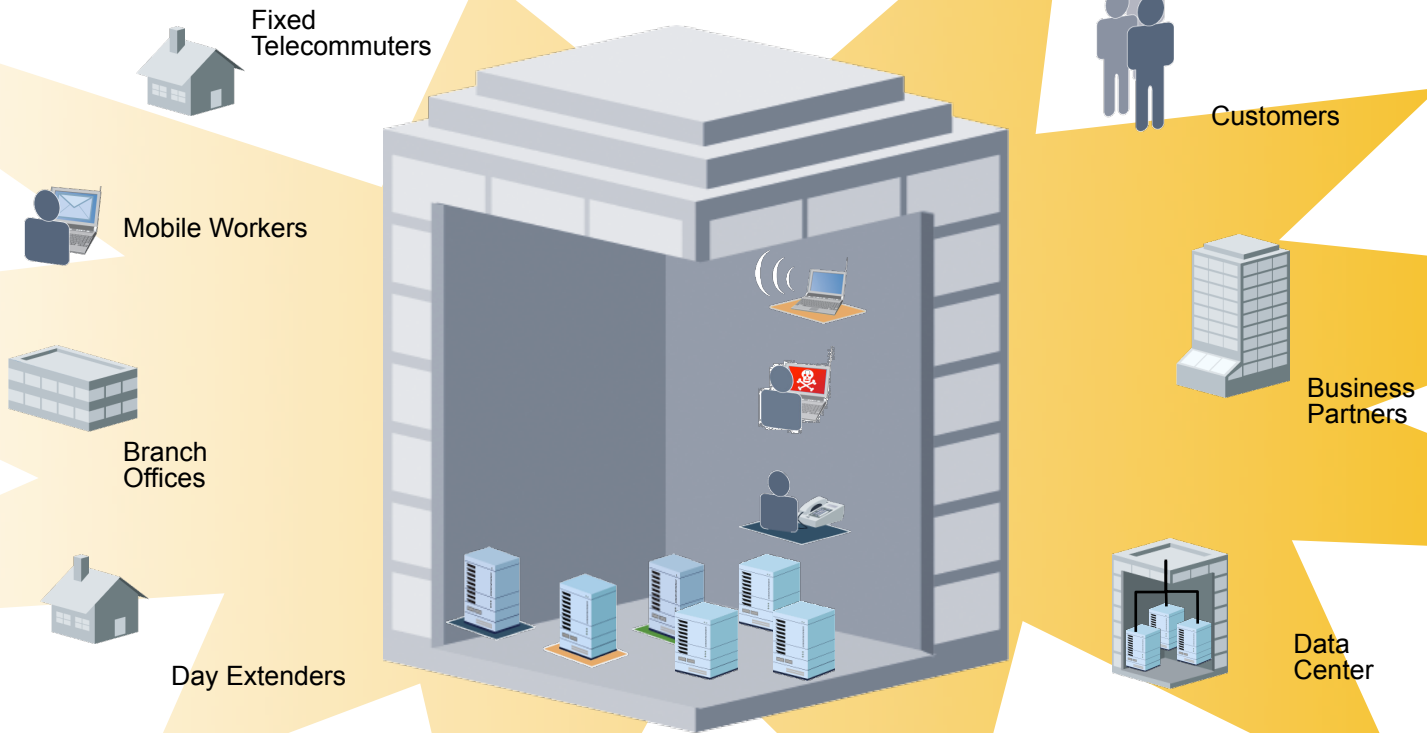


IPSec or SSL VPN?



