



Building the Distributed Enterprise: Implementing Secure VPN for Telecommuting and Remote Network Access

Speaker: Rob Greer
Vice President, Systems Engineering



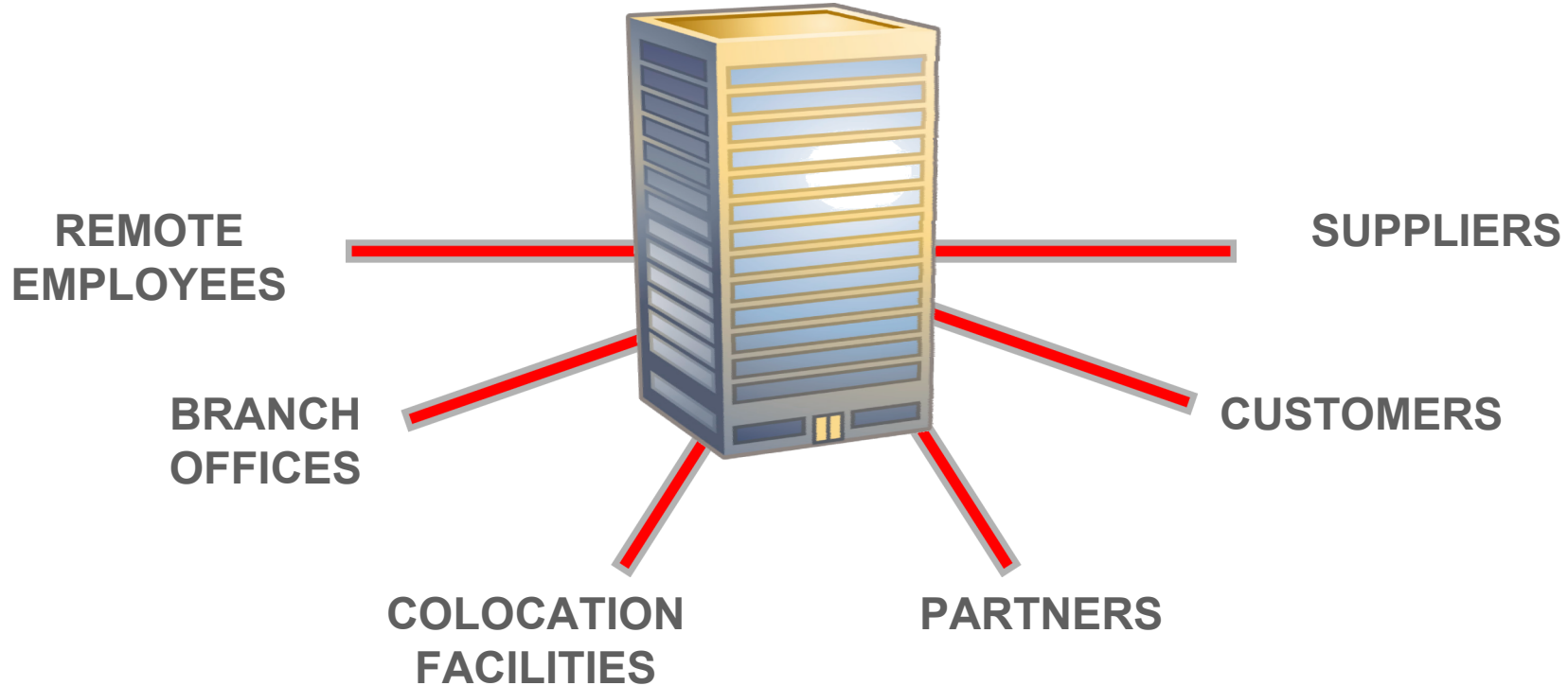
SONICWALL

Agenda








- ▶ Connectivity Business Challenges and Options
- ▶ Defining Virtual Private Networking (VPN)
- ▶ Benefits of VPN
- ▶ Key Considerations When Deploying VPN
- ▶ Enabling Telecommuting
- ▶ Enabling Office to Office Communications
- ▶ Enabling Manageability as the Security Perimeter Grows
- ▶ SonicWALL “enables” Secure Connectivity



Connectivity Business Challenges



Connectivity Options

| | LOW-COST | HIGH-SPEED | SECURE |
|-----------------------------|--|---|--|
| DIAL-UP MODEM |  |  |  |
| LEASED LINE/ FRAME RELAY |  |  | |
| BROADBAND |  | |  |



