

Is Network Security an Oxymoron?

Chris Hopen, CTO, Aventail Corp.



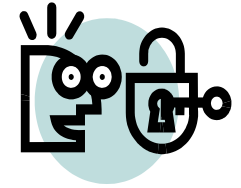
Two World Views on Security



Network Companies

- Remote Access is a special use case
- Networks can be made intelligent and secure – at a cost \$\$\$
- More firewalls, more private infrastructure
- Retrofit Infrastructure to ensure *security*
- Model after PSTN

Aventail



- Everything is Remote – So ~~Remote~~ goes away
- *Drive Secure Communications*
Assume networks are insecure -- always
- More public networks, shared infrastructure
- Focus the investment on *reliability* of service
- Model after e-commerce

Driving Toward “Always On” VPN

Market Trends:

- Ubiquity of broadband
- Penetration of devices
- Increasing prevalence of VOIP
- Phenomenon of inverted networks

From: *Anywhere* VPN → To: *Everywhere* VPN

The Emergence of A Platform

Everywhere VPN:

*Manageability,
Scalability,
Reliability*

Application Security

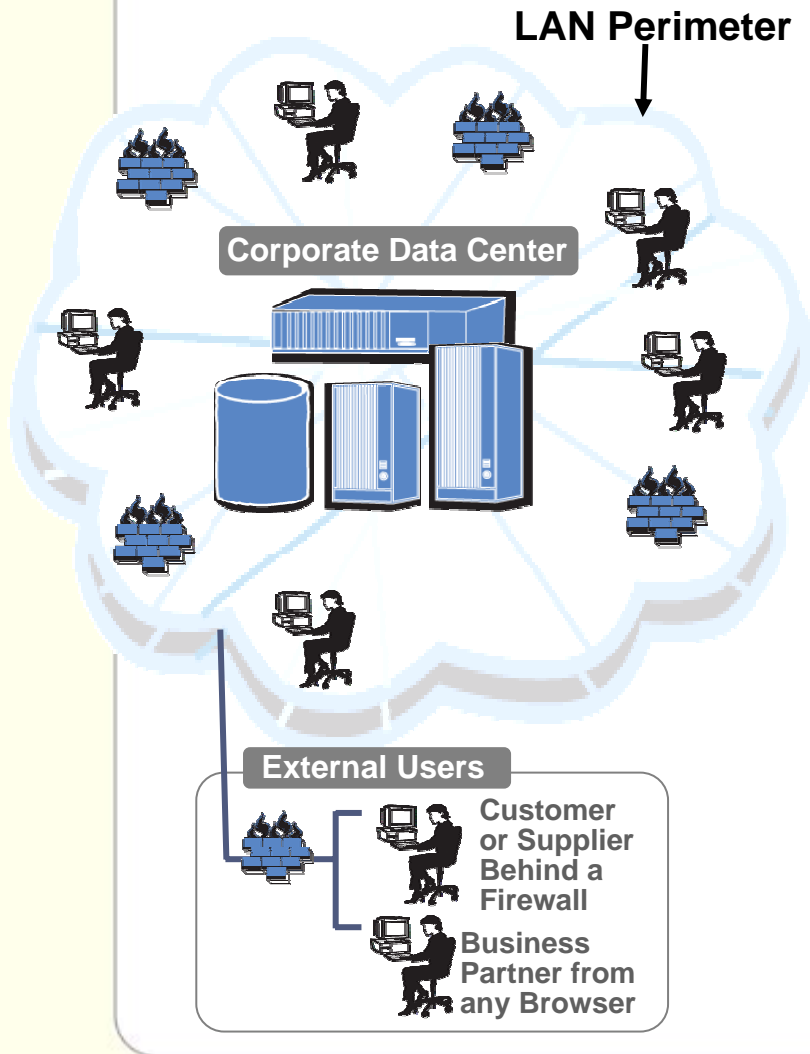
Policy / Authorization

End Point Control

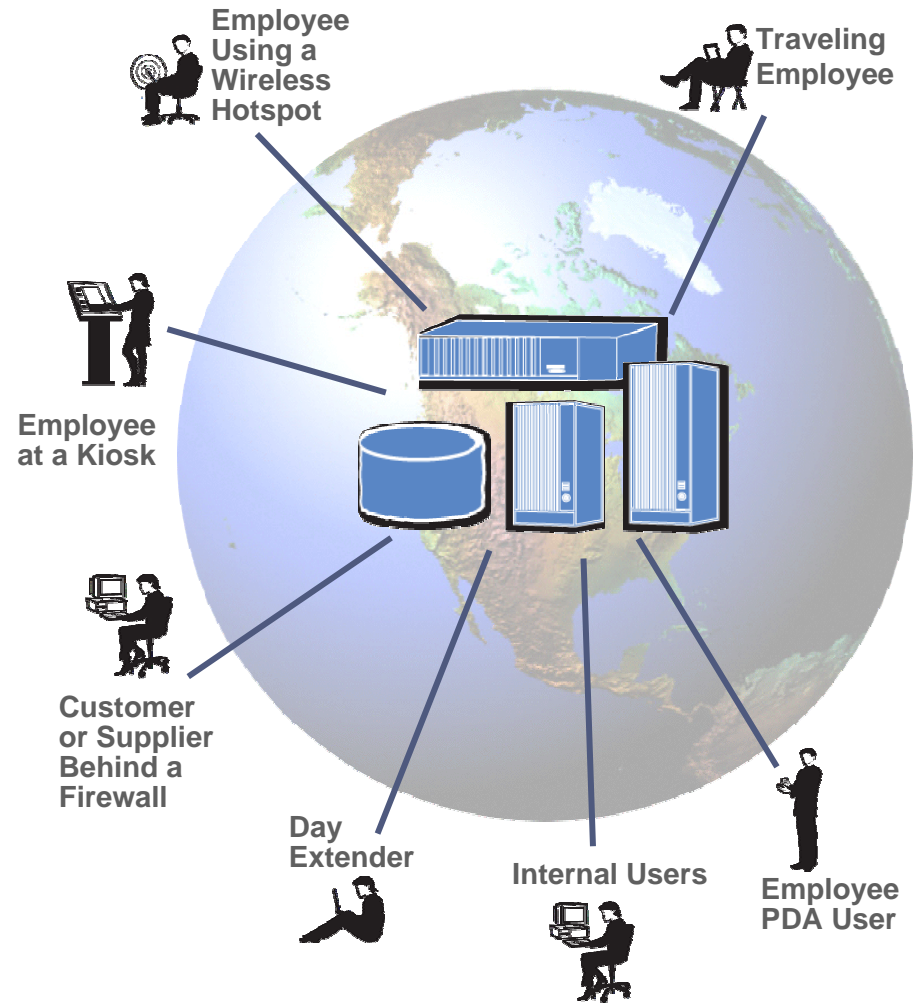
SSL VPN (Access)

