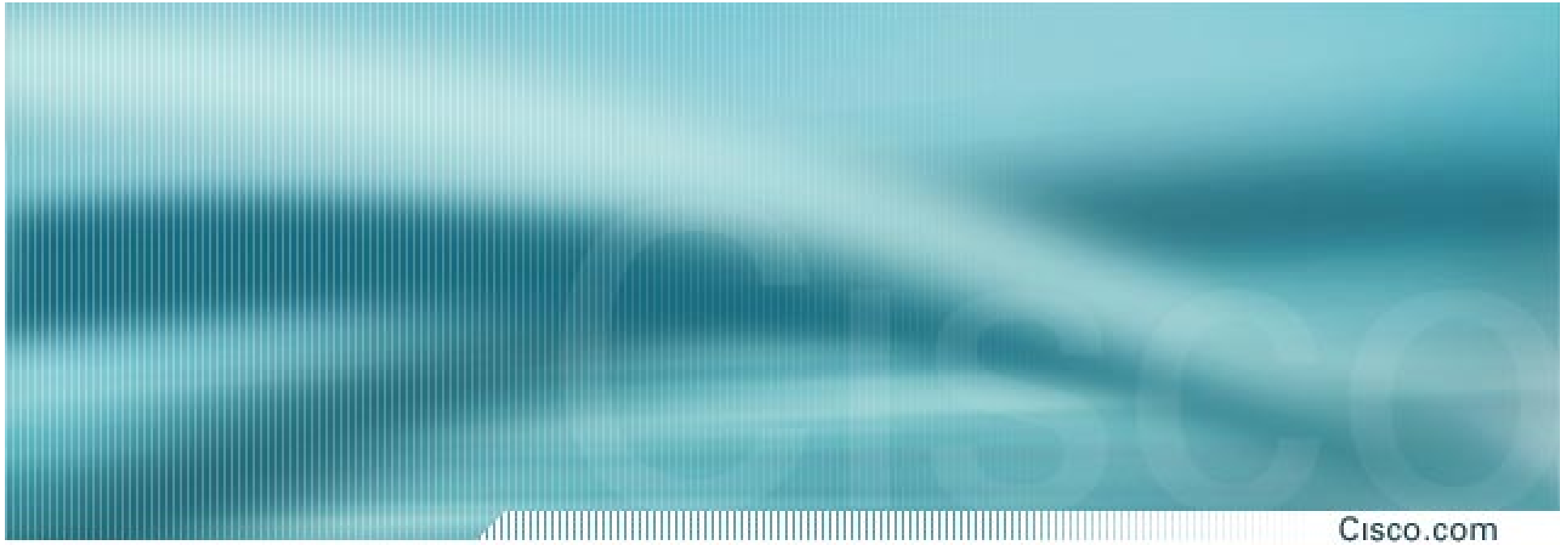


What's Next In Network Security?