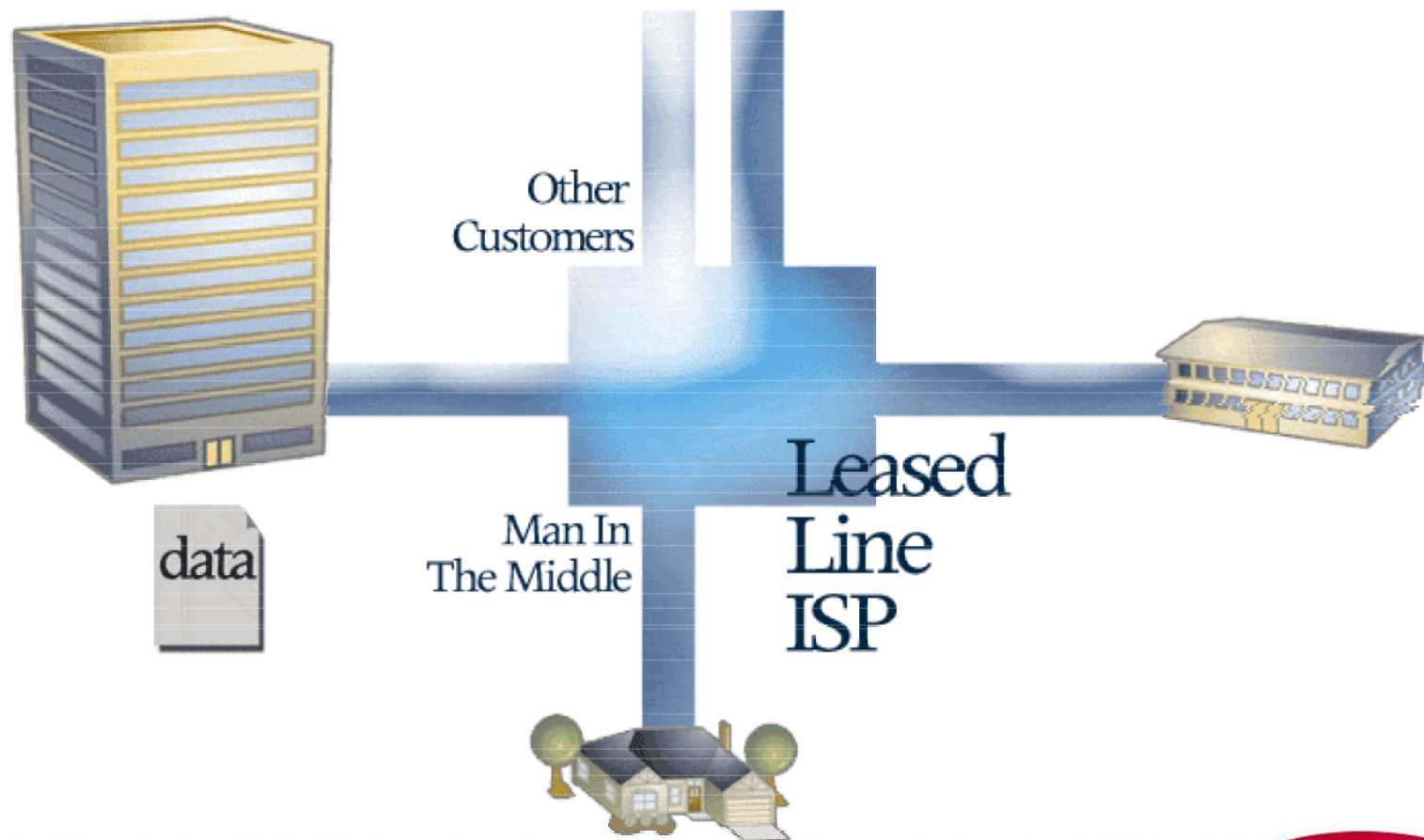
Scenario #1: Communicate in the “Clear”

- ▶ Connecting two sites with a “private” leased line has been the standard approach
 - > Costly
 - > Inflexible



Scenario #1: Communicate in the “Clear”

- ▶ “Private” leased lines may not be as “private” as you think!



