

The Business Ramifications of the IPv6 Security Model

French IPv6 Summit

Cannes, France

November 14 – 15, 2006

Presented by Yurie Rich

Who is Command Information?

- IPv6 Professional Services firm
- Helps large organizations leverage new capabilities of IPv6
- Provide business solutions related to:
 - IPv6 Integration & Education
 - Application Development
 - Systems Integration
 - Technology Research & Development
 - DoD/Federal IPv6 Technology Adoption
- 350 people and \$50M USD in annual sales

IT Security in a nutshell

Basic Security Axiom

“Protection is required by every device that is participating in networked communication and all information that is either stored on a device or is in transit between communicating devices or is processed by the devices.”

Basic Security Framework

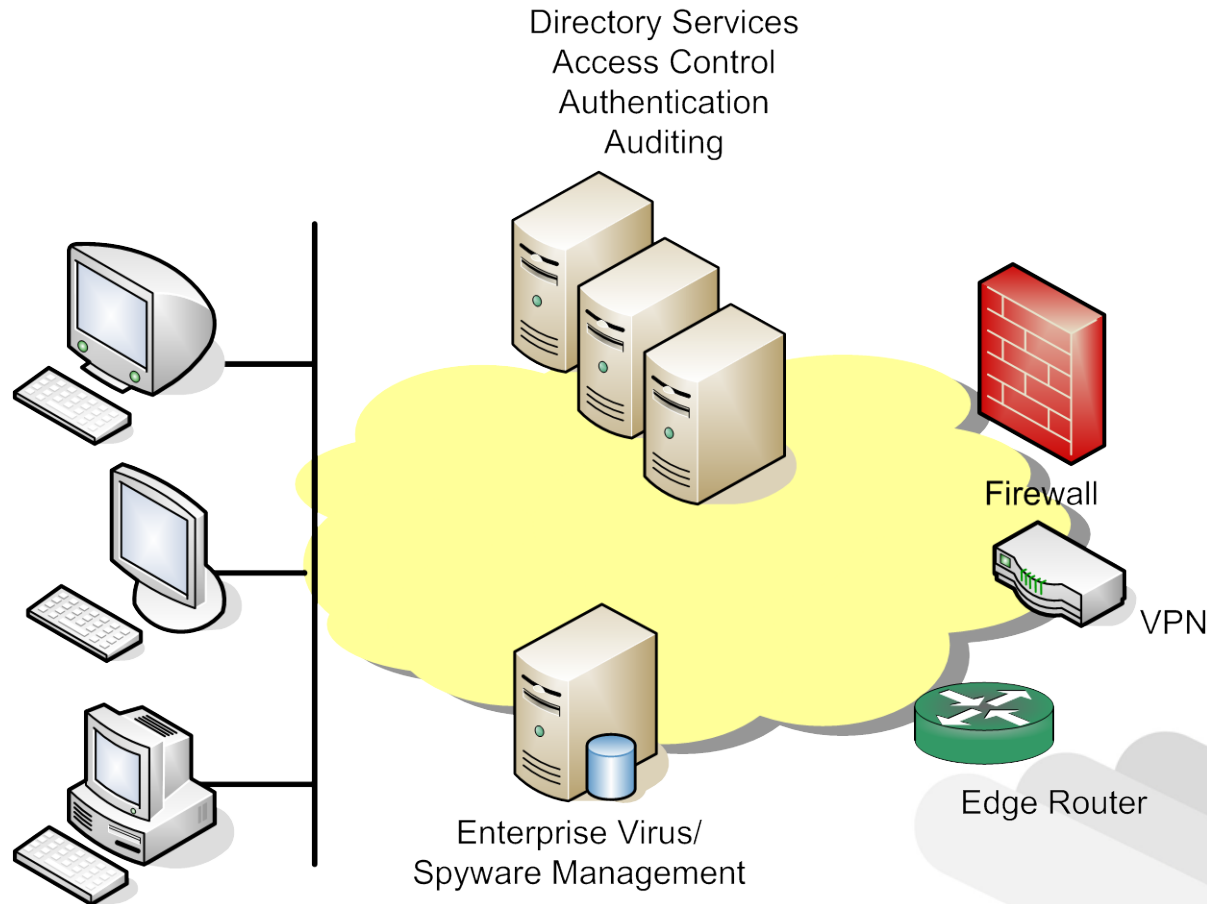
“A combination of application, host and network-based security is required to securely conduct business on the network of networks which makes up the Internet”

