

Apani

Enter the Matrix:

A Look At Next Generation Security Architectures





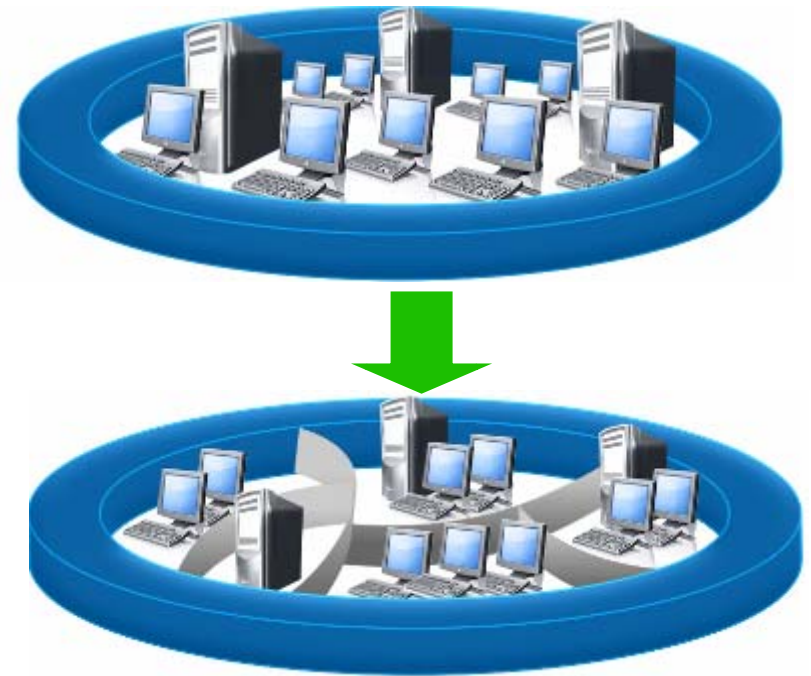
- **The perimeter is no longer viable as the basic design for security**
- **Security must be expanded to inside the perimeter**