Defining Virtual Private Networking (VPN)

- ▶ VPN leverages the cost advantages of the public Internet infrastructure while keeping communications “private”



Understanding IPSEC VPN











- IKE (Internet Key Exchange)
- Manual Key

- HMAC-MD5 (128-bit) algorithm
- HMAC-SHA-1 (160-bit) algorithm

- DES (Data Encryption Standard) - 56 bit
- 3DES - 56 bit
- AES (Advanced Encryption Standard) - 128 bit



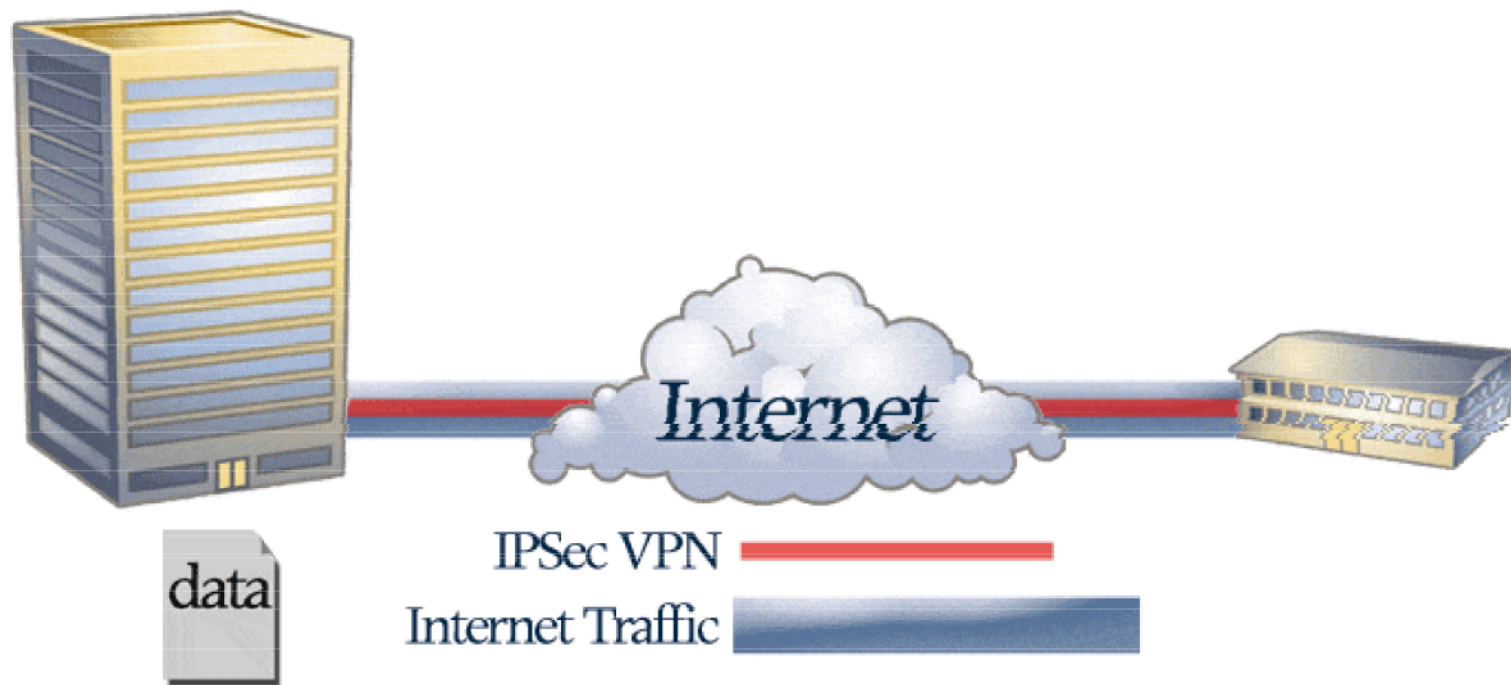
Benefits of IPSEC VPN Over Broadband

| | LOW-COST | HIGH-SPEED | SECURE |
|-----------------------------|--|---|--|
| DIAL-UP MODEM |  |  |  |
| LEASED LINE/ FRAME RELAY |  |  | |
| BROADBAND |  | |  |
| IPSEC VPN OVER BROADBAND |  | | |



Scenario #2: Secure Data Transmission

- ▶ VPN ensures that communications traffic is encrypted and authenticated



Scenario #2B: Secure Data Transmission Issues

- ▶ However, if the endpoints of a VPN tunnel are left unprotected, malicious activity can still compromise the network



Scenario #3: Secure Data WHILE Protecting Resources

- ▶ Implementing other layers of security at each point of the network ensures complete protection
 - > Firewall
 - > Anti-virus



