

**Nowocześnie i bezpiecznie – zdalny
dostęp do zasobów firmowych z
wykorzystaniem rozwiązań SSL VPN
firmy Juniper Networks**

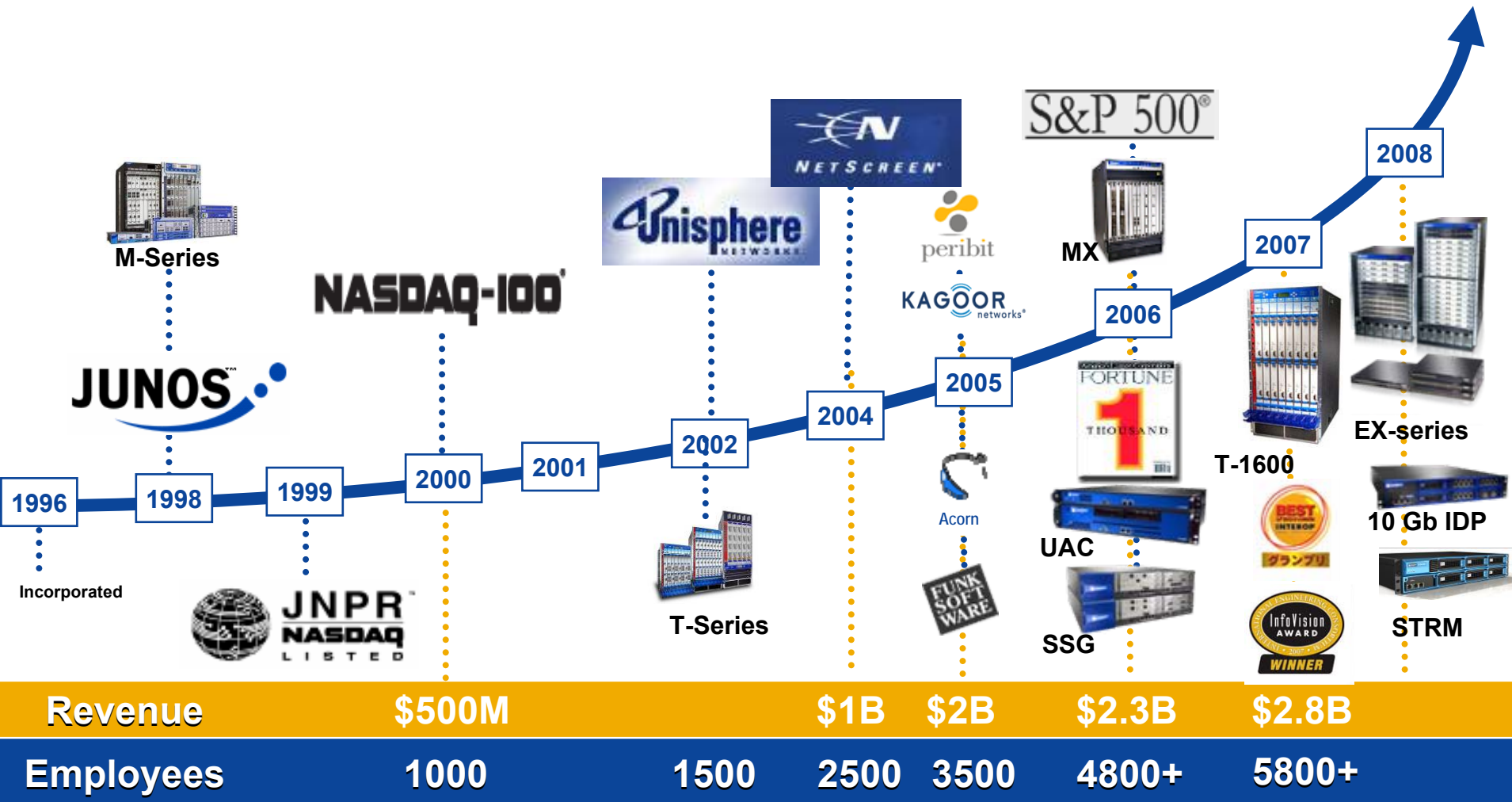
Piotr Kędra
pkedra@juniper.net

Agenda

- **Few words about Juniper**
- **SSL VPN Use Cases**
- **Access Control & AAA**
- **End-to-End Security**
- **Secure Meeting**
- **Hardware, Management and High Availability**



More Than A Decade of Innovation



Juniper's Portfolio Breadth



Routing

Deliver high levels of security, uptime and performance with simplified operations in converged IP and IP/MPLS infrastructures through professional-grade routers based on the advanced, modular JUNOS OS.



