IPSec or SSL VPN?
The Extended Enterprise

- Fixed Telecommuters
- Mobile Workers
- Branch Offices
- Day Extenders
- Customers
- Business Partners
- Data Center
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
IPSec and SSL VPNs
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

- Dial Networks
- Virtual Private Networks
- Custom Extranets
- Secure, Point-to-Point Communications
- SSL VPNs
- Leverage Low-Cost Internet Transport
- Broadened Application Access
- Increased Security & Client Transparency
- Client & LAN Transparency

Time
### IPSec VPN vs SSL VPN

#### Application Type
- Remote, Branch Office
- Site to site

#### Type of Connection
- Fixed

#### Remote Network Security
- Managed, Trusted

---

### Managed, Trusted Remote Network Security

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

- **Remote Network Security**
  - Managed or Unmanaged, Trusted or Untrusted

- **Type of Connection**
  - Mobile or Fixed
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

**Fixed/Site-to-Site**

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

**Remote Access**

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

**Options**

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

---

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)
what is needed?

<table>
<thead>
<tr>
<th>Type of Application</th>
<th>Type of PC</th>
<th>Remote Network Security</th>
<th>Type of Connection</th>
<th>Type of VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Office/Branch Office</td>
<td>Corporate</td>
<td>Managed, Trusted</td>
<td>Fixed</td>
<td>IPSec</td>
</tr>
<tr>
<td>Mobile Employee</td>
<td>Corporate or Non-Corporate</td>
<td>Unmanaged, Untrusted</td>
<td>Mobile</td>
<td>SSL VPN</td>
</tr>
<tr>
<td>Partner/Customer</td>
<td>Non-Corporate</td>
<td>Unmanaged, Untrusted</td>
<td>Mobile</td>
<td>SSL VPN</td>
</tr>
</tbody>
</table>
### VPNs Meet Business Needs

<table>
<thead>
<tr>
<th>Requirements:</th>
<th>IPSec VPN</th>
<th>Secure Access SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>• Integrated purpose-built solution • Integrated high performance, robust firewall (w/ Zones)</td>
<td>• Hardened appliance, AAA policy integration, and access privilege management</td>
</tr>
<tr>
<td>Affordable</td>
<td>• Route-based VPNs offer low TCO for site-to-site or fixed configurations</td>
<td>• No client or server changes • Low TCO for remote/mobile employees, partners and customers</td>
</tr>
<tr>
<td>Ease of use</td>
<td>• Dynamic Route-Based VPNs leverage &quot;self-healing&quot; capabilities • Centralized management</td>
<td>• Simple Web interface • Centralized management for administrators</td>
</tr>
<tr>
<td>High Performance &amp; Availability</td>
<td>• Resiliency at device, network and VPN level</td>
<td>• Stateful failover an a variety of clustering options</td>
</tr>
</tbody>
</table>
# VPN Needs

## By User Type and Network

<table>
<thead>
<tr>
<th>IT environment:</th>
<th>IPSec VPN</th>
<th>SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of connection</td>
<td>Fixed connection</td>
<td>Transient connection</td>
</tr>
<tr>
<td>Type of device</td>
<td>Managed corporate device</td>
<td>Varying devices</td>
</tr>
<tr>
<td>Type of access</td>
<td>Site-to-site</td>
<td>Remote employee, business partner, customer</td>
</tr>
<tr>
<td>Access Controls</td>
<td>Robust firewall functionality</td>
<td>Enables access management policy enforcement</td>
</tr>
</tbody>
</table>
# VPN Needs

By User Type and Network

<table>
<thead>
<tr>
<th>User constituency:</th>
<th>IPSec VPN</th>
<th>SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote office employees</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IT staff</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mobile employees</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Day extenders</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Consultants</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Customers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Business partners</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## VPN Needs
### By User Type and Network

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