Key Considerations For VPN Applications

- ▶ Vendor
 - > Financial stability
 - > Security expertise
 - > Installed base & reference accounts
 - > Growing business
- ▶ Existing Network / Security Infrastructure
 - > Interoperability requirements
 - > IP addressing
 - > IP allocation methods: PPPoE, DHCP, PPTP, Static
- ▶ Types of Remote Access Required
 - > Telecommuting
 - > Branch office connectivity
 - > Roaming User or “Road Warrior”

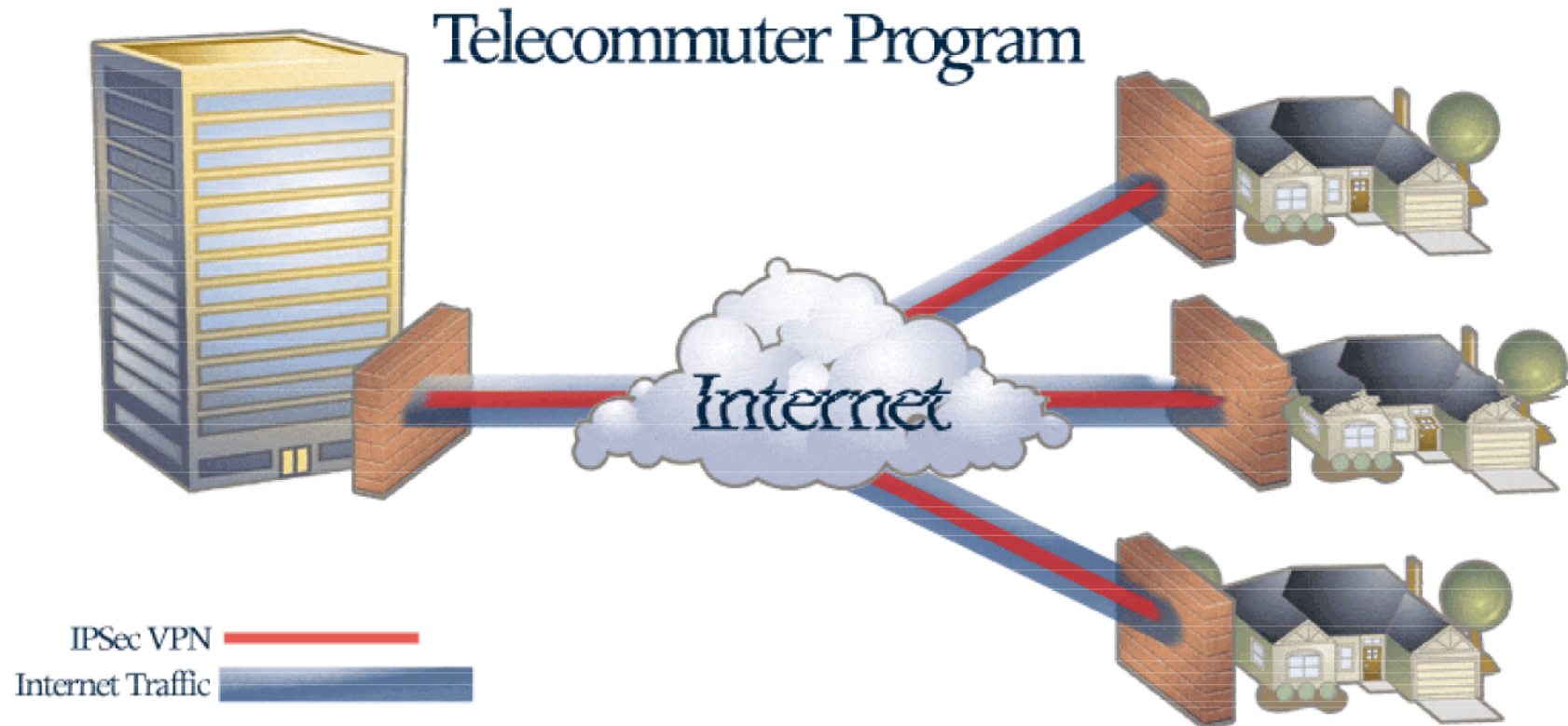
Key Considerations For VPN Applications

- ▶ Supported Connectivity Types
 - > xDSL,
 - > Cable modem
 - > Frame-relay
 - > Point-to-point circuits
 - > Satellite
- ▶ Growth Plans
 - > 6 months
 - > 12 months
 - > 18 months
- ▶ Ongoing Management & Support
 - > In-house IT Responsibilities
 - > Outsourced IT Responsibilities (i.e. value added reseller, Managed Security Services Provider)



