



Rethinking Security Architecture in Light of De-perimeterization

Dan Blum
Senior VP, Principal Analyst
dblum@burtongroup.com

Presented for Jericho Forum
9/11/07

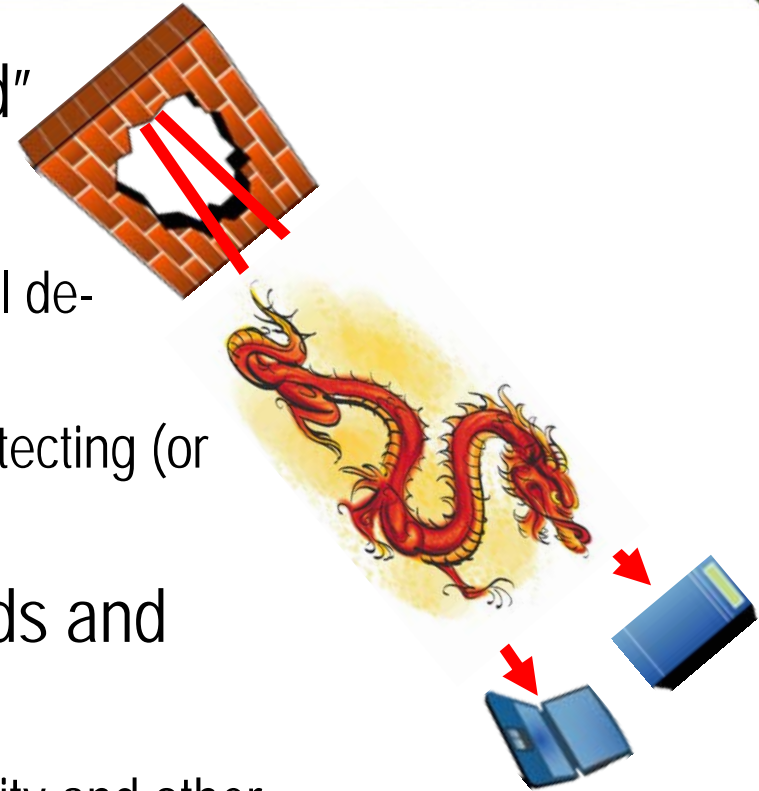


Rethinking Security Architecture

De-perimeterization implications

- Not an all or nothing proposition
- Perimeter controls will always be needed in certain areas
- Enterprise security architecture must change to shift many controls from the network to the endpoints, data centers, information repositories and applications
- Clear issues, architecture targets and challenges are coming up over the next 2-3 years

- The single firewall model is “busted”
- Order of the day
 - “Re-perimeterization followed by eventual de-perimeterization”
 - Loads of vendor appliances offerings protecting (or clogging?) the network
- Gaps in endpoint security, standards and tools for more granular security
 - Projects leveraging NAC, federated identity and other new technologies still at the early, tactical stage
- While de-perimeterization brings a major issue into the open



What's the network's role in security?



Oposing Viewpoints

- Network Perimeter Model
 - Router ACLs, VLANs, firewalls, IDS/IPS, proxy servers, security zones, DMZs, etc.
 - Relies primarily on the network for security policy enforcement
- Overlay Model
 - VPN encrypted tunnels to servers in data centers
 - Relies primarily on endpoints for security policy enforcement





What's the Network's Role in Security?

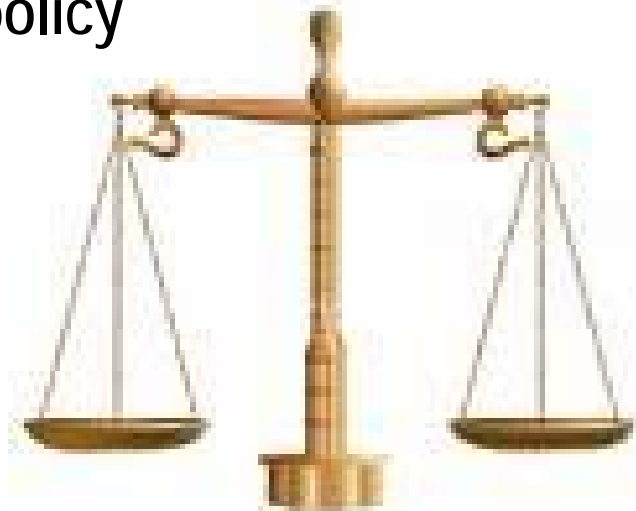
Tradeoffs

Overlay
Model

Pushing security to endpoints requires client agents, centralized policy admin, and access gateway systems

Network
Perimeter Model

Pushing security intelligence into the network creates operational and administrative challenges