The Extended Enterprise



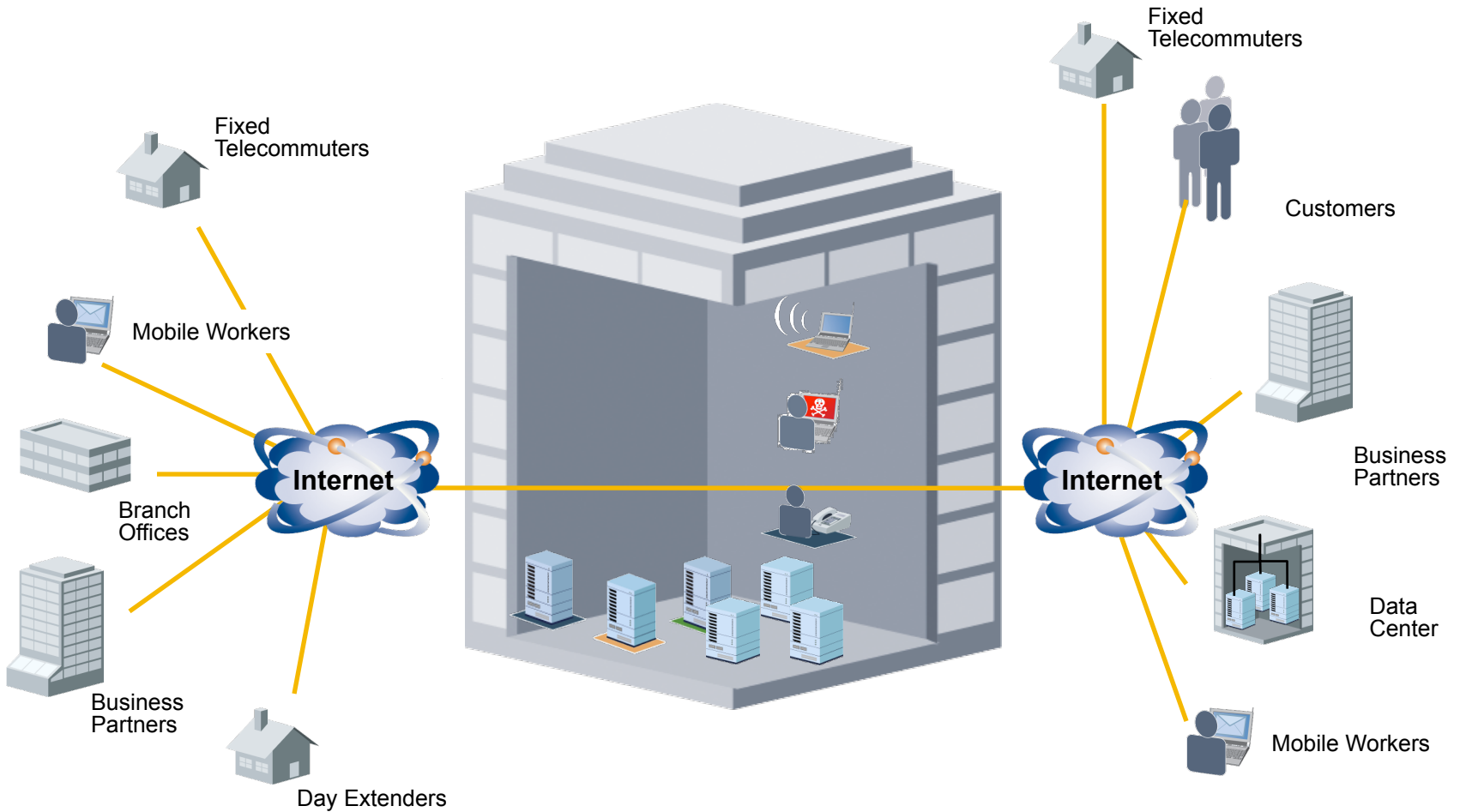
Juniper your Net

Connectivity Requirements

- Must support business productivity for all audiences, while cost-effectively securing communications
 - Secure
 - Affordable
 - Raise Productivity
 - High Performance & Availability