Enabling Telecommuting

- ▶ Leveraging security devices at every telecommuter ensures protection for your “distributed” network



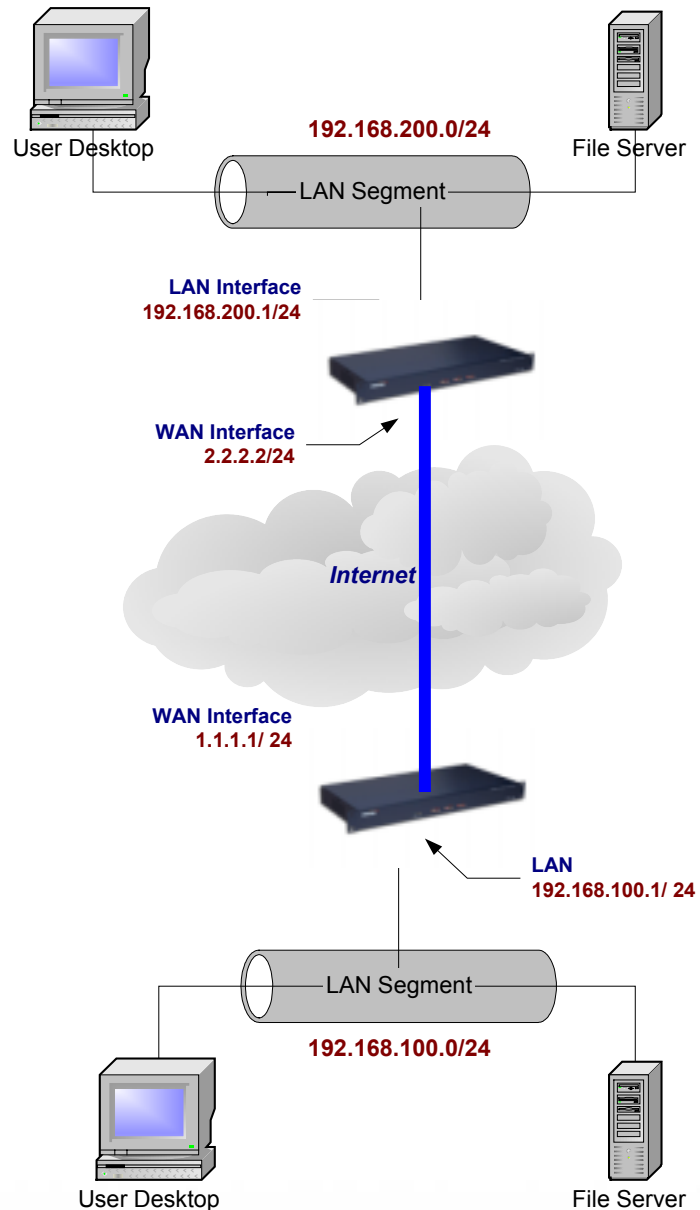
Enabling Secure Office-to-Office Communications

- ▶ Security devices at all office locations ensure both secure communications and reliable high-performance connectivity

Office-To-Office Communications



Building an IPSEC VPN “Tunnel”



Assumptions:

- 1) Both sites connect to the Internet via ADSL
- 2) Both ends have static IP addresses
- 3) Only one destination network exists at both ends
- 4) The key management mode chosen is IKE using Pre-Shared Secret

Information Required for a SINGLE Tunnel:

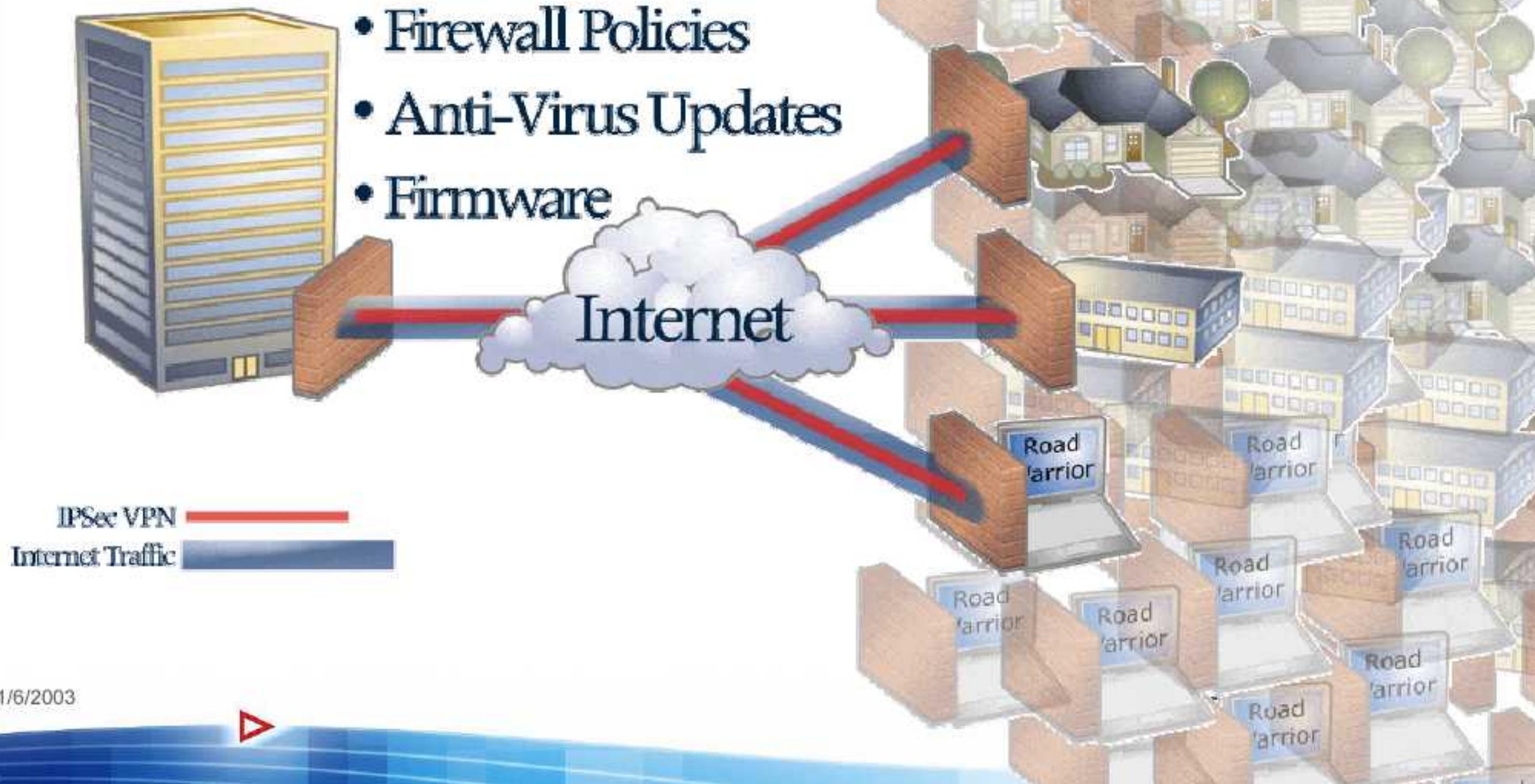
- 1) WAN IP Address or FQDN for both VPN devices
- 2) Internal Destination Networks for both VPN devices
- 3) Matching Encryption & Authentication Methods for both VPN devices (Phase 1 & Phase 2)
- 4) A matching Pre-Shared Secret for both VPN devices
- 5) TCP / IP traffic allowed to traverse the VPN tunnel



Enabling Manageability as the Security Perimeter Grows

Central Management

- Firewall Policies
- Anti-Virus Updates
- Firmware



Effective Management Platform

- ▶ Centralized Management
- ▶ Scalable
- ▶ Easy to Use
- ▶ Lightweight Graphical User Interface (i.e Web Based)
- ▶ Role-Based Administration
- ▶ “Group” Policy Support
- ▶ “Inheritance” Concept Applied
- ▶ Provisioning Tools
- ▶ Enterprise Database Support (i.e. Oracle, MS SQL Server)
- ▶ Native License & Subscription Management
- ▶ Built in Graphical Reporting Capabilities



Summary

- ▶ Connectivity outside corporate headquarters is not just a luxury....it's a business imperative
- ▶ VPN ensures that all communications are “private” and enable networks to leverage the public Internet
- ▶ VPN encryption combined with firewalls and other security techniques are essential for complete protection
- ▶ Successful VPN implementations depend on a robust management platform

