Panel Title: Public Networks for Private Access

Panel Chair: Dr. Tina Bird, Secure Network Systems

Panelists: Fred Chase, MITRE
Tom Gilbert, Blue Ridge Networks
Stacey Lum, InfoExpress
Roy Pereira, TimeStep

Session Abstract:

The typical corporate network now extends beyond company headquarters to sites around the country, if not around the world. Employees need access to corporate computer resources from a wide variety of locations. Internet-based connectivity is replacing privately maintained dial-in access in many companies, because of the widespread availability of Internet access.

Many organizations have been willing to use minimal authentication and security mechanisms for remote access via modems, because telephone circuits are perceived (correctly or not) to be "private." But the same companies are much more cautious about allowing inbound connectivity via the Internet, where threats to data confidentiality and integrity are common.

Virtual private network technologies address many of the security risks inherent in providing "private network" access to remote users over the Internet. This panel will discuss mechanisms available today for mitigating these public network risks. We will specifically address the following questions:

1) How do I assess the remote access requirements of my organization?

2) If VPN is a reasonable fit, how do I determine which VPN solution to implement?

3) How do I integrate VPN into my existing network infrastructure?

Tina Bird (panel chair):

Tina is a security analyst at Secure Network Systems, a small consulting firm in Lawrence, KS. She has implemented and managed a variety of wide-area-network security technologies, such as firewalls and VPN packages; built and supported extranet and intranet remote access packages; and developed, implemented and enforced corporate IS security policies in a variety of environments. Her main focus in the last year has been on the evaluation and implementation of virtual private networking solutions in small- to mid-sized networks (40 to 4000 hosts). Tina is the moderator of the Virtual Private Networks mailing list, and is currently writing a book on VPN implementations with Ted Stockwell (Ascend). Tina has a BS in physics from Notre Dame and an MS and Ph.D in astrophysics from the University of Minnesota.

Dr. Tina Bird, CISSP
Secure Network Systems
729.5 Massachusetts St.

Lawrence, KS 66044
v: (785) 843-8855 x111
f: (785) 843-4981
tbird@netdefense.com

David Bovee:

David is a Security Engineer for Verio Northwest, provides consulting to customers seeking to implement VPNs. Additionally, he provides value-added integration services for various VPN products. He has participated actively in the publication of various NT security related resources, including SANS Institute's "NT Security, Step-by-Step".

David Bovee, MCSE
Verio Northwest
15400 SE 30th Place, Suite 202
Bellevue, WA 98007
v: (425) 649-7466
f: (425) 649-7451
dbovee@nw.verio.net

Fred Chase:

Fred has been with The MITRE Corp. since 1984. He is currently responsible for secure remote access (the only kind, at MITRE!) and network infrastructure vulnerability analyses. Fred's previous work at MITRE includes specification of security-relevant parts of the Space Defense Operations Center (SPADOC); membership on a Technical Advisory Panel, assembled by the Air Force Studies Board of the National Academy of Sciences, that investigated the security of NORAD's missile warning correlation center system; evaluation of VAX/VMS for the NCSC; and development of ANSSR, a tool for assessing risk of information disclosure in complex systems. Fred holds a BA in physics from Swarthmore, and a MSCS from Penn State.

Frederick N. Chase
MITRE Corporation
202 Burlington Road
Bedford, MA 01730
v: (781) 271-7769
f: (781) 271-3816
fnc@mitre.org

Tom Gilbert:

Tom is Vice President of Sales and Marketing and a founder of Blue Ridge Networks, producers of high security virtual private network products for the U.S. Government. Mr. Gilbert has been involved in secure networking for government applications since 1982. He was part of a product team that delivered the first packet filtering IP router in 1988, the first VLAN in 1990 and the first commercial VPN product in 1994. As Director of Marketing at Network Systems Corporation in 1995, his team introduced the packet encrypting Security Router, which won the Best Internet Product Award at InterOp. Tom has thirty years of experience in the computer and data communications industry. He has a BS Degree from Rensselaer Polytechnic Institute.