A Cisco Perspective

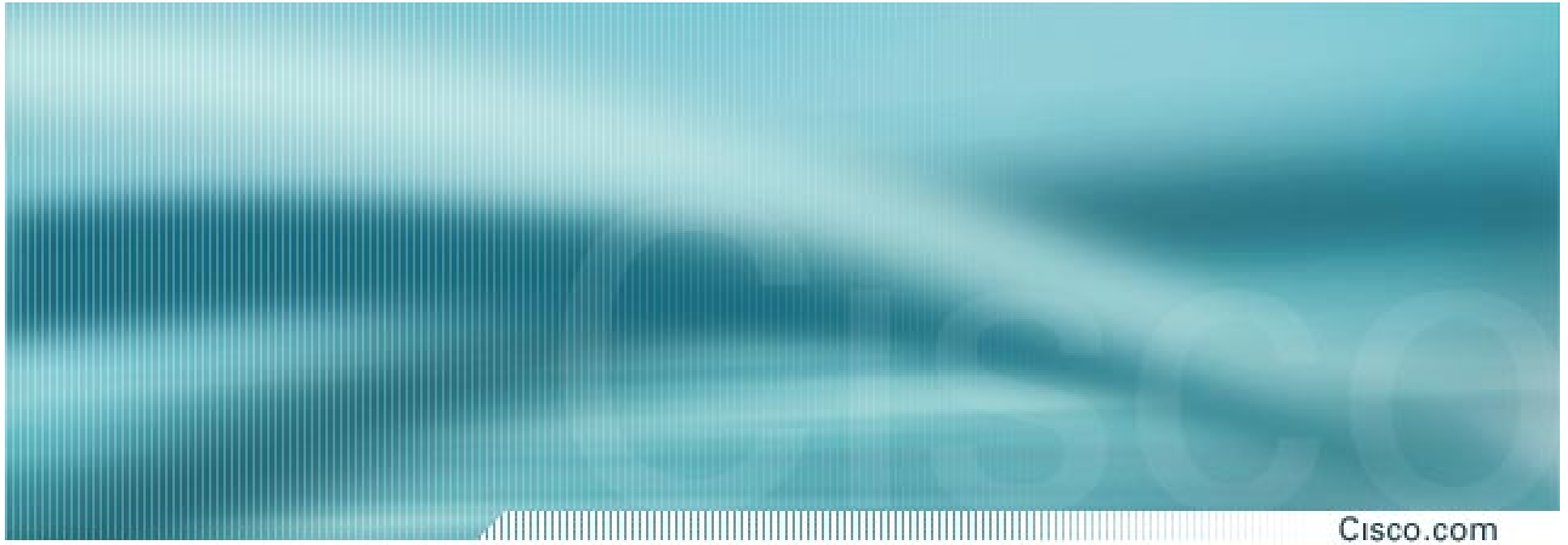
27 June 2002

Bob Gleichauf

CTO, VPN and Security BU

A Shifting Landscape

- Pervasive Security
- Integration and Convergence
- HTTP-Based Services
- The Outer Limits
- Secure Protocols
- Identity and Trust Models



Pervasive Security

Transparent Services

- **Security ultimately needs to become a transparent component of IP networks**
- **Until this happens security will continue to be viewed as more of an impediment than a enabler**

