



PRESENTS

**NETWORLD INTEROP**

an INTEROP event

# VPN—When and Why to “Roll Your Own”

---

**Michael Fuhrman**

**Manager, Security Consulting**

**13 September, 2001**



# Agenda

- **Assumptions**
- **What do I need to do?**
  - Business issues**
  - Technology issues**
- **Limitations**
- **Costs**
- **Pros and cons**
- **Peanut butter cup**

# Assumptions

- **Already justified that VPN is right choice**
- **Currently do own network management**
  - Competent staff**
  - Budget**
- **Don't have **mission critical** needs**
- **Planning for future technology deployments**
  - Mobile**
  - Partner/customer extranets**
  - IP Telephony**

# What Do I Need To Do?

- **Consistent inventory**
  - Where are the devices?
  - What are the configurations?
- **Provisioning**
  - Create, modify, decommission
  - Configure parameters and schedule
  - Establish secure connectivity to devices
- **Auditing/monitoring**
  - Uptime
  - Throughput
- **Policy/methodology**
  - Encryption, authentication, topology



# Business Issues



- **Security at endpoints**

What is provider's state of security?

SLA... so what?

Then again... what is my state of security?

Who's between me and my service provider?

- This is about **privacy**, right?

Is my data also my competitor's data?

Then again... can my manufacturing access our financials?

What can the provider do with my usage data?

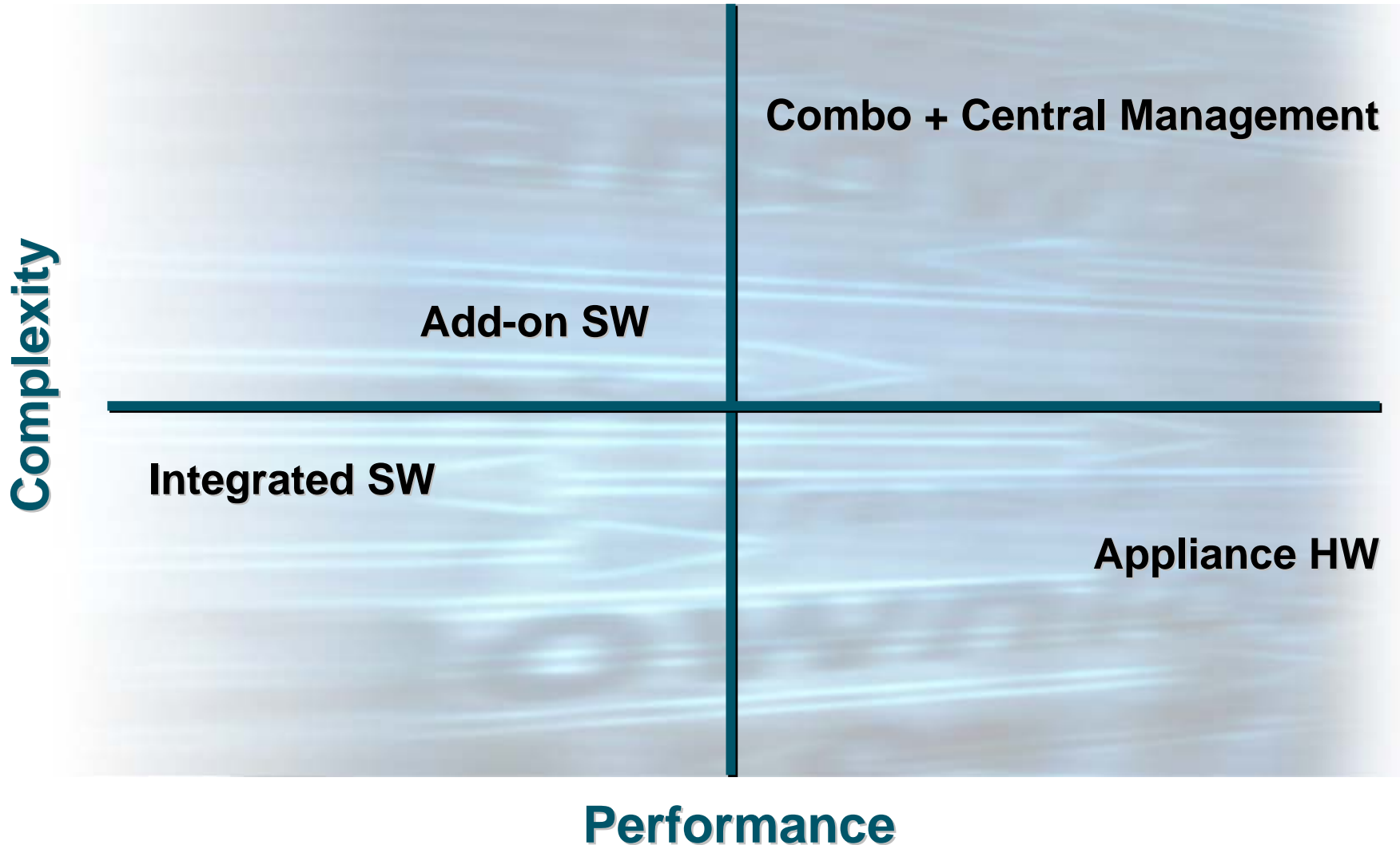
- **Maturity of the market**
  - Site-to-site is maturing**
  - Remote access still in infancy**
  - Big players may lack skill sets**
  - Smaller players may lack capital, reach**