To Meet the Changing Corporation

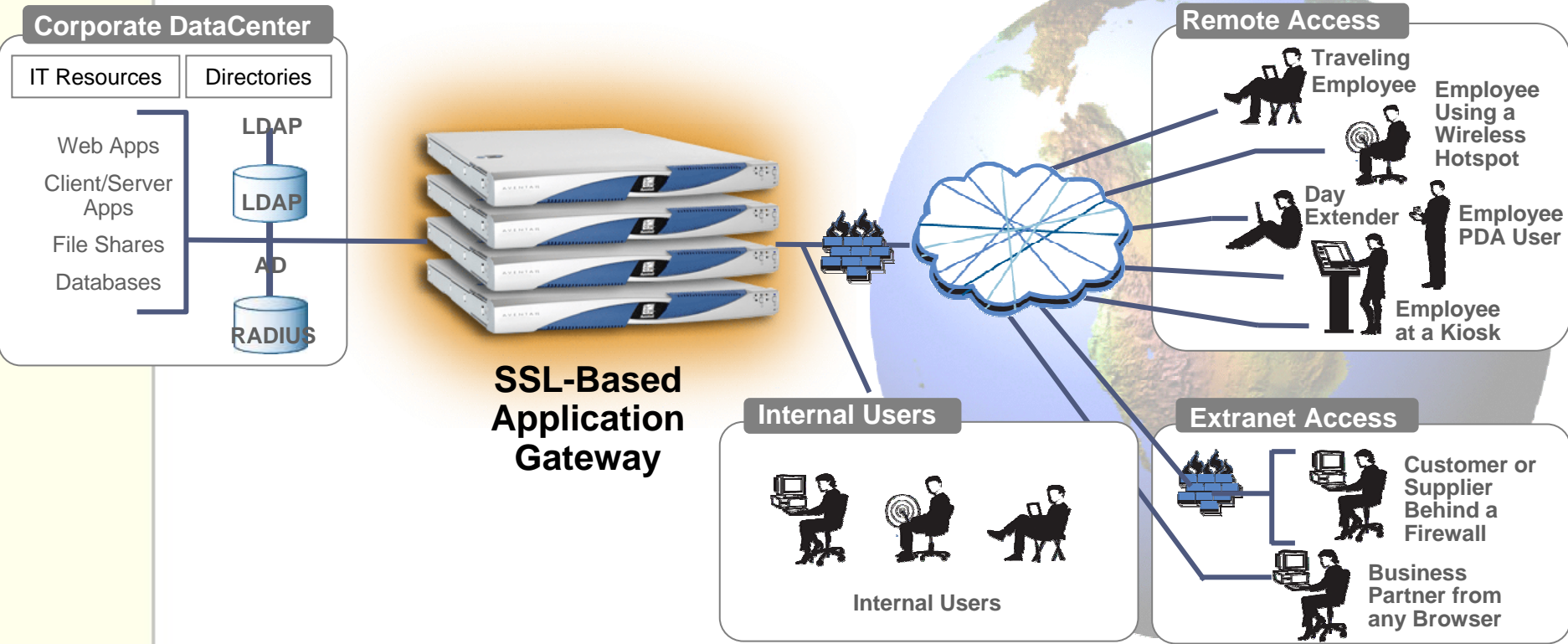
1995: Network Perimeter



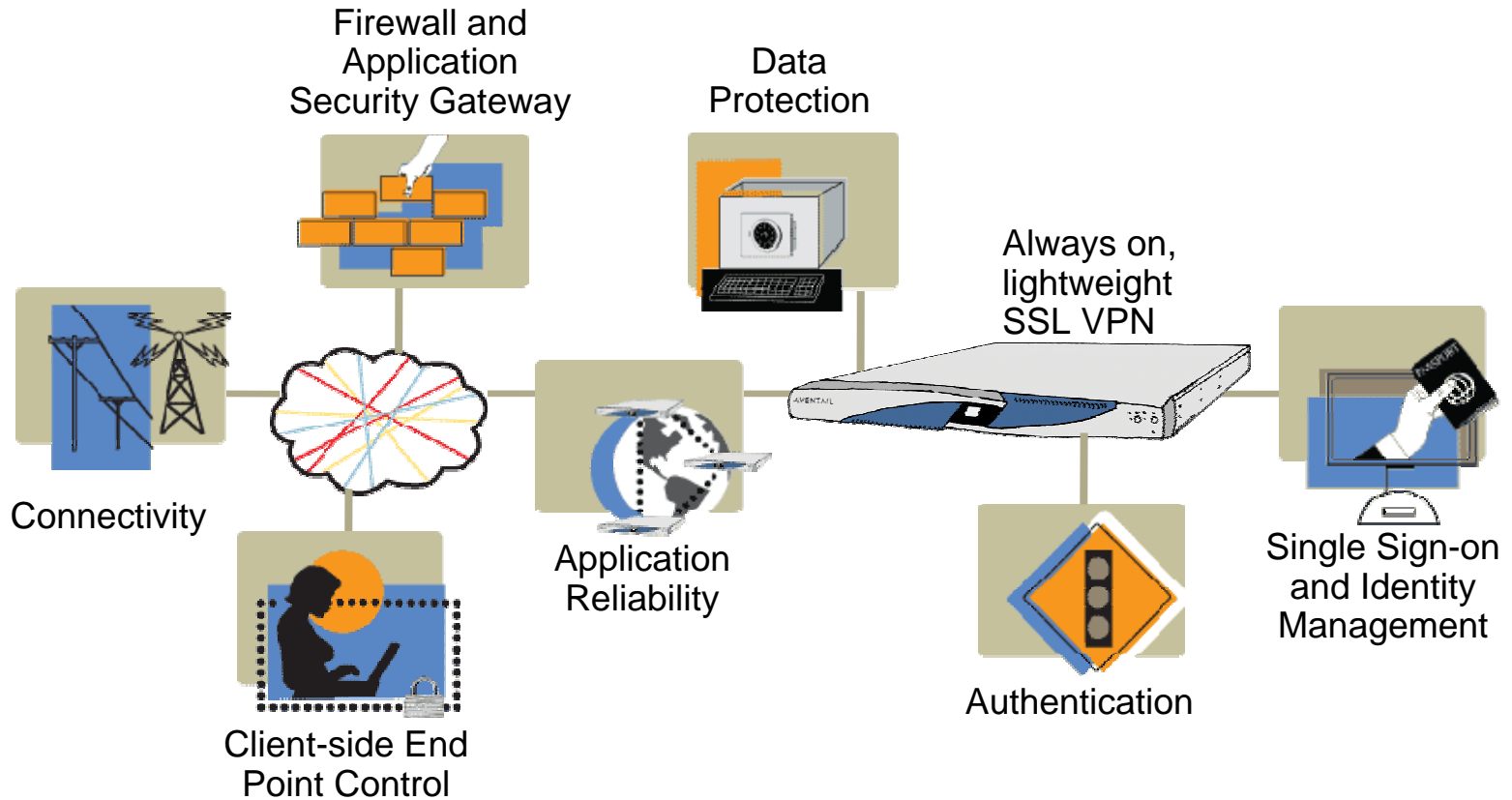
2010: Invisible Perimeter



SSL VPNs at the Application Perimeter



The Framework for Application Security



SSL VPNs will provide a framework enabling maximum application interoperability for end-to-end application security

SSL VPNs Are the Future of Remote Access

Compared to traditional remote access via IPsec, SSL VPNs provide:

- **A single solution for all remote users**
 - Internal or external, client or clientless
 - Enabling increased productivity for employees and partners
- **More Security and Control**
 - Granular access control and end point security
- **Ease of use and Management**
 - Transparent access
 - Policy management
- **Lower total cost of ownership**
 - Leverage public infrastructure and the Internet
 - Clientless option saves money
 - Huge drop in support calls for remote access

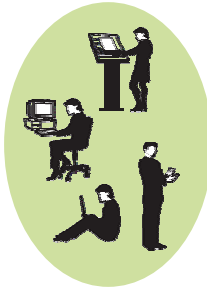
SSL VPNs provide a single solution

Web and client solution for both non-managed and IT managed devices for all users and access scenarios