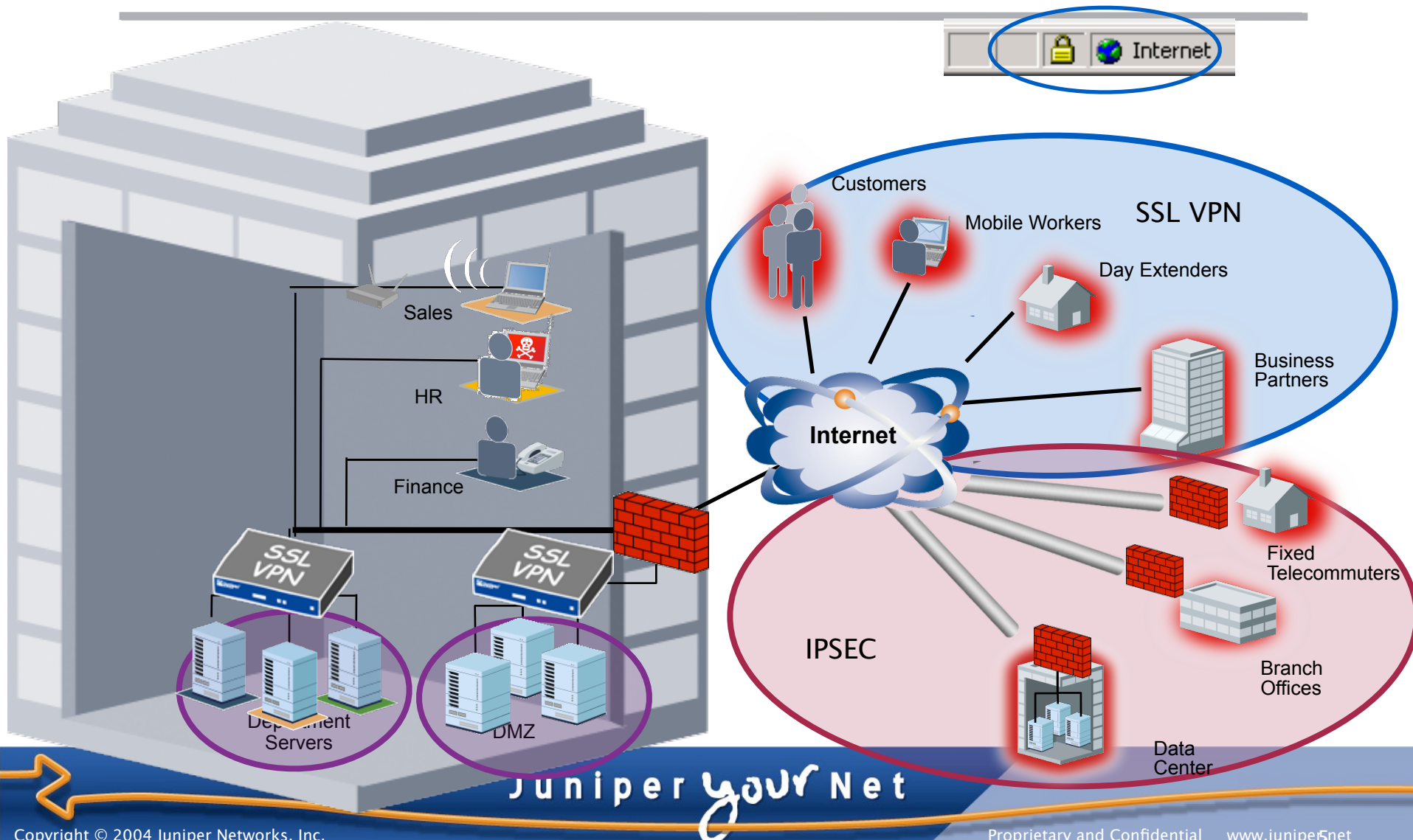
The Enterprise Connectivity Solution

Use the Internet to replace leased lines



Juniper your Net

IPSec and SSL VPNs



Customer Challenges: Access vs. Security

Maximize Productivity

- Extend application to partner (Partner Extranet)
- Increase employee efficiency (Intranet portals, ERP)
- Support different users (customized, controlled)
- Enable provisional worker (Contractor, off-shoring)