# Technology Issues

- **Encryption choices**
  - DES, RSA, 3-DES—How do I know what I need?
  - Export issues—Can I or can't I?
- **Tunneling options**
  - PPTP, L2TP, IPSec
  - What are the pros and cons to each option?
  - What devices do I currently have and what do they support?
- **Authentication**
  - Internet Key Exchange (IKE), RADIUS, PKI
  - Key management
  - Certificates?
- **Vendor interoperability (management)**



# Know Your Limitations





# Cost—Remote Access\*

- **Components**

  - User device/platform**

  - User security (personal firewall, authentication, disk encryption)**

  - User connectivity (dial or fixed)**

  - Head-end infrastructure**

- **Deployment for 500–1000 users**

  - \$30/month/user with RADIUS authentication**

  - \$34/month/user with token-based authentication**

- **750 users = \$22,500 – \$25,500 per month**

# Pros and Cons to Build— Remote Access

- **Pros**

- Ease of deployment**

- Head-end management**

- Lack of managed services maturity**

- **Cons**

- Client life-cycle and general management**

- Coverage**

- Objective reporting**

# Cost—Site-to-Site\*

- **Components**

  - **Head-end infrastructure (headquarters)**

  - **Remote infrastructure (branch office)**

- **\$200–\$500/site/month to cover management costs**

  - **Should decrease as new tools arrive**

  - **Makes most sense with expensive WAN links**

- **Large enterprise with 15 remote sites**

  - **\$3,000–\$7,500 per month**

\* META Group, July 2001

# Pros and Cons to Build—Site-to-Site

- **Pros**

- Security (or at least perceived security)**

- Lack of SLA**

- Choice of technology**

- Choice of network**

- **Cons**

- Vendor interoperability, flexibility, immaturity**

- Management**

- Lack of SLA**

- Cost of build-out**

# The Peanut Butter Cup

- **Mix of carrier-monitored and customer-managed**
  - Carrier designs and delivers VPN equipment**
  - Customer has “local” tool for policy and provisioning**
  - Carrier manages from NOC**
- **Pros**
  - Balance between carrier and customer—customer maintains “control” and insight**
  - Reduced cost compared to total outsourcing**
- **Cons**
  - Balance between carrier and customer—the blame game**
  - Cost may not equal carrier contribution**
  - Early in adoption lifecycle—exact balance yet to be found**



# Summary

- **Build strategy still right for certain corporations**
  - 150:1 ratio of users to support personnel for DIY\***
  - Remote access easier decision**
  - Site-to-site for low priority traffic and right staffing**
- **Don't do it "just because..."**
  - Know your limitations**
  - Understand the ROI**
- **Try the peanut butter cup to achieve MPLS benefits**
- **Network-based services at forefront by 2004–5**
- **Managed services market will consolidate**
- **Security biggest reason to go it alone right now**

\* TeleChoice, 1999



PRESENTS

**NETWORLD INTEROP**

an INTEROP event

# VPN—When and Why to “Roll Your Own”

---

**Michael Fuhrman**

**Manager, Security Consulting**

**13 September, 2001**