Tom Gilbert
Blue Ridge Networks
14120 Parke Long Court, Suite 201
Chantilly, Virginia 20151
v: (703) 631-0700
tom@blueridgenetworks.com

Stacey Lum:

Stacey is president and chief technology officer of InfoExpress, a supplier of remote VPN software. Lum was the original author of the company’s flagship product, VTCP/Secure, and currently leads the development of InfoExpress’s network security products. Lum has been involved in the design and development of Internet, wireless, and WAN protocols for over 15 years. Stacey has a BS in Electrical Engineering and Computer Science from University of California at Berkeley.

Stacey Lum
InfoExpress, Inc.
425 First Street, Suite E
Los Altos, CA 94022
v: (650) 947-7880
f: (650) 947-7888 FAX (August 1)
lum@infoexpress.com

Roy Pereira:

Roy is the product manager for TimeStep Corporation, a Newbridge affiliate dedicated to developing secure virtual private network (VPN) solutions. He is heavily involved with product management, product direction, product integration and security. Roy has been an active participant in the ANX initiative and the IETF, working in the IPSec and IP Compression working groups. His previous position was that of security architect, where he was involved in Internet standards and new technology. After having done undergraduate computer science studies at Carleton University, Roy has over 11 years experience in the software development industry with a focus on Internet protocols, telecommunications protocols, software APIs, and e-mail systems.

Roy Pereira
TimeStep Corporation
362 Terry Fox Drive
Kanata, Ontario K2K 2P5 Canada
v: (613) 599-3610 x4808
f: (613) 599-3617
rpereira@timestep.com

Public Networks for Private Access

National Information Systems Security Conference

October 5-8, 1998

Panel Members

- Dr. Tina Bird, Secure Network Systems -- Chairperson
- Fred Chase, MITRE
- Tom Gilbert, Blue Ridge Networks
- Stacey Lum, InfoExpress
- Roy Pereira, TimeStep

Requirements for Remote Access

- Provides remote connectivity to private network
- (+) Controls and monitors remote use of private network resources
- (+) Maximizes possible number of remote locations

Requirements for Remote Access cont.

- (+) Minimizes cost of hardware, network utilization and support personnel

What is a secure Virtual Private Network (VPN)?

- Protected network connection between an individual and a private network (client-to-server) or a remote LAN and a private network (client-to-server)

VPN Security Features

- Encrypted session (protects data from eavesdropping during transmission)
- Digitally signed (protects data from unauthorized modifications)
- Strongly authenticated, either by user or by machine (verifies identity of remote endpoint)

VPN Security Features cont.

- Access control mechanisms (provide granular access to private network resources)
- Hides private network topology (hides potential network targets from attackers)

VPN Design Issues

- Who are your remote users: travelling employees, branch office workers, business partners, consultants?
- Where are your remote users located: hotels, branch offices, customer sites, overseas?

VPN Design Issues cont.

- What client systems are in use: Win95/NT, UNIX, Mac?
- What applications do you need? What network protocols will they use?
- What authentication requirements will be enforced?

VPN Design Issues cont.

- What network throughput will you need?
- Does your firewall or router system already support secure VPNs?

Selection & Testing

- Business and technical requirements determine type of VPN
- Use specific security requirements to narrow VPN selections to 2-3 products for in-house testing