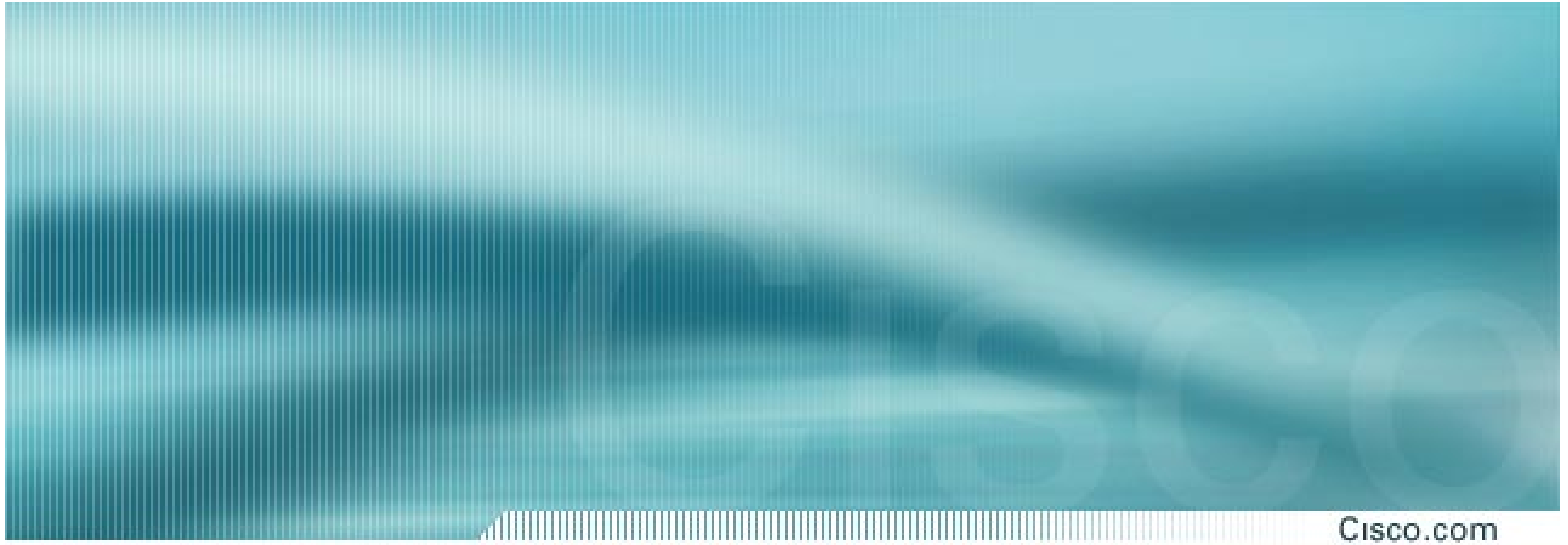
Cisco Is the Network

- **Cisco is uniquely positioned to deliver pervasive, integrated security…**
  - **The incentives are there**
  - **We are a major network infrastructure provider**
  - **We have most of the required pieces**
- **In order to succeed we must:**
  - **Apply a solutions approach to our product-oriented strategy**
  - **Eliminate product-feature redundancy**
  - **Establish minimal security standards and features across platforms**
  - **Lower the cost of ownership**
  - **Make security an integral part of our culture and processes**

Cisco Systems Security Council (CSSC)

- Sponsored by Mario Mazzola, CDO
- The CSSC is a corporate resource for security:
  - Baselines
  - Best practices
  - New technologies and markets
- Mission statement

  To help identify, prioritize, and define strategic security initiatives that will have a positive impact on our products and services, on our customers, on our partnerships, and on the Internet as a whole.



Integration and Convergence

Integration and Convergence

- Consolidation of security services is happening all around us

  FW + VPN + IDS…

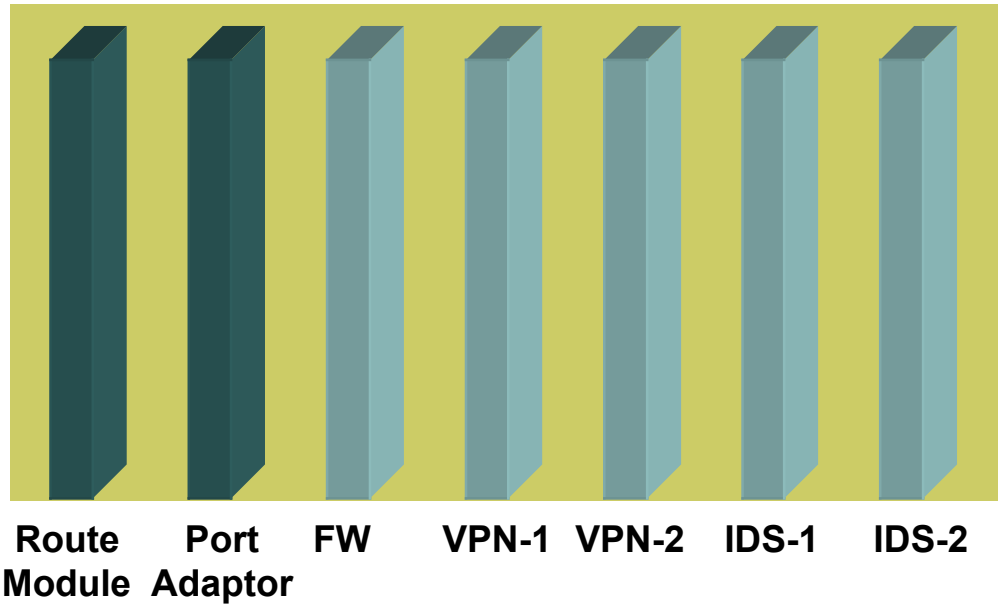
- This convergence is driven primarily by Cost of Ownership…
  it is also an early sign of the migration of security services into the network infrastructure
- The problem is that this approach is typically based on fixed configurations that do not scale
- This approach currently makes the most sense at the low end