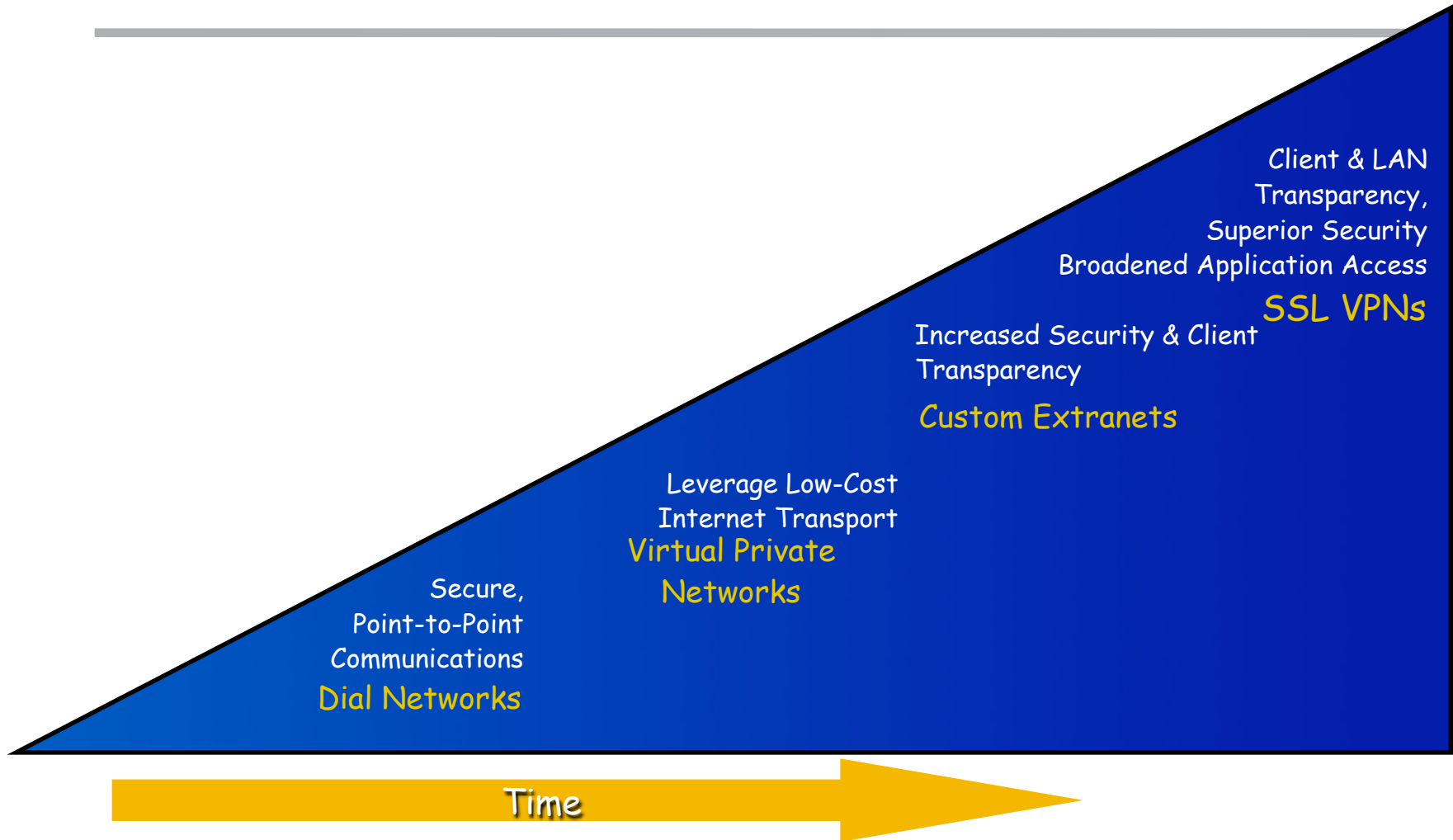
Enforce Strict Security

- Restrict access to appropriate level
- Mitigate risks from untrusted sources (i.e. kiosks, non-employees)
- Consistently apply security policy