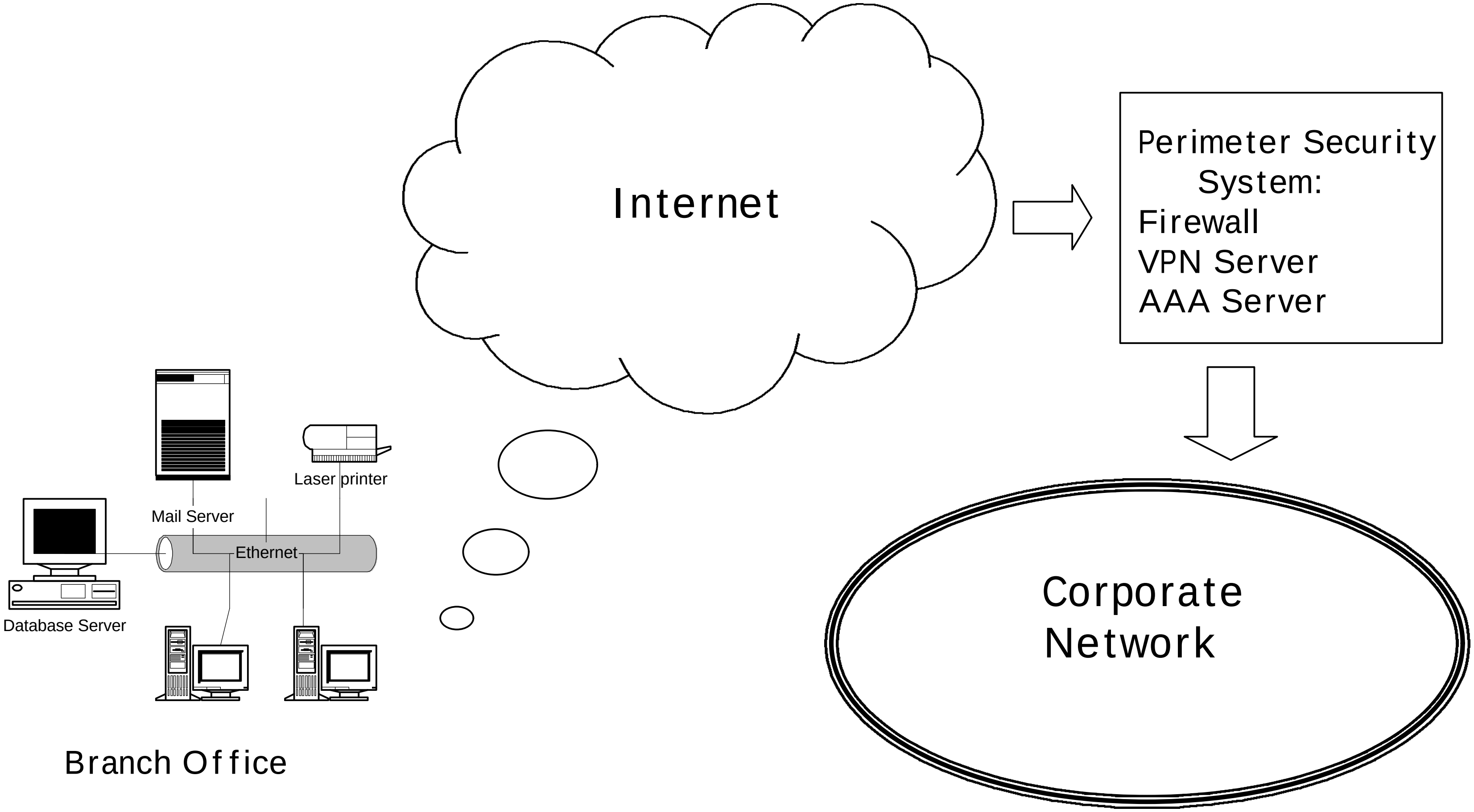
VPN Differentiators

- Supports your organization’s RAS policy - strong authorization, granular access, flexibility of encryption algorithm and key length
- Ease of use and management, for both client and server