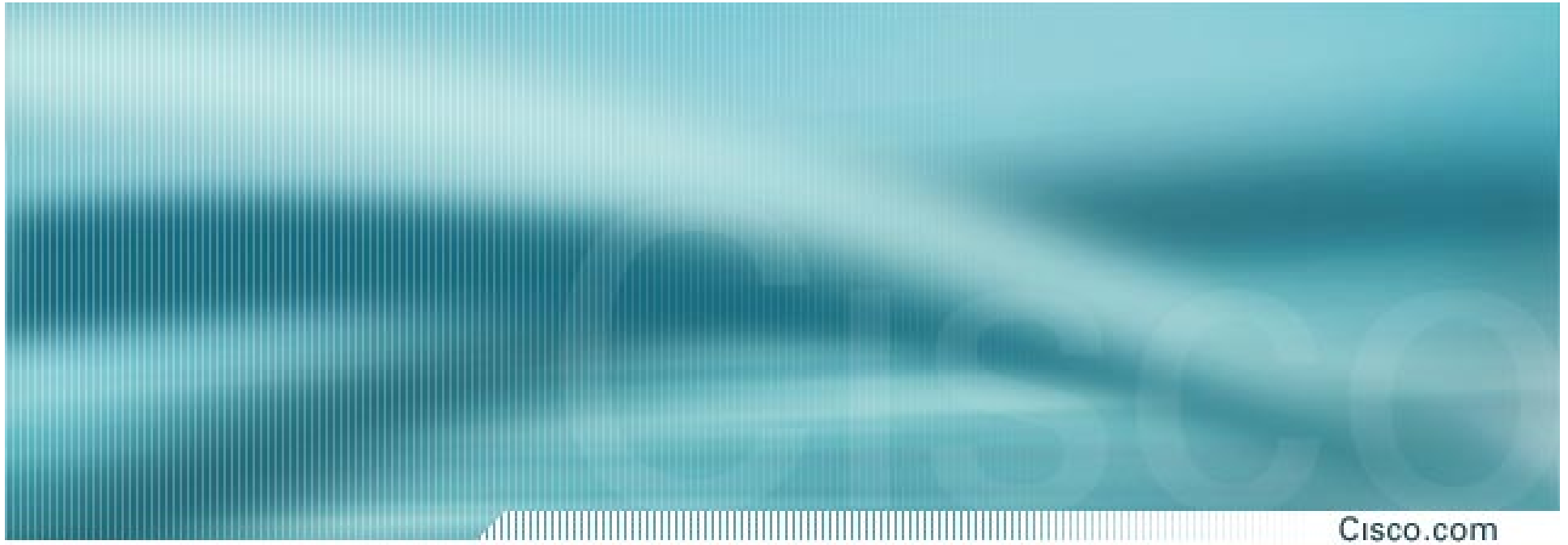
A Better Approach at the High End

- Cisco's router and switch platforms make a great platform for delivery of (security) services that are:

  Modular **Scaleable** **Redundant**

- It creates an ecosystem that customers can reconfigure as their requirements change