Must Balance against Costs

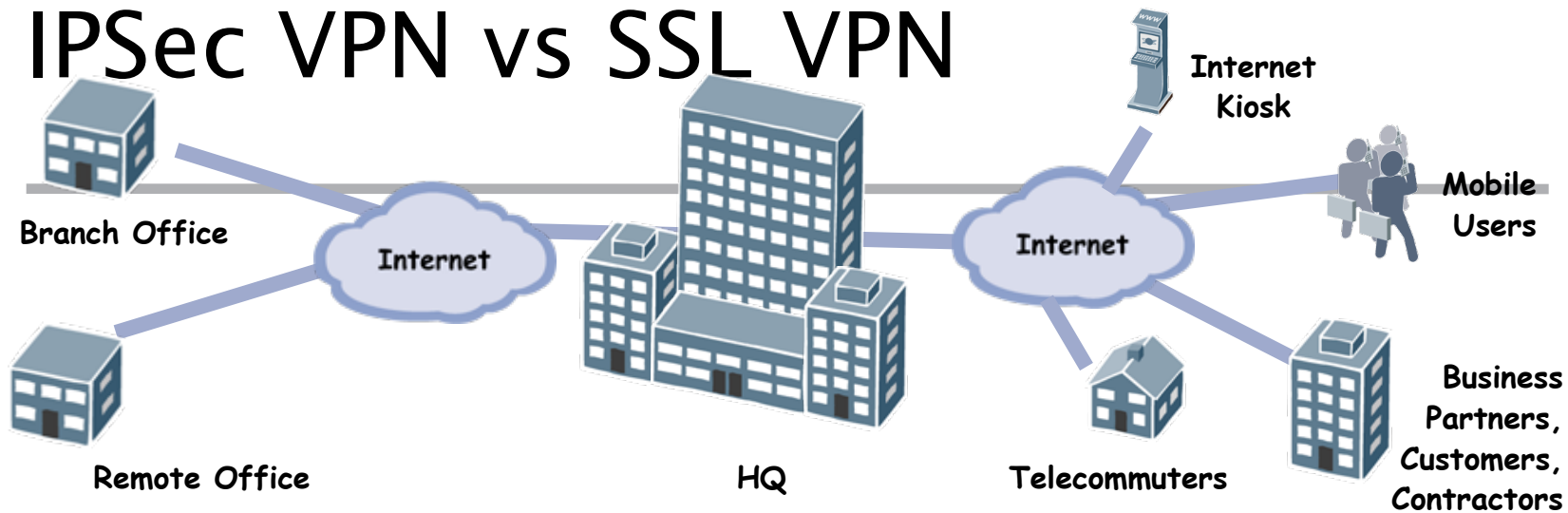
- Capital Expense
- Ongoing admin and support

Evolution of Secure Access Technologies



Juniper your Net

IPSec VPN vs SSL VPN



Application Type

Remote, Branch Office
Site to site

Type of Connection

Fixed

Remote Network Security

Managed, Trusted

Application Type

- Mobile User
- Partner Extranet
- Customer Extranet
- Contractor, offshore employee
- Telecommuter/day extender