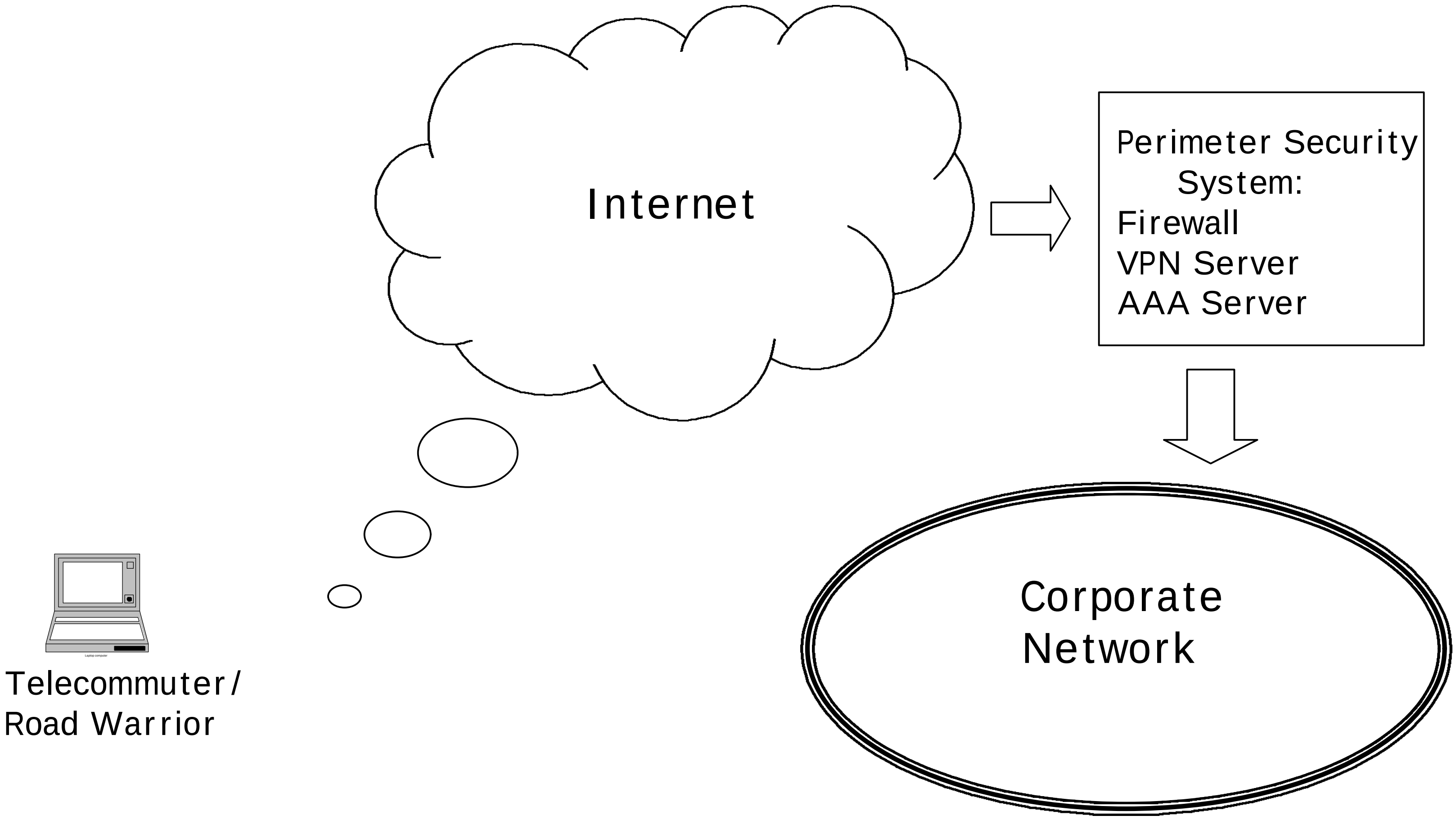
VPN Differentiators cont.

- Supports your applications and network protocols (+non-standard!)
- Ability to function in both client-to-server and server-to-server mode
- Quality of technical support
- Price of software, hardware required