HTTP-Based Services

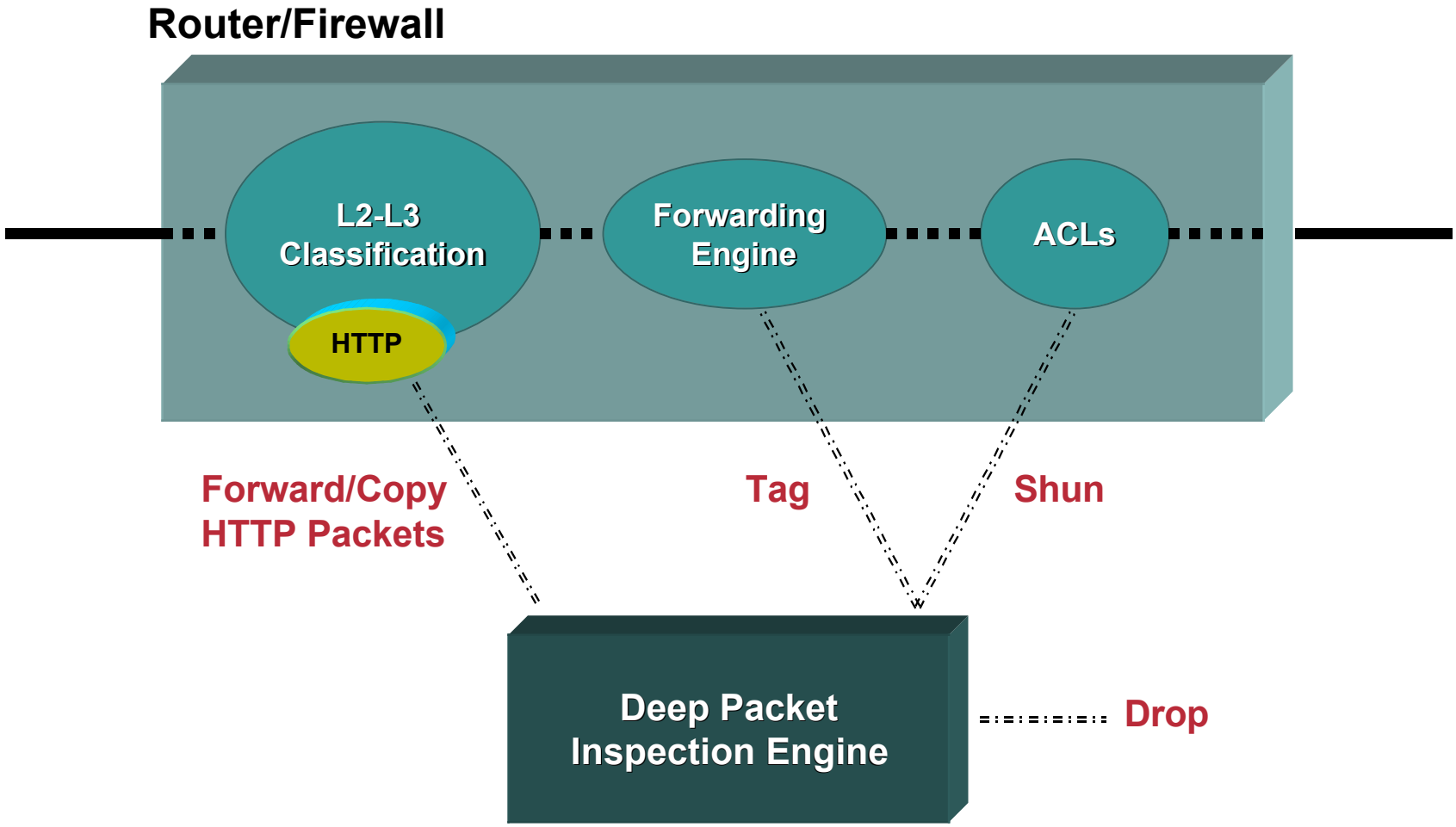
The Port 80 Problem

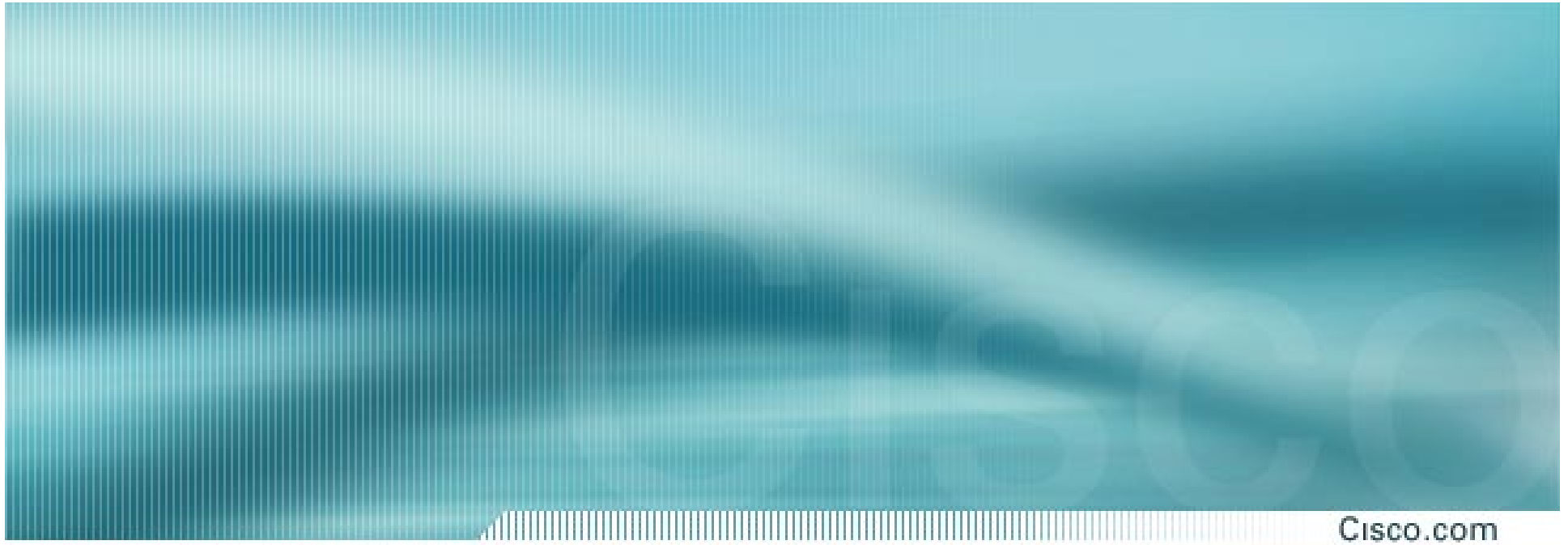
- More and more companies are adopting B-2-B and B-2-C applications that use HTTP as a transport to tunnel through firewalls
- This trend challenges the value proposition of Cisco's edge devices (FW, IDS, Load Balancing, Caching, etc)
- Cisco does not want to become a dumb pipe company
- Two options:

  Develop high-speed Deep Packet Inspection Engines (DPIEs)

  Architecturally decouple Packet Inspection (PI) from Policy Enforcement (PE)

Helper DPIEs





The Outer Limits

The Outer Limits

- Systems are only as secure as their weakest link, which is frequently at the endpoints (the Outer Limits) of the network
- This becomes even more of an issue as (HTTP-based) applications migrate to port 443 (SSL).
- Cisco has traditionally shied away from the outer limits of the network because of…

