with their product and service launches
  - Attending and contributing to industry forums and standards bodies
  - Supporting key industry test activities at Network World and Light Reading

CISCO

Alcatel·Lucent

BROCADE

at&t

中国移动通信 CHINA MOBILE

IEEE

I E T F

NETWORKWORLD®

LIGHT READING

SPIRENT Communications

Inspired Innovation

Spirent Professional Services

Test Services

Equipment Rental
Test equipment rental that is flexible based on technologies, features, number of ports, and timeframe required

Test Engineers
Qualified Test Engineers in Asia to support testing onsite based on technologies and networks being evaluated

Test Planning
Defining test requirements for individual devices, network design, and implementation according to service level requirements today and in the future

Test Reporting
Summarizing results using appropriate illustrations and graphs to show how devices and networks performed against requirements, highlighting any key points

SPIRENT Communications

Inspired Innovation


SPIRENT
Communications
Spirent Avalanche
Inspired Innovation