Type of Connection

Mobile or Fixed

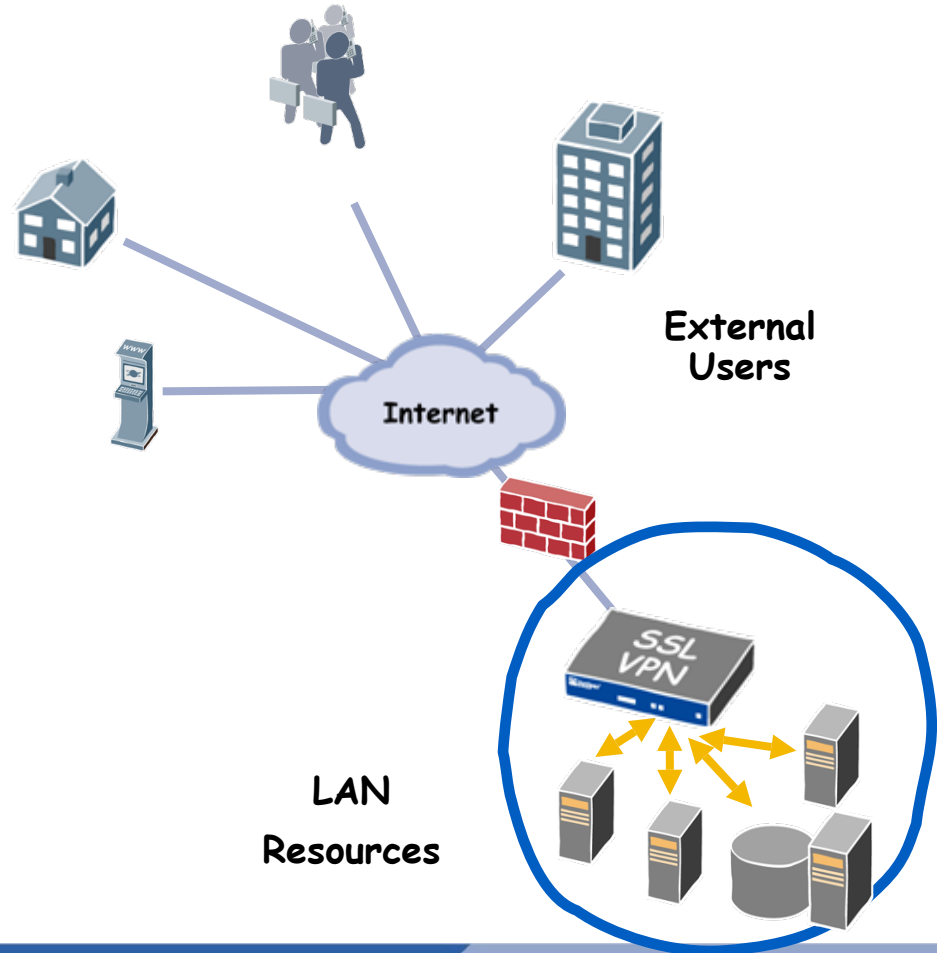
Remote Network Security

Managed or Unmanaged,
Trusted or Untrusted

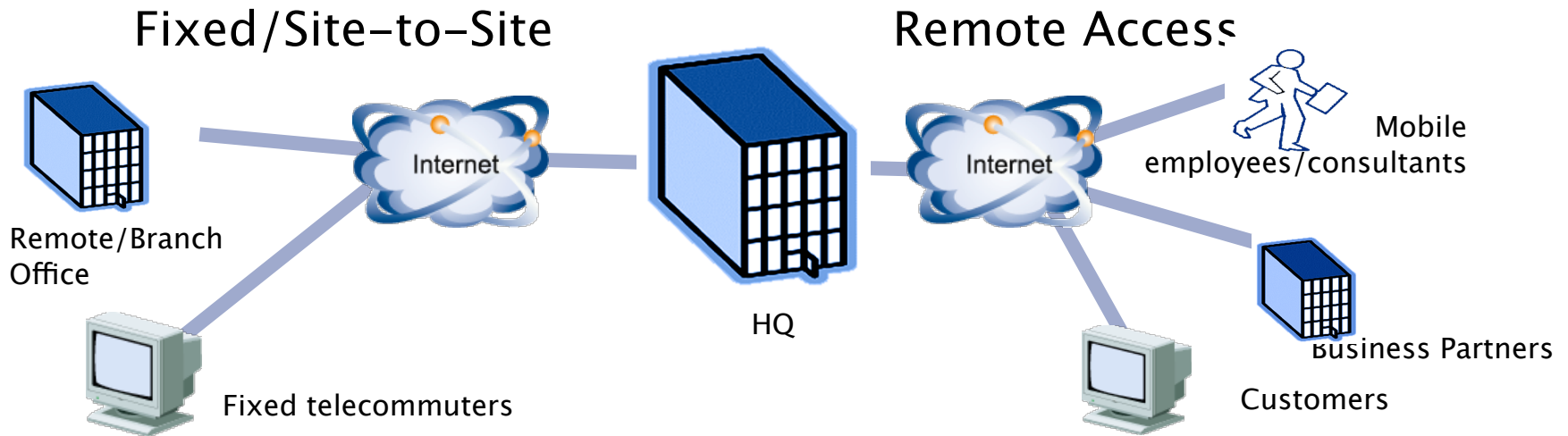
SSL VPN Value Proposition

Proof Points:

- **Clientless Deployment:** Minimal Cap Ex, Deployment, Configuration or Support Overhead; Requires No Changes to LAN/Server Resource
- **Application-Layer Security:** Controls access to only the application resource, not to native network
- **User Flexibility/ Enterprise Productivity:** Delivers secure access to users from just a Web browser



The Secure Access Landscape



Connectivity Requirements:

- Bridge fixed, “trusted” networks
- Managed devices
- Transparent access to remote LAN
- Full access to network resources
- Network-layer mgmt & administration

Options:

- Internet VPNs (IP Sec)
- Network VPNs (MPLS)

Connectivity Requirements:

- Access from “untrusted” networks
- Access from unmanaged devices

Options:

- SSL VPNs

what is needed?