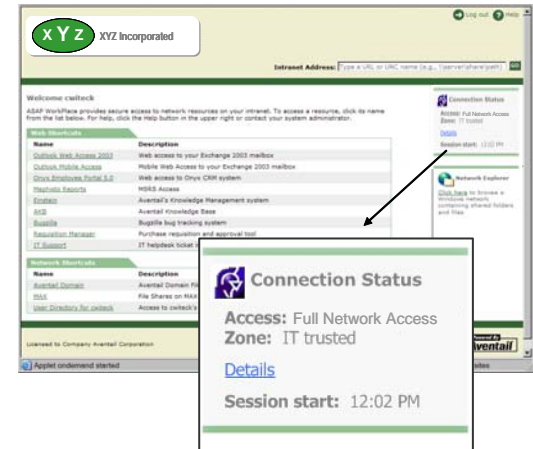
Clientless experience

Clientless Browser Based Access

Kiosk Users
Extranet
Day Extenders
PDA Users



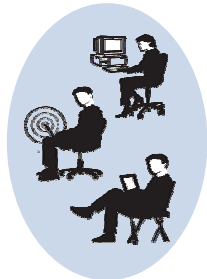
Tunnel access is integrated into the portal, providing full application reach via the Web.



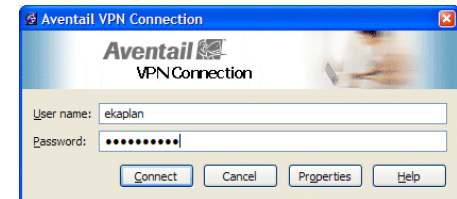
Client experience

Client Based Access

Internal Users
Wireless LANs
IT-Mgd Devices



Tunnel provides complete network access from a Web deployed/delivered Windows client, providing a complete "in office" experience.



Aventail VPN Connection Speed: 100.0 Mbps

Secure Tunnel Technology

IPSec VPNs create a Layer 3 network tunnel for open access to the entire network. What's needed is a tunnel that combines the reach of Layer 3 with the policy control of Layers 4 through 7.

Clientless Web Access



Client-installed Access



Corporate Network



VoIP Applications



File Shares



Traditional Client/Server Applications

- *Layer 3 Tunnel with Layers 4 – 7 Policy Control*
- *Bidirectional Tunnel Control*
- *Closed security model by default*

End Point Control based on Policy

Strong end point control enables access from places IT cannot possibly control, based on the level of trust for the user and the device

Trusted Zone

Device Profile: IT-Managed

- Application/Process
- Directory/File
- Registry key
- Windows domain → *in.xyz.seattle.com* or *in.xyz.phoenix.com*
- Anti-Virus → *Norton AV*
- Personal Firewall → *Sygate*

Data Protection

- Aventail Cache Control
- Aventail Secure Desktop

Semi-Trusted Zone

Device Profile: Home Machine

- Application/Process
- Directory/File
- Registry key → \geq *...HKEY_LOCAL_MACHINE\SWSymantec\SharedDefs*
- Windows domain
- Anti-Virus → *Norton AV*
- Personal Firewall → *Sygate* or *Zone*

Data Protection

- Aventail Cache Control
- Aventail Secure Desktop

Un-Trusted Zone

Device Profile: Unknown

- Application/Process
- Directory/File
- Registry key
- Windows domain
- Anti-Virus
- Personal Firewall

Data Protection

- Aventail Cache Control
- Aventail Secure Desktop

- *Admin defines the Policy Zone by specifying the Device Profile and Data Protection Level*
- *Device is interrogated prior to authentication to ensure security*

Ease of Use

User does not have to “work” at access, as the right access method is transparently and quickly deployed

The screenshot shows a web browser window displaying the XYZ Incorporated intranet. The page features a header with the XYZ logo and navigation links for Home and Network Explorer. A search bar for the Intranet Address is present. The main content area includes a welcome message for user 'cwiteck' and two tables of shortcuts: Web Shortcuts and Network Shortcuts. A sidebar on the right displays connection status details, including agent information and session start time. The footer contains licensing information and the Aventail logo.

XYZ Incorporated

Home Network Explorer

Intranet Address: GO

Welcome cwiteck

ASAP WorkPlace provides secure access to network resources on your intranet. To access a resource, click its name from the list below. For help, click the Help button in the upper right or contact your system administrator.