Scenario #1: Branch Office Connectivity



Scenario #2: Remote Employees



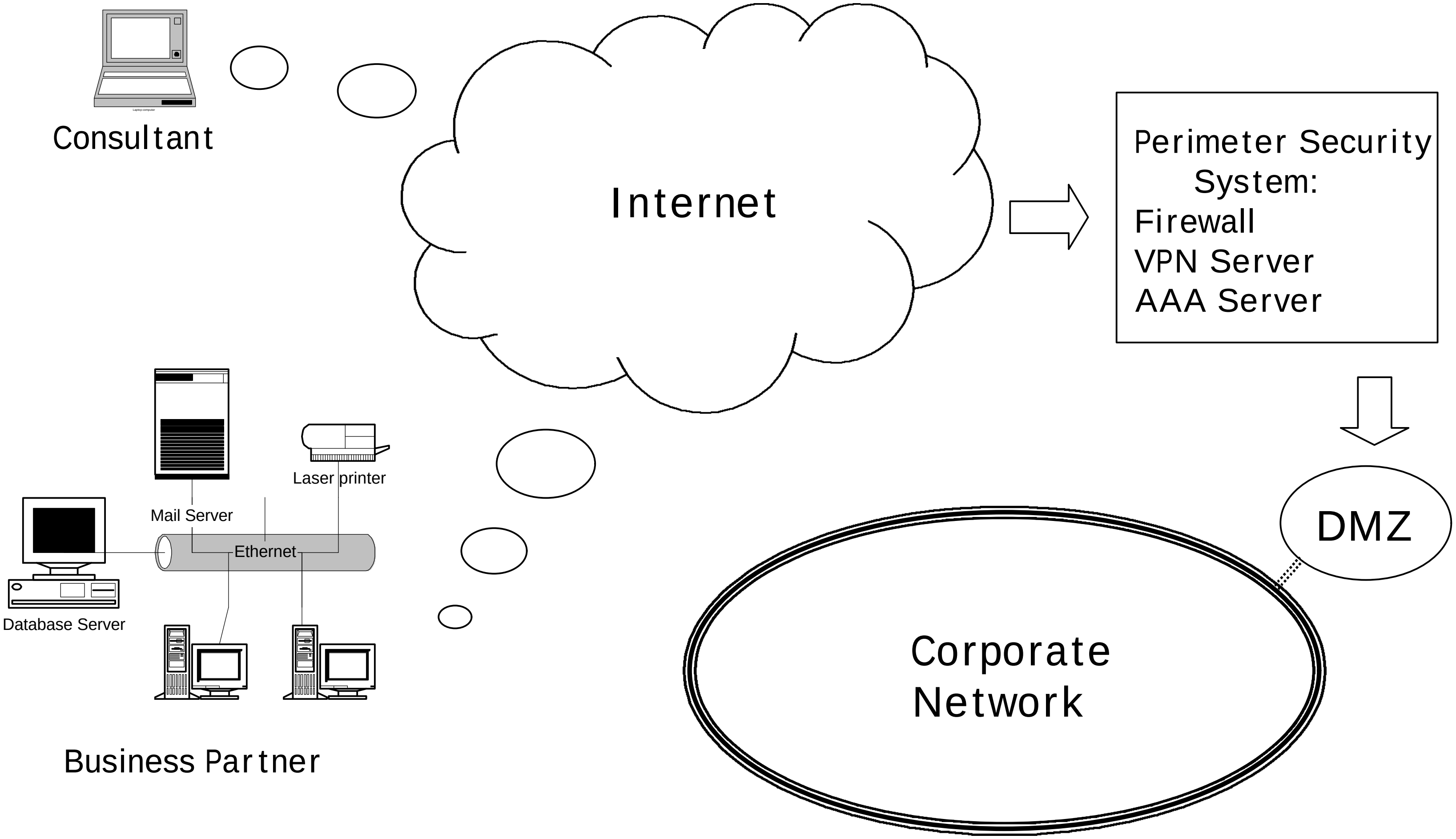
Internet

Perimeter Security System:
Firewall
VPN Server
AAA Server

Corporate Network