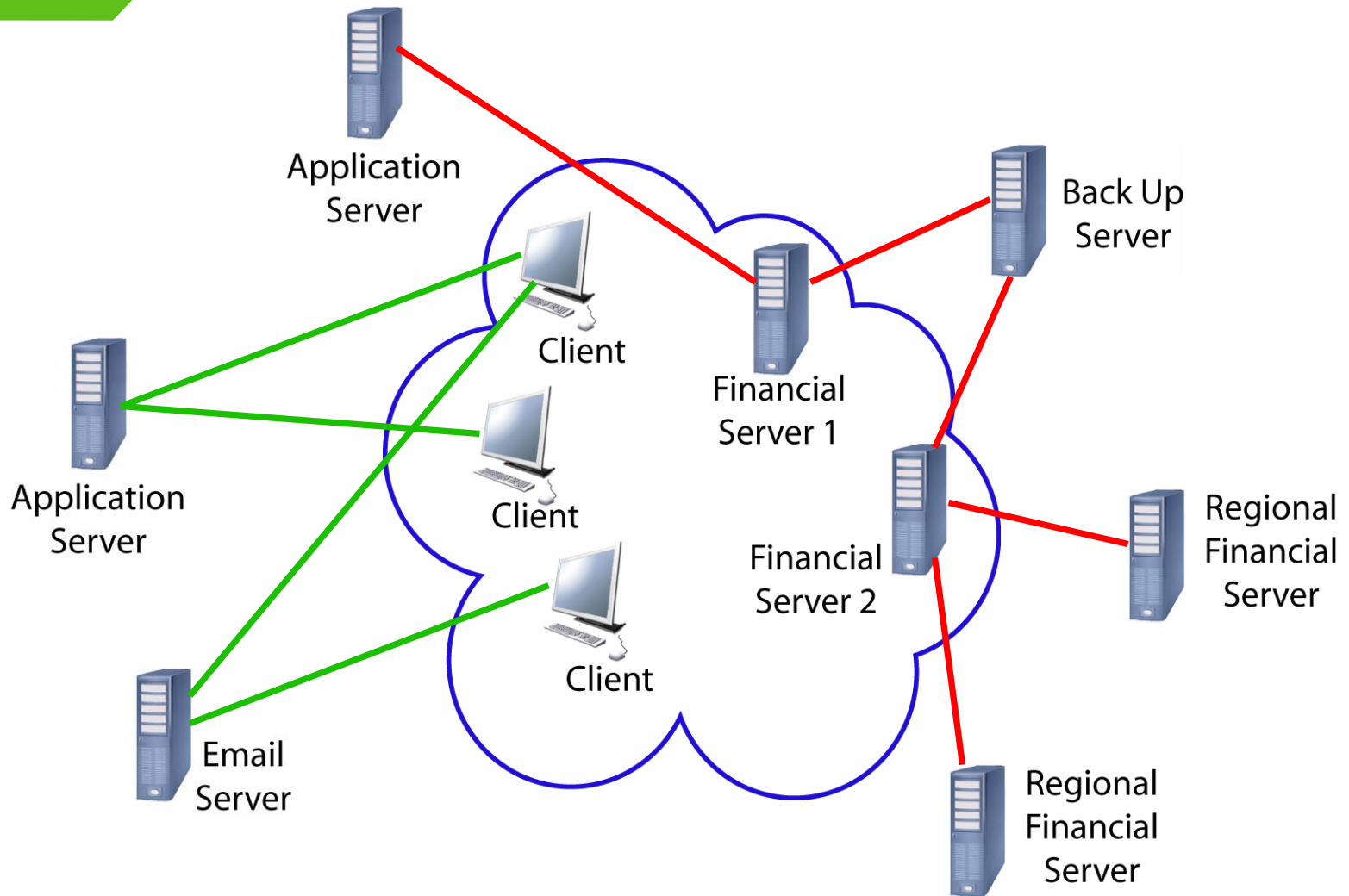


- **TCP / IP was designed as “default allow”**
- **Point to point traffic**
 - Gateways = bottlenecks
- **Scope**
 - Large # of applications
 - Legacy systems
 - Multi-vendor environment
 - Large # of protocols
- **Management**
 - Large number of policies (n^{n-1})