Switches

The EX switches run under the JUNOS software, which provides Layer 2 and Layer 3 switching, routing, and security services. The same JUNOS code base runs on all Juniper Networks routing platforms.



Integrated Firewall/VPN

Integrated security devices with Stateful firewall and IPSec VPN, including models with integrated IDP for the Data Center and integrated Unified Threat Management at the branch office.



Secure Access SSL VPN

Eliminate the need for client access software, changes to internal servers, and costly ongoing maintenance & desktop support while providing added security through endpoint validation agents



Intrusion Detection and Prevention

Stand alone or integrated intrusion prevention with Comprehensive protection against current and emerging threats at both application and network layer. Day Zero protection against worms, Trojans, spyware, keyloggers, and other malware



UAC

Enables access control for guests, contractors and employees. Provides enforcement using any vendor's 802.1X-enabled infrastructure, existing Juniper firewalls or both



WAN Acceleration

Provide a scalable approach to accelerating application performance, increasing WAN capacity, and enabling application prioritization and visibility in speeds from 64 Kbps to 155 Mbps



Management

Common management system (NSM, NSMXpress); Log Management and SIEM (Security Information and Event Management) system (STRM)



Customer Challenges: Access vs. Security

Maximize Productivity

- Partner access to web applications (Partner Extranet)
- Increased employee productivity (Intranet portals, ERP)
- Customized experience and access for diverse user groups
- Enable provisional worker (Contractor, off-shoring)
- Support myriad devices (PDA, laptop, kiosk)
- Anywhere access (home, airport, hotel room)

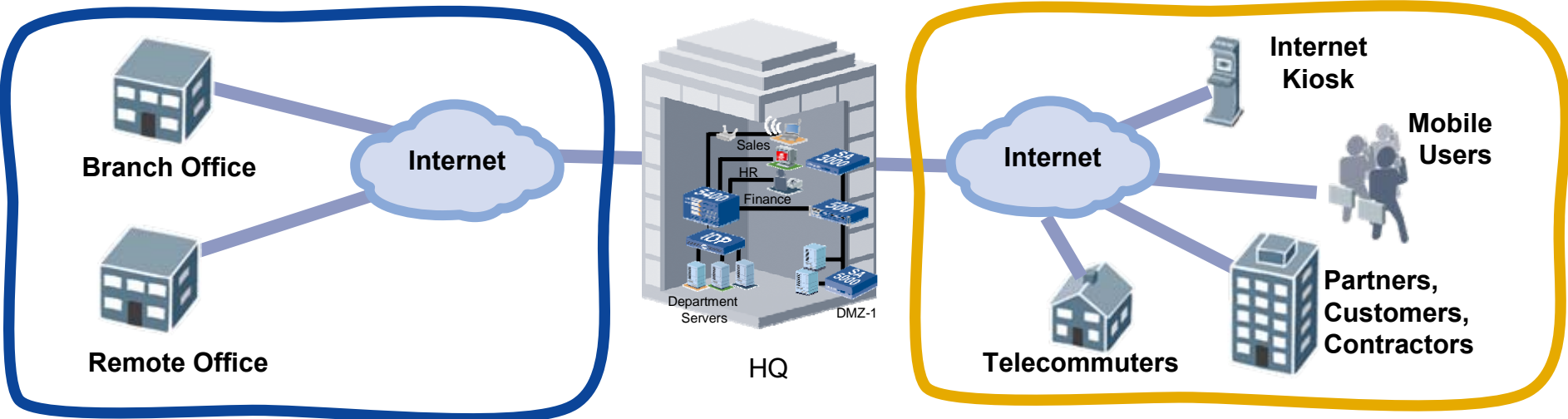
Enforce Strict Security

- Allow access only to necessary applications and resources
- Mitigate risks from unmanaged sources (i.e. kiosks, non-employees)
- Apply consistent security policy