-Merike Kaeo, NAv6TF Whitepaper, IPv6 Network Security Architecture

Realities of ROI and Security

- Network Security itself does not provide any type of ROI – it is about cost management
- Example – You buy a Picasso straight from the artist and a safe to store it in. The safe adds no value to the painting – only helps prevent its loss (i.e. a cost to you)
- An organization that fails to adequately prepare a robust security solution faces potential loss from:
 - Lost productivity/Lost e-commerce revenue
 - Regulatory penalties
 - Tort litigation
 - Long-term business loss from lost customer confidence

Current Security Paradigm

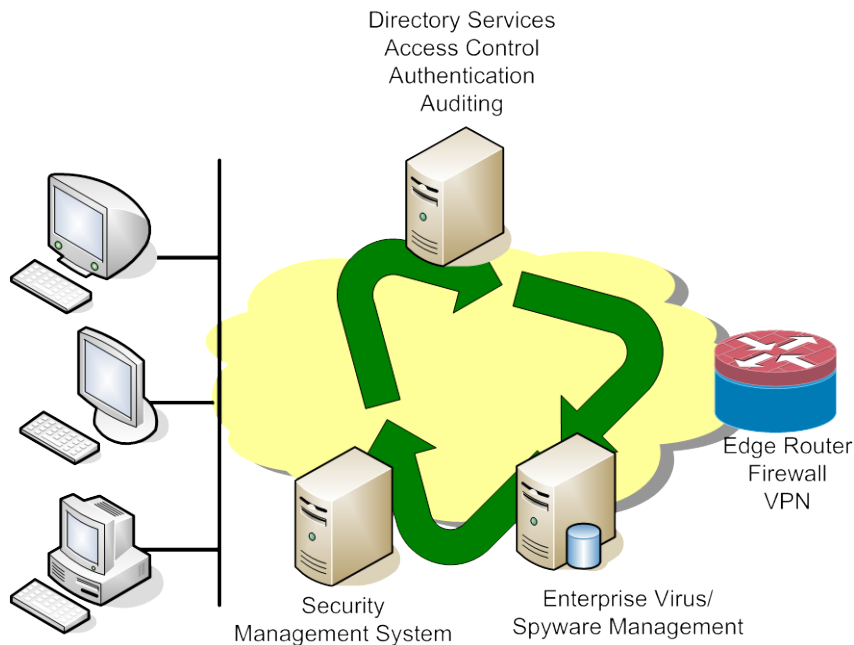


- Security environment quite complex today with many services offered by multiple vendors – including singular products that offer multiple services

IPv6 Security Models - Outcomes

- Defense-in-Depth security models will require better collaboration between all system components:
 - Edge & Host-based Firewall
 - IDS/IPS & Host-based IDS/IPS
 - VPN
 - Identity Management Systems
 - Application Security
 - NBAD, MARS, Wireless Security
- To manage requirements, improved security managements systems will be needed

Future Security Environment



- Future environments will require greater integration, otherwise too complicated
- NAC/NAP like function emerging, including new IETF working group (NEA – network endpoint assessment)
- Security systems will also need to address P2P communications
- Regulatory requirements require increased traceability

The Cost of Security in IPv6

- The cost of securing networks is rising!
 - Has nothing to do with IPv6
 - IPv6 will not make your cost of security less
- What will increase security costs is running dual-stack environment
 - Need to minimize the time spent in dual stack mode
- Additional security costs around managing the e2e aspect prominent in v6
 - Greater levels of application security and integrated, cooperative security management required
 - Cost is likely to be offset by the intrinsic value gained from P2P relationships

Revenue Opportunities in Security



Image Source: <http://www.trisec.com.au>

IPv6 Networked Home – Premise

- High degree of connection in the home, including P2P, P2M, M2M
- Security requirements are high and must include:
 - Intrusion Prevention
 - Integrity
 - Privacy
- Security needs likely to be too complicated for “average” user to manage

IPv6 Networked Home - Opportunity

- IPv6 Networked Homes represent new business opportunities:
 - Security software developers like Symantec, McAfee, Trend Micro can develop security management systems for the home
 - Security services companies such as Verisign can add PKI services for home users
 - ISPs can provide comprehensive security management services, including monitoring, identity management, and PKI infrastructure for increased ARPU (avg. revenue/user)

Special Thanks to:

Merike Kaeo – Double Shot Security

John Spence – Command Information