Telecommuter/ Road Warrior

Scenario #3: Extranet Connectivity



Consultant

Internet

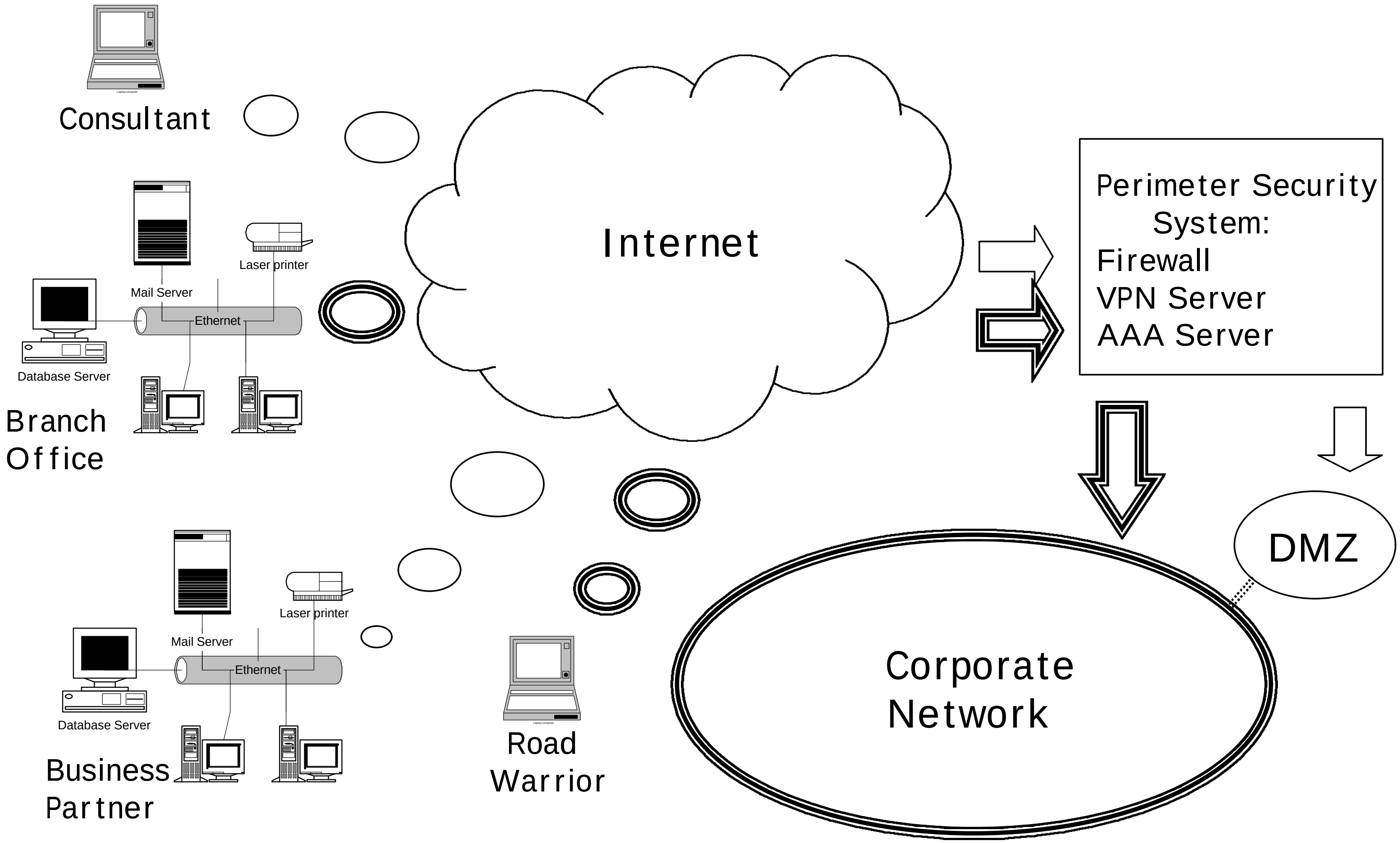
Perimeter Security System:
Firewall
VPN Server
AAA Server