Web Shortcuts

Name	Description
Intranet	Access to company information - news, directory, events, and departments
OWA	Outlook Web Access 2003
AMC	Use Aventail's Management Console
WTS	Windows Terminal Services
Citrix	Citrix Metaframe XP application portal

Network Shortcuts

Name	Description
internal_domain	
DC	
exchange	

Connection Status

Agent: Aventail
Ondemand - Dynamic Mode
Zone: Trusted Zone

[Details](#)

Access any URL/Client server application

Session start: Tue Sep 28 21:22:22 GMT 2004

Licensed to Company Aventail SE

Powered By **Aventail**

Applet ondemand started

Internet

This block shows a detailed view of the connection status sidebar from the screenshot. It includes a globe icon, the title 'Connection Status', and the same text as seen in the main screenshot: 'Agent: Aventail Ondemand - Dynamic Mode', 'Zone: Trusted Zone', a 'Details' link, 'Access any URL/Client server application', and 'Session start: Tue Sep 28 21:22:22 GMT 2004'. An arrow points from the 'Details' link in the main screenshot to this detailed view.

Connection Status

Agent: Aventail
Ondemand - Dynamic Mode
Zone: Trusted Zone

[Details](#)

Access any URL/Client server application

Session start: Tue Sep 28 21:22:22 GMT 2004

Ease of Management

- SSL VPNs allow for easier set-up, configuration and management
- Policy can be set for users & groups, resources and access methods
- Best management is a Unified Policy model

The screenshot displays the Avenail ASAP Management Console interface. The main title is "Avenail ASAP Management Console". The left sidebar contains a navigation menu with the following sections:

- Security Administration**
 - Access Control
 - Resources
 - Users & Groups
- System Configuration**
 - Network Settings
 - SSL Settings
 - Authentication
 - General Settings
 - Maintenance
 - Services
- Monitoring**
 - System Status
 - Active Users
 - Logging
 - Troubleshooting
- User Access**
 - ASAP WorkPlace
 - Avenail OnDemand
 - End Point Control

The main content area is titled "Add/Edit Access Rule" and includes a breadcrumb trail: "Access Control > Add/Edit Access Rule". The page contains the following sections:

- Create or modify an access control rule.**
 - Number: * ID: AV 1096404099638
 - Description: The Description appears in log files and is useful in debugging.
 - Action: Permit Deny Disabled
- Basic Settings**
 - Users/Groups: Click an **Edit** button to manage the list of users or destination resources in this access rule.
 - Destination resources:
- Access methods**

Choose the access methods from which you will control access to this resource:

Any Selected

 - Web browser (HTTP/HTTPS)
 - Network Explorer (Web access to file system resources)
 - Avenail Connect and/or Avenail OnDemand (TCP/IP)
- End Point Control zones**

Choose the zones from which you will permit or deny access to this resource:

Zones:
- Advanced**

At the bottom of the page, there are three buttons: "Save", "Save and Add Another", and "Cancel".

SSL vs IPSec – the bottom line

SSL VPN

IPSec VPN

Usage types	Multiple remote access use cases	Only LAN-to-LAN remote access
Available access points	Managed and unmanaged environments: corporate laptops, home PCs, PDAs, kiosks, partner extranets	Managed environments only: corporate laptops
Access control	Application-level control	Unrestricted network access
End point control	Client integrity protection to ensure access point is safe, data protection to make sure nothing sensitive is left behind	Limited capabilities to determine security of the end point
Minimum access requirements	Standard Web browser and any Internet connection	Computer with pre-configured client and most Internet connections

Summary

- Communication and technology trends are driving **radical changes** in enterprise IT
- **Dumb, fast, redundant**, publicly available networks will become more desirable for enterprises
- The traditional enterprise IT is slowly migrating to the **E-Commerce organization model** to drive value
- SSL VPN based platform will provide the foundation for a lightweight secure **Always-On VPN**
- The market size for this opportunity is larger than today's FW/VPN market -- **larger than most suspect**

Questions ?