  Lousy margins

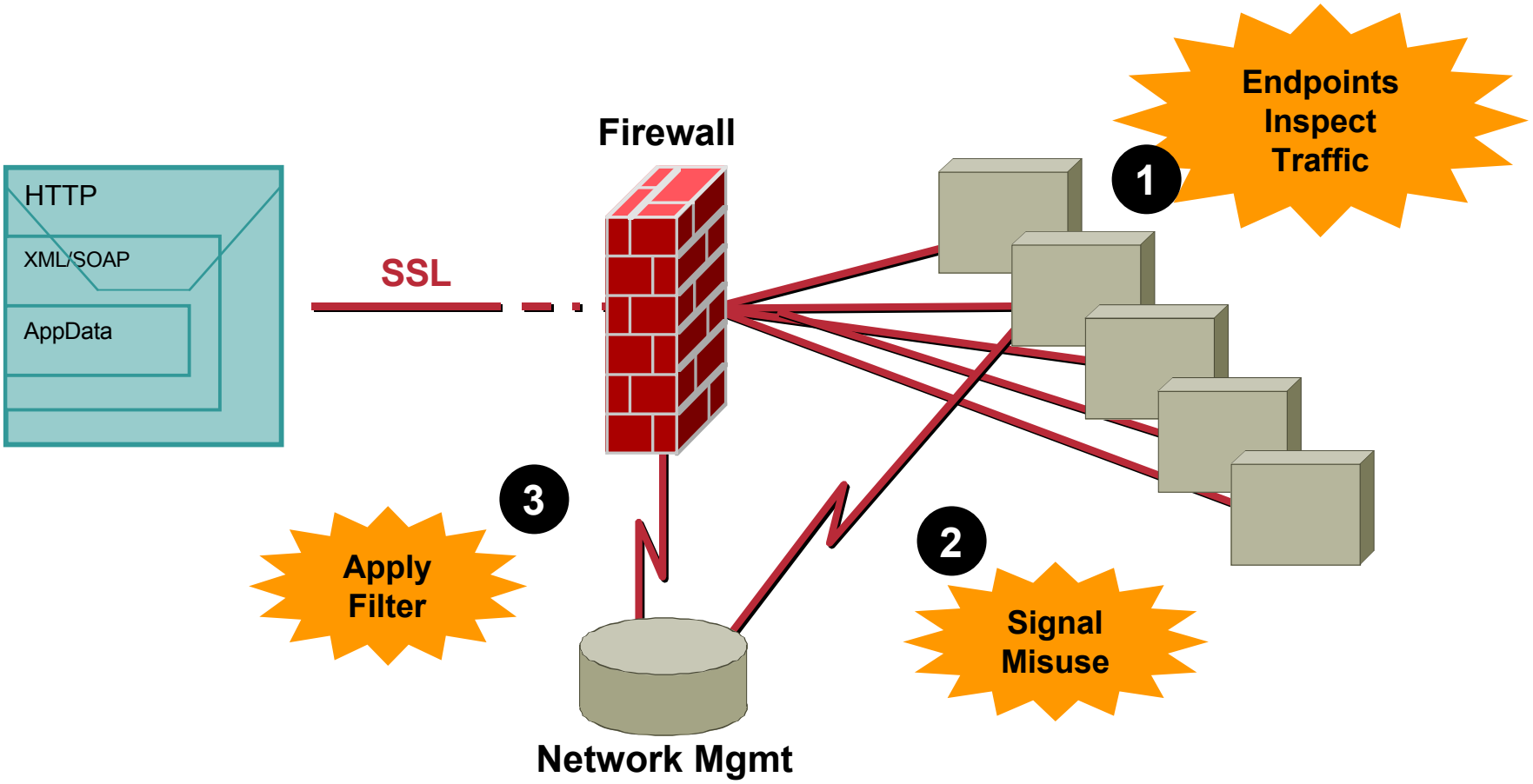
  Higher touch software distribution model

  Microsoft

- When will Cisco play at the Outer Limits?