- **The first step to protect against D-P is segmentation ...**

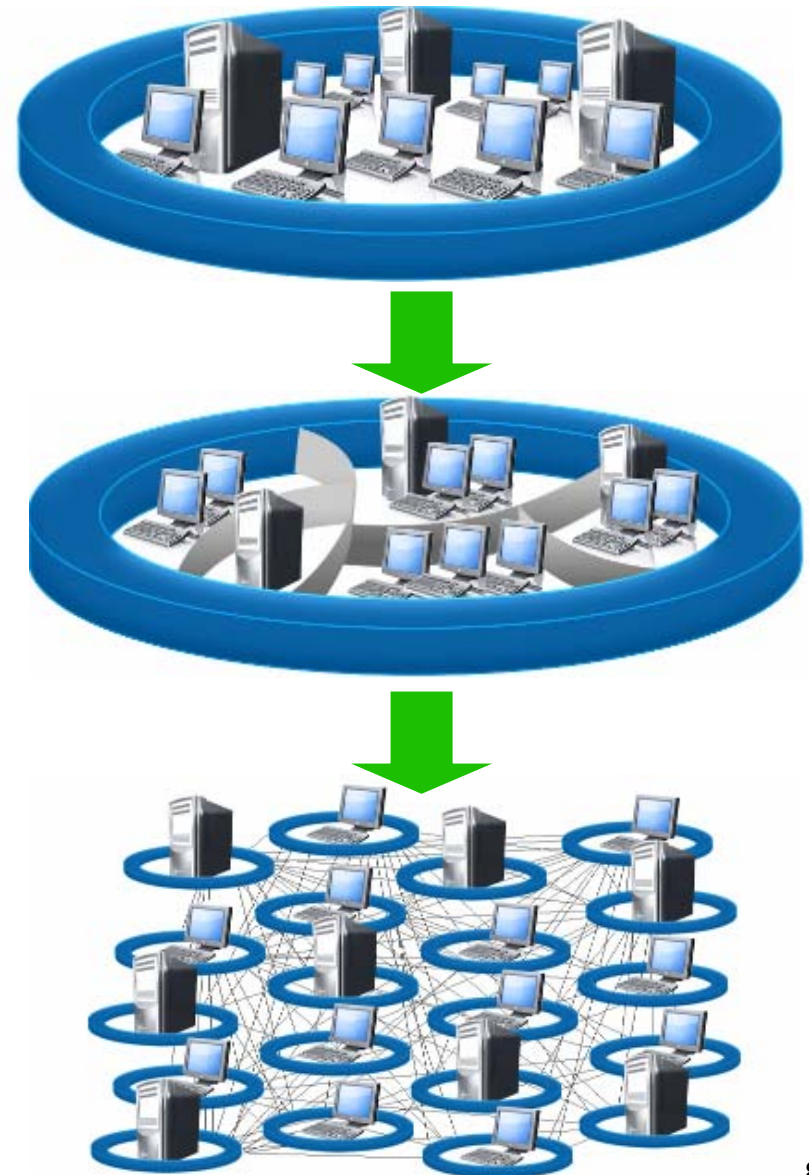




- Adds barriers
- Reduces the scope
- Contains risk
- But, really more of a networking strategy than a security one
 - Tough to manage
 - No security within the segment
 - Can impose rigidity to the network

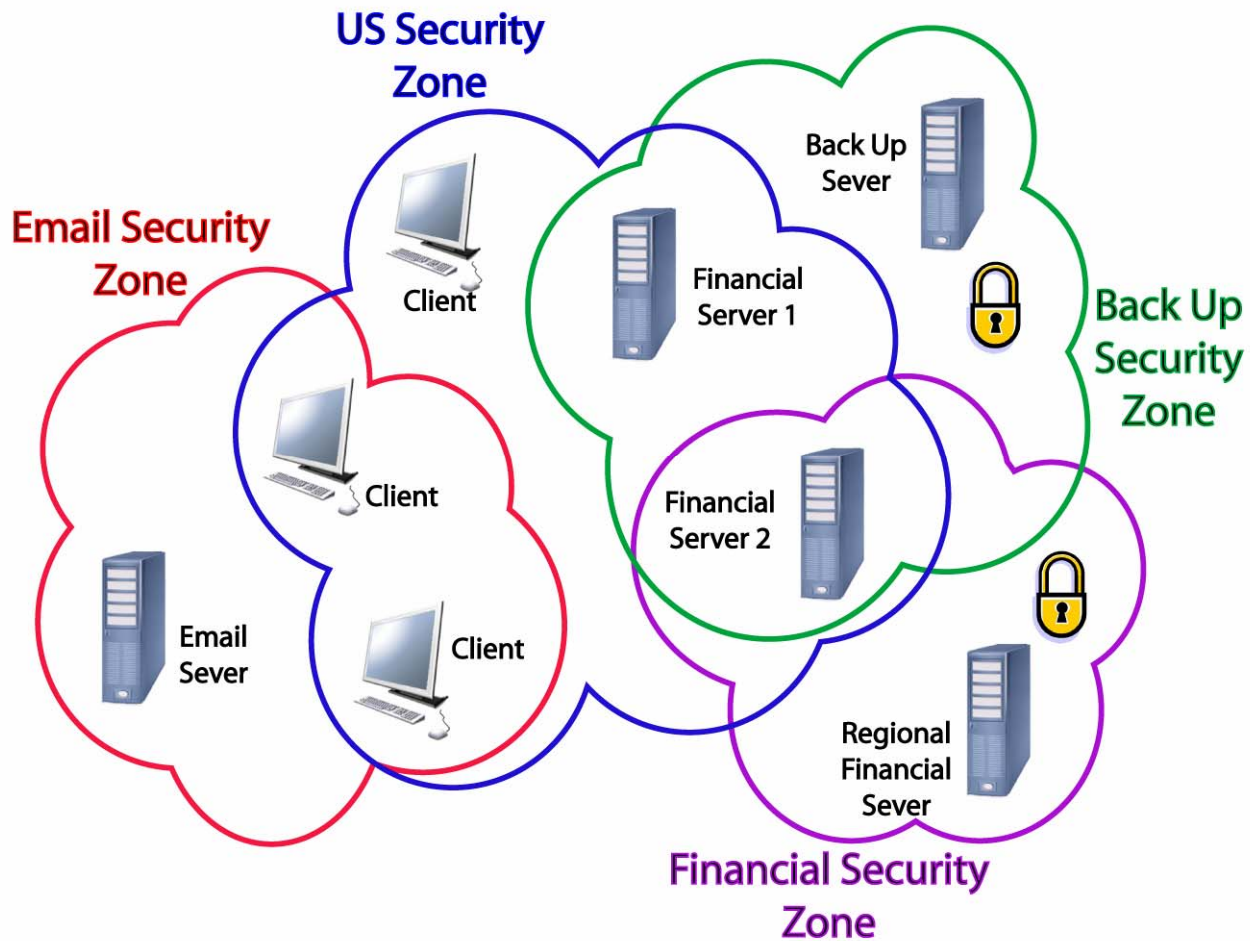


- **Segmentation is a first step, not the total solution**
- **Conceptually, need to move to a “perimeter of one” or matrix**