DMZ

Corporate Network

Business Partner

Scenario #4: The Real World



Consultant

Branch Office

Business Partner

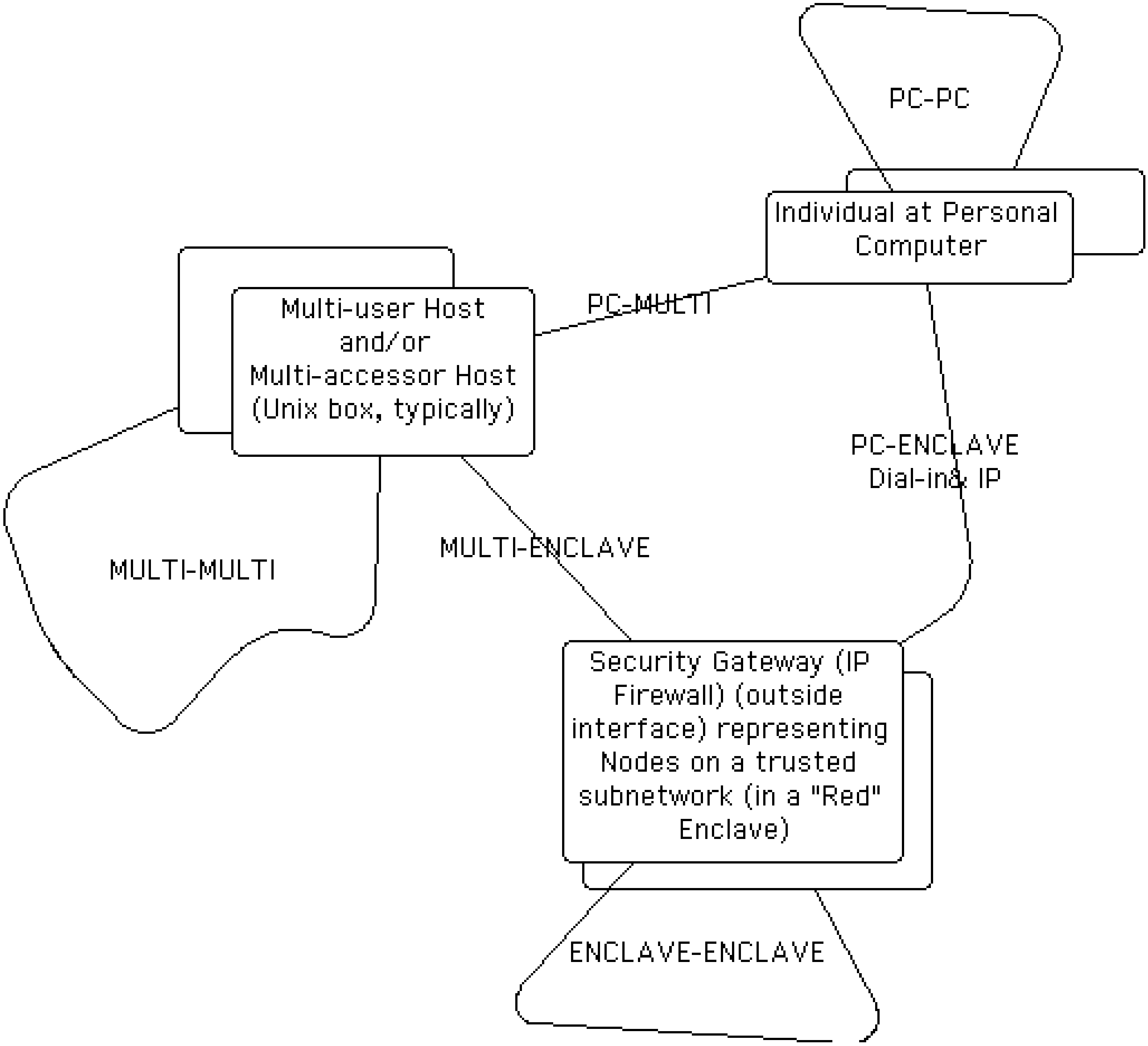
Road Warrior

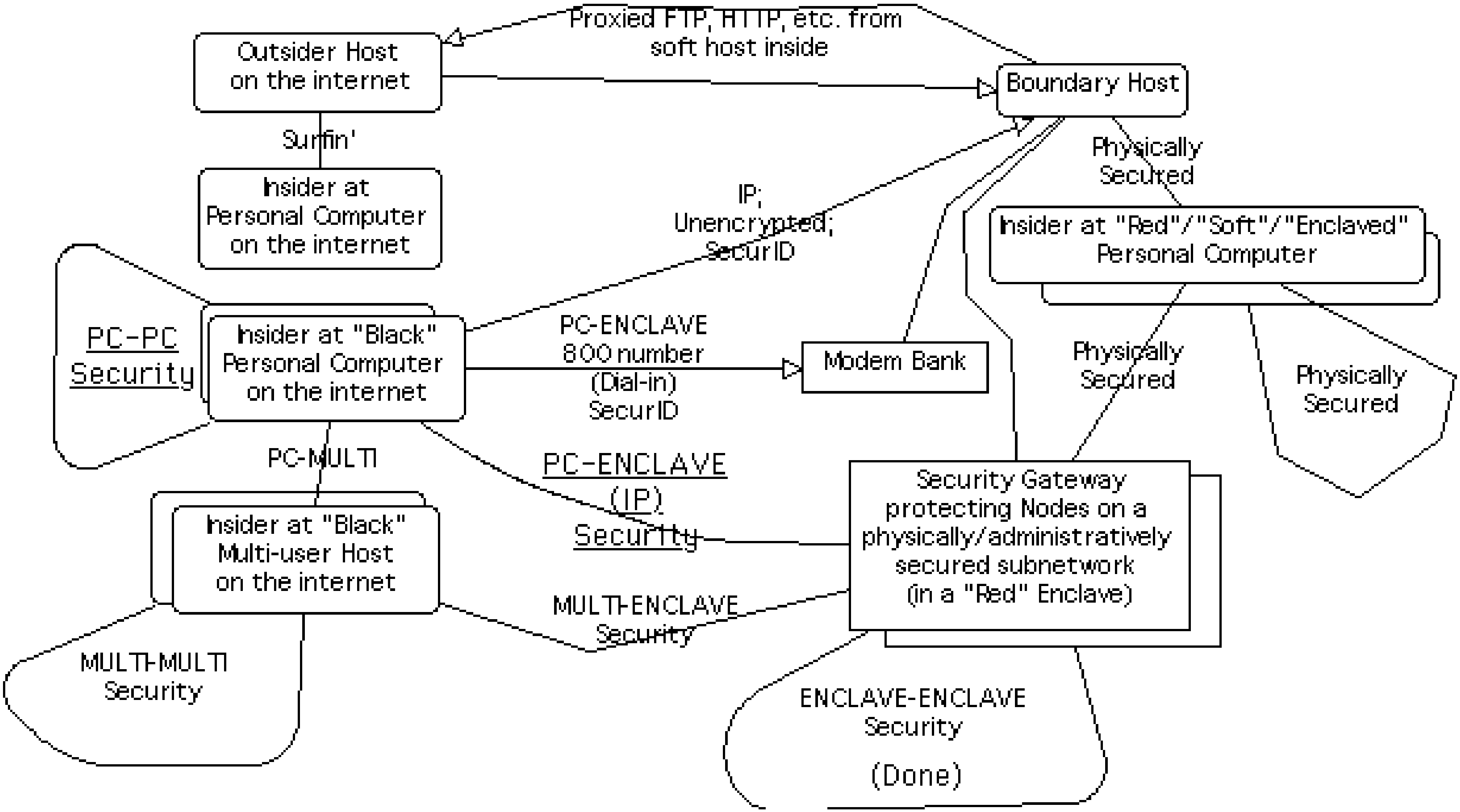
Internet

Perimeter Security System:
Firewall
VPN Server
AAA Server

DMZ

Corporate Network


PC-PC
Individual at Personal Computer
Multi-user Host and/or Multi-accessor Host (Unix box, typically)
PC-MULTI
PC-ENCLAVE Dial-in& IP
MULTI-MULTI
MULTI-ENCLAVE
Security Gateway (IP Firewall) (outside interface) representing Nodes on a trusted subnetwork (in a "Red" Enclave)
ENCLAVE-ENCLAVE


Proxied FTP, HTTP, etc. from soft host inside
Outsider Host on the internet
Boundary Host
Surfin'
Physically Secured
Insider at Personal Computer on the internet
IP; Unencrypted; SecurID
Insider at "Red"/"Soft"/"Enclaved" Personal Computer
PC-PC Security
Insider at "Black" Personal Computer on the internet
PC-ENCLAVE 800 number (Dial-in) SecurID
Modem Bank
Physically Secured
Physically Secured
PC-MULTI
PC-ENCLAVE (IP) Security
Security Gateway protecting Nodes on a physically/administratively secured subnetwork (in a "Red" Enclave)
Insider at "Black" Multi-user Host on the internet
MULTI-ENCLAVE Security
MULTI-MULTI Security
ENCLAVE-ENCLAVE Security
(Done)