Architecture Vision



Assumptions

- Laptops and mobility are increasing
- Most endpoints already equipped with security software to survive on the open network
- Network perimeter
 - Needed as first line of defense against DoS and some external attacks
 - Not very effective against attacks on applications
- The closer the “intelligence” making security decisions is to the target
 - The better the granularity
 - The more likely policies will be maintained correctly
- Data center consolidation is increasing



Architecture Vision

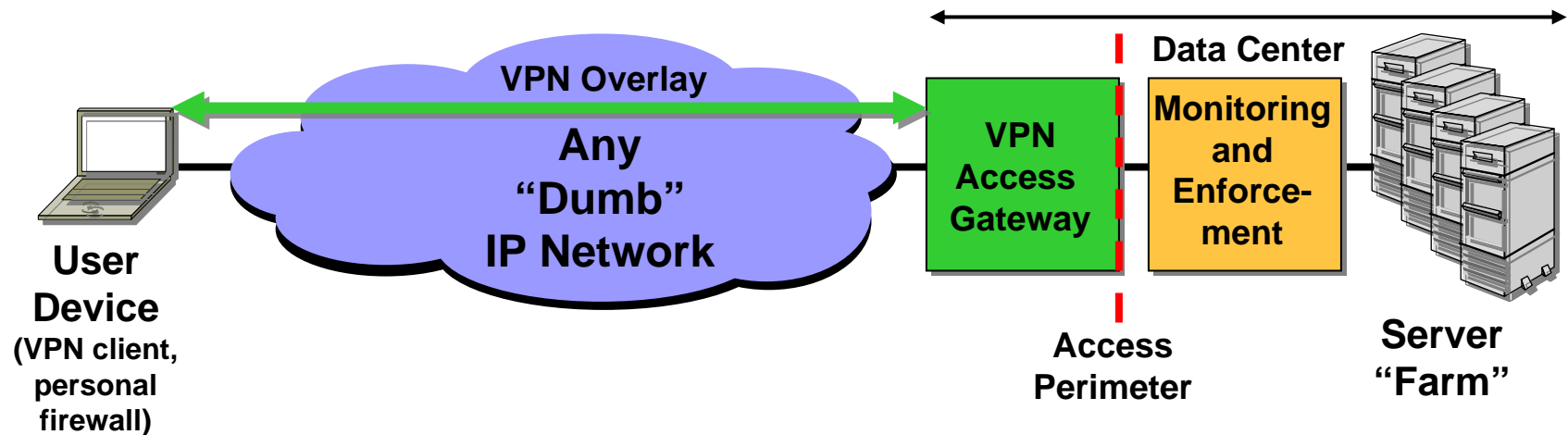


- *The **overlay model** is used for most client devices all the time. Great flexibility comes when devices and users can roam anywhere in relative safety. Visitors can enter and leave sites, retain network access, and pose relatively little danger to one another.*