- **Controls “point-to-point”**
 - Host based control provides access control / authorization
- **Embeds security**
 - Can include strong authentication, authorization and point to point encryption.
- **But...**
 - Wide variety of host operating systems
 - Exponential numbers of policies $n^{(n-1)}$
 - How do you provision and manage it?







Manage, secure and control point-to-point traffic

- Host-based access control enables secure, end-to-end connectivity

Embed security elements to secure inside segments

- Strong authentication & authorization limit access to sensitive data

Management Challenges Solved

- The “n” in $(n^{(n-1)})$ becomes the number of segments, not systems
- Closed user communities simplify management & audit

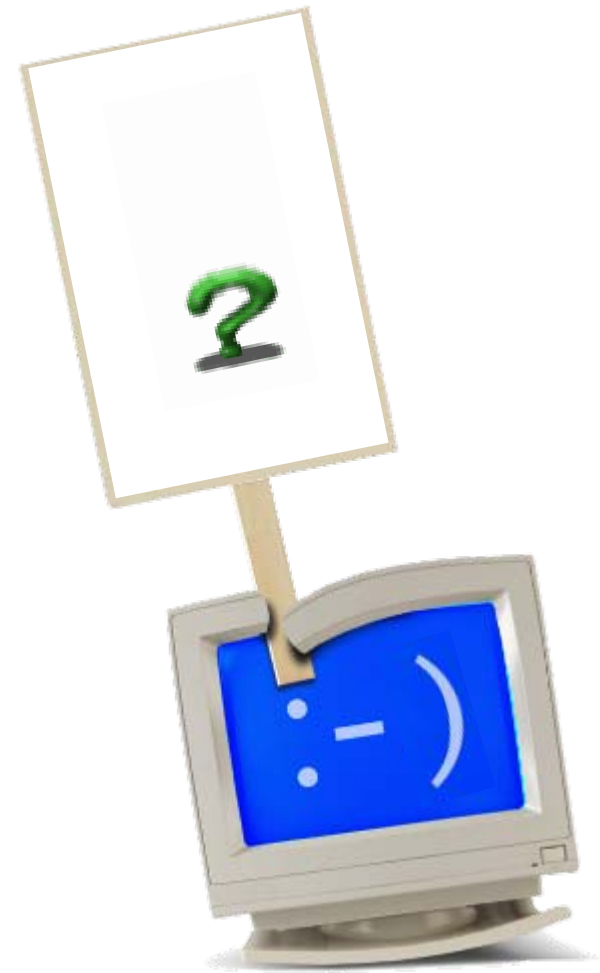
- **De-perimeterization is here to stay**
 - Can't exclusively rely on the perimeter for gateways or 'choke-points
- **An updated security architecture is needed to secure both at and within the perimeter**
- **Best design includes the following elements:**
 - Segmentation
 - Host-based control
 - Built in security elements
 - Centralized management
 - Highly scalable, automated with multi-vendor support
- **This architecture is now available, solving the enterprise data protection issues you are currently facing, and preparing you for those of tomorrow**

Apani

Questions?

Contact Information:

Mike Kuch
mkuch@apani.com
+1 (714) 674-1600



- **Apani provides information security for regulated industries**
 - **Apani EpiForce provides enterprise data protection inside the network perimeter**
 - **International, Fortune 500 client base**
 - **Partnerships with HP and other major system integrators**
 - **Hughes Electronics spin-off, NSA Project**



- **EpiForce enables you to:**
 - **Meet compliance requirements for SOX, GLBA, FDA 21 CFR Part 11, PCI, HIPPA & Basil II**
 - **Secure and control access to financial systems**
 - **Minimize internal and external audit exposure**
 - **Maintain accuracy of reported data and reduce fraud**
 - **Restrict unauthorized access to sensitive data**
 - **Avoid negative media coverage, loss of customers and brand degradation**