Return on Investment

- Capital Expense
- Ongoing administration and support

IPSec VPN vs. SSL VPN



Application Type	Remote/Branch Office
Type of Connection	Fixed Site-to-Site
Type of Endpoint Device	Managed
VPN Type	IPSec VPN
Access Requirement	Network Access
Control Requirement	IP to IP control
Remote Network Security	Managed, Trusted

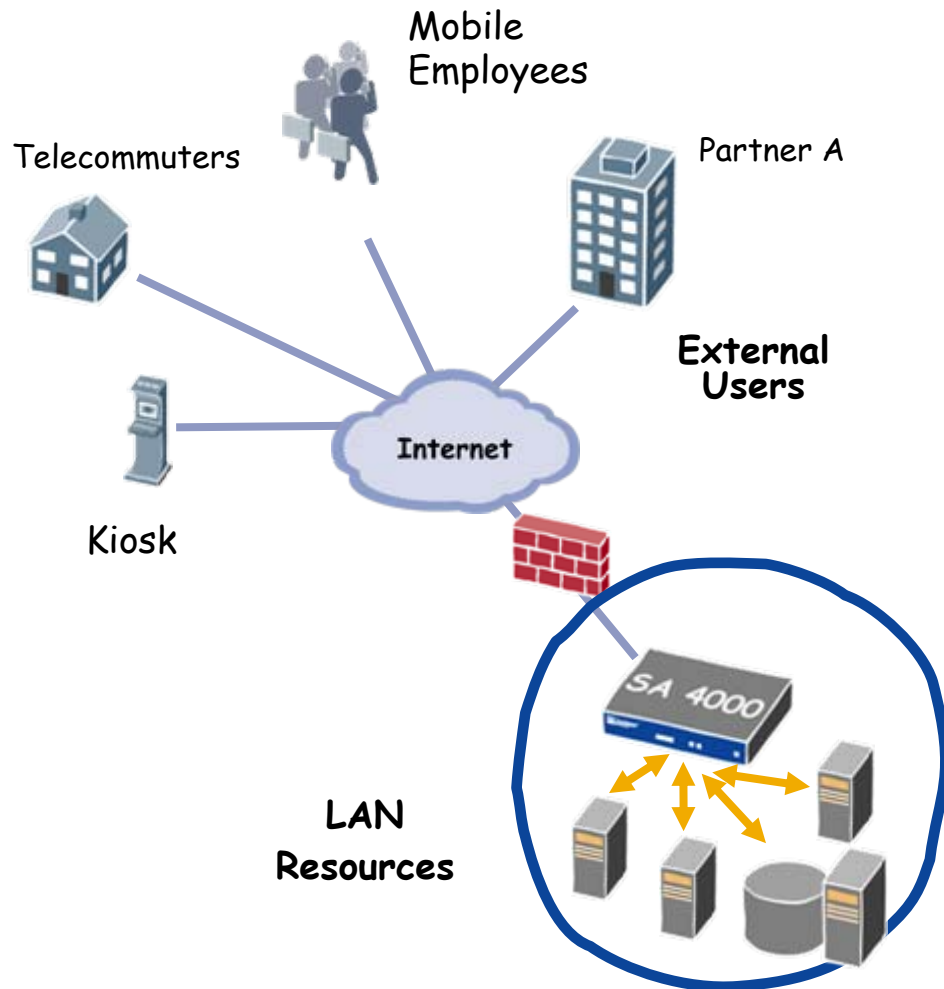
Application Type	Employee Remote Access, Telecommuter, Mobile User, Partner Extranet and Network access
Type of Connection	Mobile or Fixed
Type of Endpoint Device	Managed, Unmanaged
VPN Type	SSL VPN
Access Requirement	Per Application Access
Control Requirement	User to Application control
Remote Network Security	Unmanaged, Untrusted



Secure Access SSL VPN enables secure, fast, anytime access to applications and files from a Web browser

Proof Points:

- **Clientless Deployment:** Minimal Cap Ex, Support Overhead; Requires No Changes to LAN/Server Resource
- **Application-Layer Security:** Mitigates hacking and viruses, management down to file level, controlled access
- **User Flexibility/Enterprise Productivity:** Delivers secure access to users from just a Web browser, grant access to partners, consultants, contractors, etc.