Type of Application	Type of PC	Remote Network Security	Type of Connection	Type of VPN
Remote Office/ Branch Office	Corporate	Managed, Trusted	Fixed	IPSec
Mobile Employee	Corporate or Non- Corporate	Unmanaged, Untrusted	Mobile	SSL VPN
Partner/Customer	Non- Corporate	Unmanaged, Untrusted	Mobile	SSL VPN

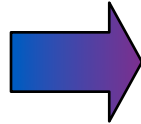
VPNs Meet Business Needs

Requirements:

IPSec VPN

Secure Access SSL VPN

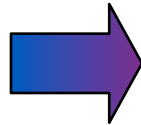
Secure



- Integrated purpose-built solution
- Integrated high performance, robust firewall (w/ Zones)

- Hardened appliance, AAA policy integration, and access privilege management

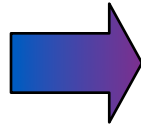
Affordable



- Route-based VPNs offer low TCO for site-to-site or fixed configurations

- No client or server changes
- Low TCO for remote/mobile employees, partners and customers

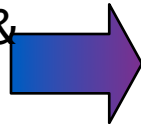
Ease of use



- Dynamic Route-Based VPNs leverage "self-healing" capabilities
- Centralized management

- Simple Web interface
- Centralized management for administrators

High Performance & Availability



- Resiliency at device, network and VPN level

- Stateful failover an a variety of clustering options

VPN Needs

By User Type and Network

IT environment:	IPSec VPN	SSL VPN
Type of connection	Fixed connection	Transient connection
Type of device	Managed corporate device	Varying devices
Type of access	Site-to-site	Remote employee, business partner, customer
Access Controls	Robust firewall functionality	Enables access management policy enforcement

VPN Needs

By User Type and Network

User constituency:	IPSec VPN	SSL VPN
Remote office employees	X	
IT staff	X	X
Mobile employees		X
Day extenders		X
Consultants		X
Customers		X
Business partners		X

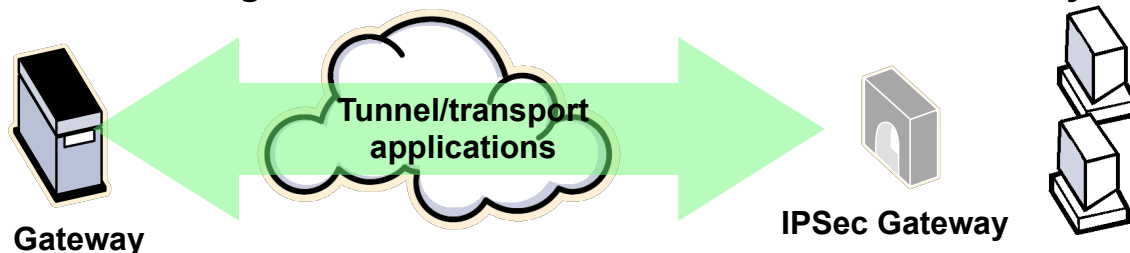
VPN Needs

By User Type and Network

Applications and content:	IPSec VPN	SSL VPN
Voice Over IP	X	
Entire subnets with no application access control required	X	
Networks, including intranets and extranets, that require access control		X
Web applications	X	X
Client/server applications	X	X
Intranet content	X	X
Email	X	X
File Servers	X	X
Server socket dependent applications	X	X

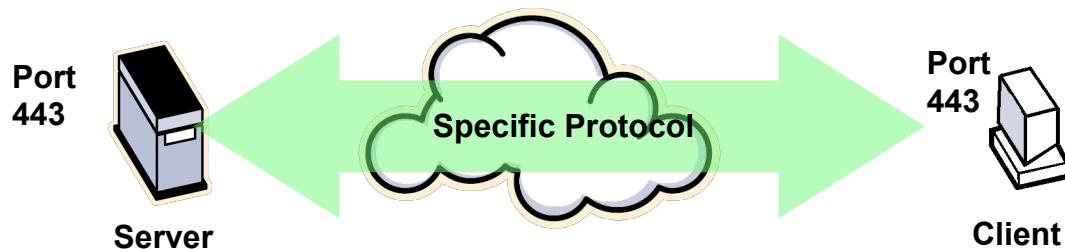
IPSec and SSL

IPSec Design Goal – low level secure network connectivity



- Network layer connection
- IPSec encryption
- Any TCP ports flow over tunnel
- Usually done with a hardware gateway on the LAN and a hardware or software client

SSL Design Goal – Secure application-to-application connectivity



- Application layer connection
- SSL or TLS encryption
- Specific port is open (easier to secure)
- Usually done in application software (included with all standard Web browsers and e-mail applications)

THANK YOU!



Juniper your Net™