Increase emphasis on the overlay model

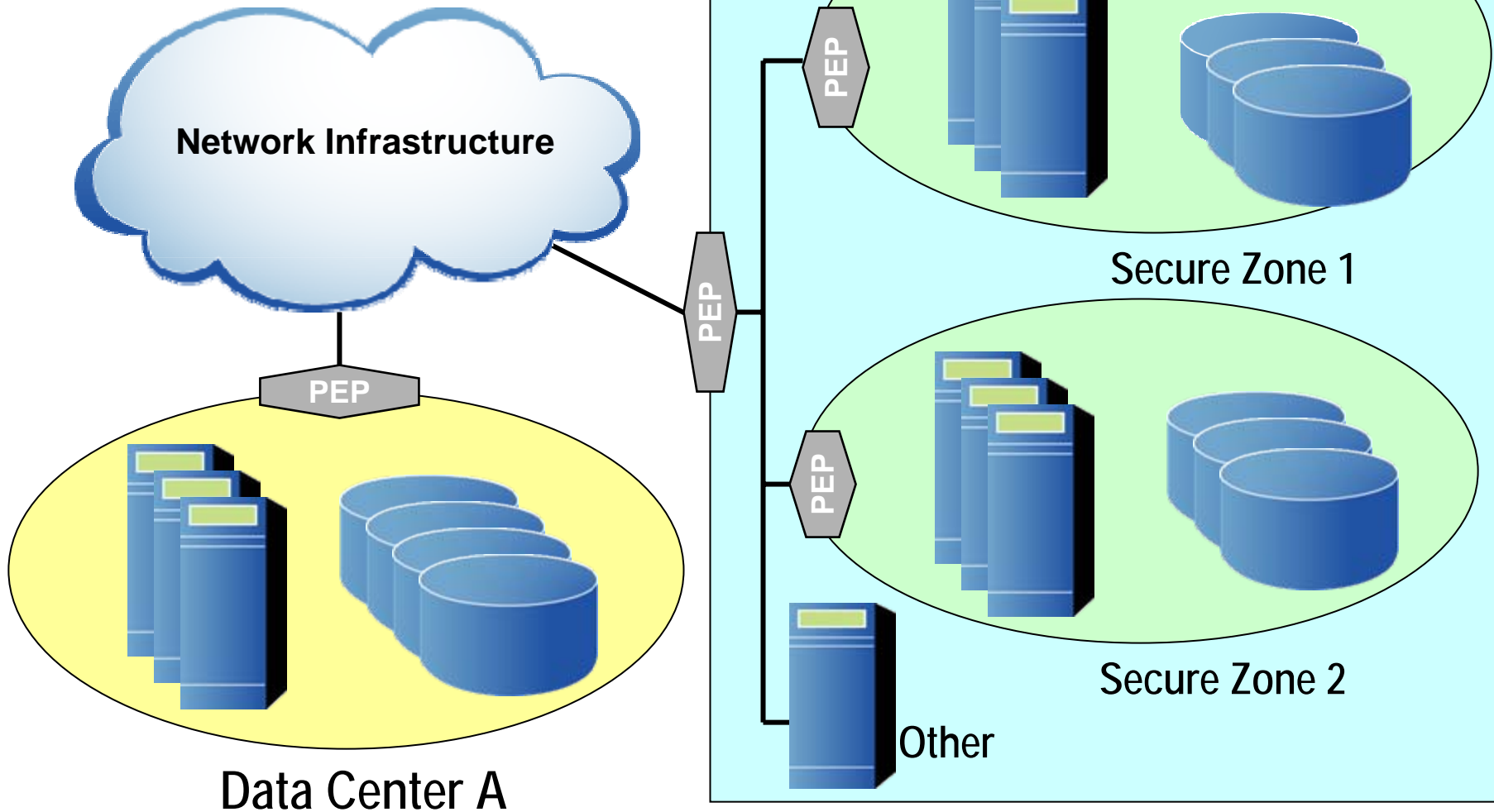
- Secure protocols protect communication
- Overlays used all the time – onsite, offsite, WIFI





- *The **perimeter model** will be used where it has the most leverage: Far out against the attacker, and close in to the applications. Data centers will rely on perimeters for protection. Data centers can provide service - both to external subjects and to insiders - with flexibility in relative safety.*

Aggregate IT assets into
secure zones





Policy enforcement at the data center boundary

- Enforcement mechanism must be
 - In the traffic stream
 - Aware of the user's identity and role
 - Able to restrict which users are permitted to access specific systems within the secure zone
 - Terminate and perhaps cascade secure tunnels
 - Optionally inspect content to filter for malware and enforce restrictions on information flows
- Examples of enforcement mechanisms
 - Access gateway – typically a VPN gateway with advanced access control features
 - Identity- and application-aware firewalls
 - Terminal server with application access control features

- VPN products designed for remote access, don't scale (yet) to 10's of thousands of users
- Endpoint security is weak
 - Unmanaged endpoints cannot be trusted
 - Managed endpoints at best only moderately secure
- We're not winning the race against malware
- Defense in depth tends to fail when information policies aren't well defined, enforced



UAC not a security boundary?!

<i>DRM Scoreboard</i>	
<i>1000</i>	<i>?</i>
<i>Hackers</i>	<i>Industry</i>

Data center boundary is not your father's perimeter - must take care of multiple functions at very high speeds

- Security filtering
- Tunnel termination
- Local / global load balancing
- WAN optimization
- Caching



As perimeter functions get mixed with switching and other functions, assurance may degrade

- Application front end networks
- Endpoint security in silicon
- Network access or admission control (NAC)
- Virtual desktops and sandboxes
- Improved identity assurance
- Federation
- Web services / SOA security





Recommendations

Assume that both perimeter and overlay models will be needed in many cases and must co-exist

Work towards securing endpoints

Set up new boundaries and control points at the data center edge

Segregate critical systems into secure subzones within larger data centers

Focus on policy, accountability and awareness – its not just a technology problem!

- *Security and Risk Management Strategies* overview “Architecture Inflection Point: Securing Networks without Borders”
- *Network and Telecom Strategies* overview “Security Architectures: What’s the Network’s Role?”
- *Security and Risk Management Strategies* overview “Architectural Alternatives for Enforcing Network Admission Requirements”
- *Identity and Privacy Strategies* report “Network Identity and the Enterprise Identity Infrastructure”
- *Security and Risk Management Strategies* report “Enterprise Firewalls and Perimeter Architecture”
- Reference Architecture Technical Positions, covering:
 - Perimeters and Zones
 - Remote Access
 - Encryption