IPSec VPNs vs. SSL VPNs

■ IPSec VPNs

- Good solution for a contained number of trusted users accessing corporate resources from managed corporate devices
- Ideal for fixed site-to-site connections where “always on” experience is essential

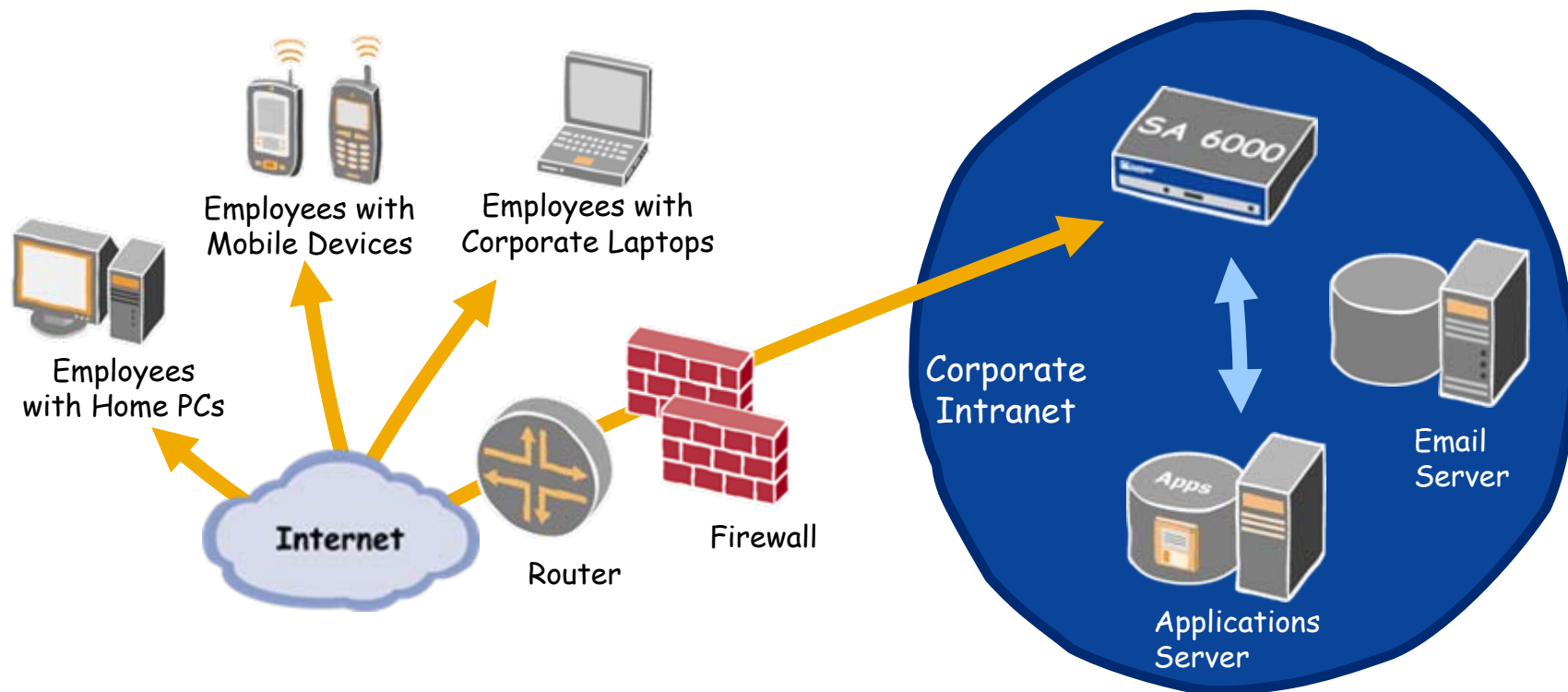
■ SSL VPNs

- Good solution for managing untrusted and trusted users:
 - From different locations (**home, airport, hotel**)
 - Using various managed or unmanaged devices (**corporate laptop, home PC, kiosk, PDA, mobile phone**)
 - That are diverse audiences (**employee, contractor, partner, customer**)