  1. When it enhances or sustains what we do within the network
  2. Where is keeps us from becoming a “dumb pipe” company

Endpoint Security



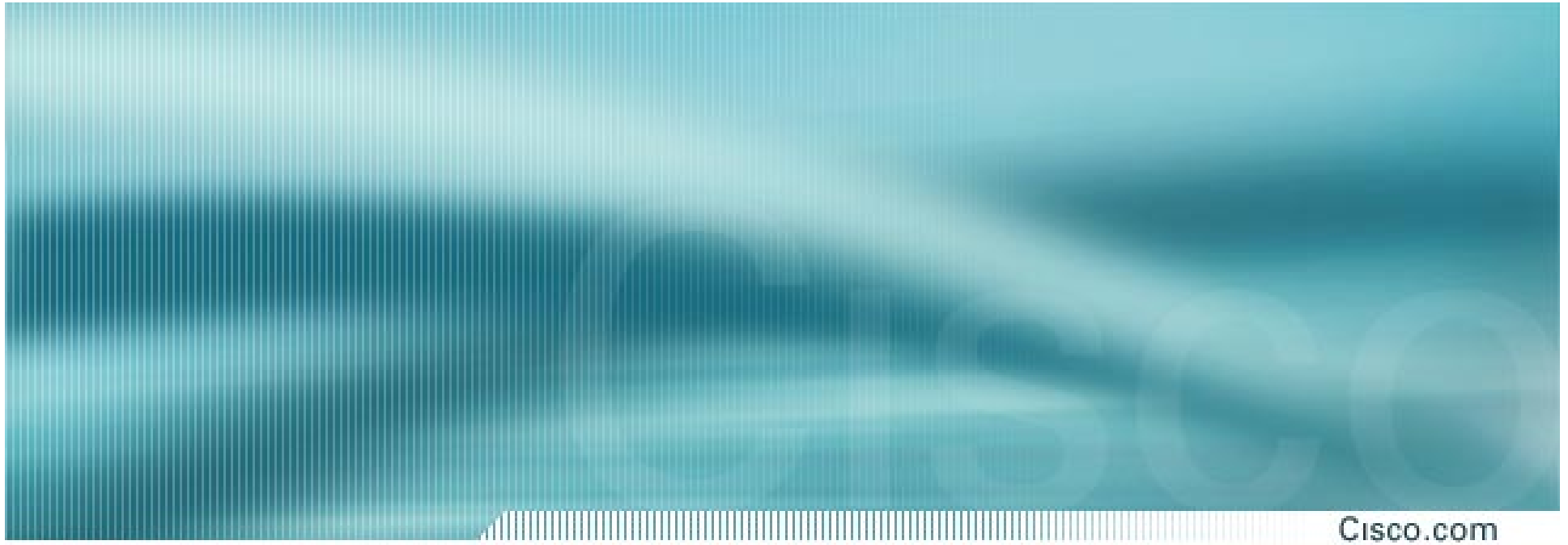
Cisco Strategy

- **Cisco will leverage the value proposition of endpoint security application through a combination of communication protocols and relationships**
- **Examples include:**
  - **Entercept HIDS**
  - **ZoneLabs System Integrity**

Beware of SSL? Edge versus End

- Web Services is the hot new thing…
- But the recent growth in end-to-end SSL communications does not necessarily mean that network edge applications are a thing of the past
- End-to-end tunnels can be conduits for misuse

  While SSL-based Web services are great for the business units that want to bring solutions quickly to market, it is in conflict with the goals of IT folks who want visibility into the wire and the ability to enforce policy
- This is why Cisco's architectures will allow for the decoupling of Packet Inspection from Policy Enforcement



Secure Protocols

Secure Protocols

- Cisco is committed to helping improve the resiliency and robustness of IP and Internet protocols
  - Gateway protocol trust models
  - Out-of-band management
  - Denial of service

Gateway Protocol Trust Models

- Built around the concept of identity
- Which in turn depends upon reliable mechanisms for the distribution and maintenance of keys
- There is also the matter of inferred trust of your neighbor's neighbor
- There are no quick fixes for this problem… it is an area of ongoing research

Out-Of-Band Management

- Creating separate control plane networks to increase core network resiliency is not a panacea
- It actually adds complexity, which in turn introduces more points of vulnerability and higher cost of ownership
- OOB networks also do not solve the fundamental key management and trust problems, they simply move the problem
- While OOB does make sense for some key network segments with smaller zones of trust…
- Alternate routes and in-band IPSec tunnels are Cisco's preferred solution

Denial of Service

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) are one of the more difficult problems to deal with**
  - **Trojans and zombies**
  - **Timing (bursts and lags)**
  - **Absence of Identity**
- **Near-term solutions**
  - **Reconfiguration of queue depths**
  - **Redundant network configurations**
  - **Data Sharing among ISPs**
- **Longer-term solutions**
  - **Emergence of second-order correlation tools that can deduce patterns from network statistics such as NetFlow and BGP**
  - **Comprehensive identity infrastructures**

Identity and Trust Models

Identity and Trust Models

- The absence of a pervasive identity infrastructure(s) is one of the biggest impediments to wider adoption of security and network technologies
- Are user identities enough, or do we need nonrepudiation at Layers 1 (hardware) and 3/4 (application) as well as Layer 7?
- This is presently an area of research and innovation that is being driven by applications such as wireless, VoIP, and Web services