- Ideal for providing secure remote access to corporate resources from any Web-enabled device and from anywhere

Use Case #1 - Employee Remote Access



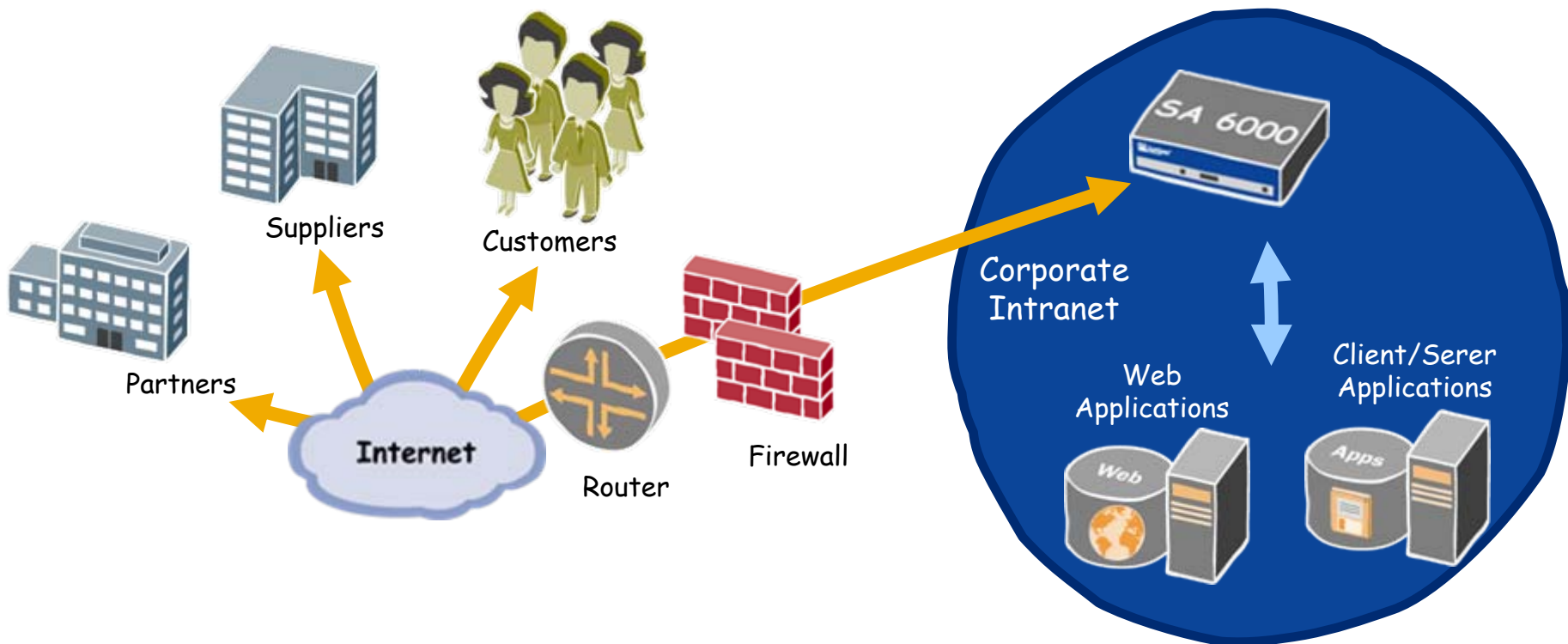
SSL VPN Ease of Use

- Anytime, anywhere access from home PC, corporate laptop, mobile phone, or kiosk
- No software to install, configure, or maintain
- Only Web-browser & Internet connection needed

Increased Security with SSL VPN

- Encrypted and authenticated access
- Restrict users' access to specific applications & resources
- Comprehensive security checks on endpoints before granting access

Use Case #2 - Extranet Portal



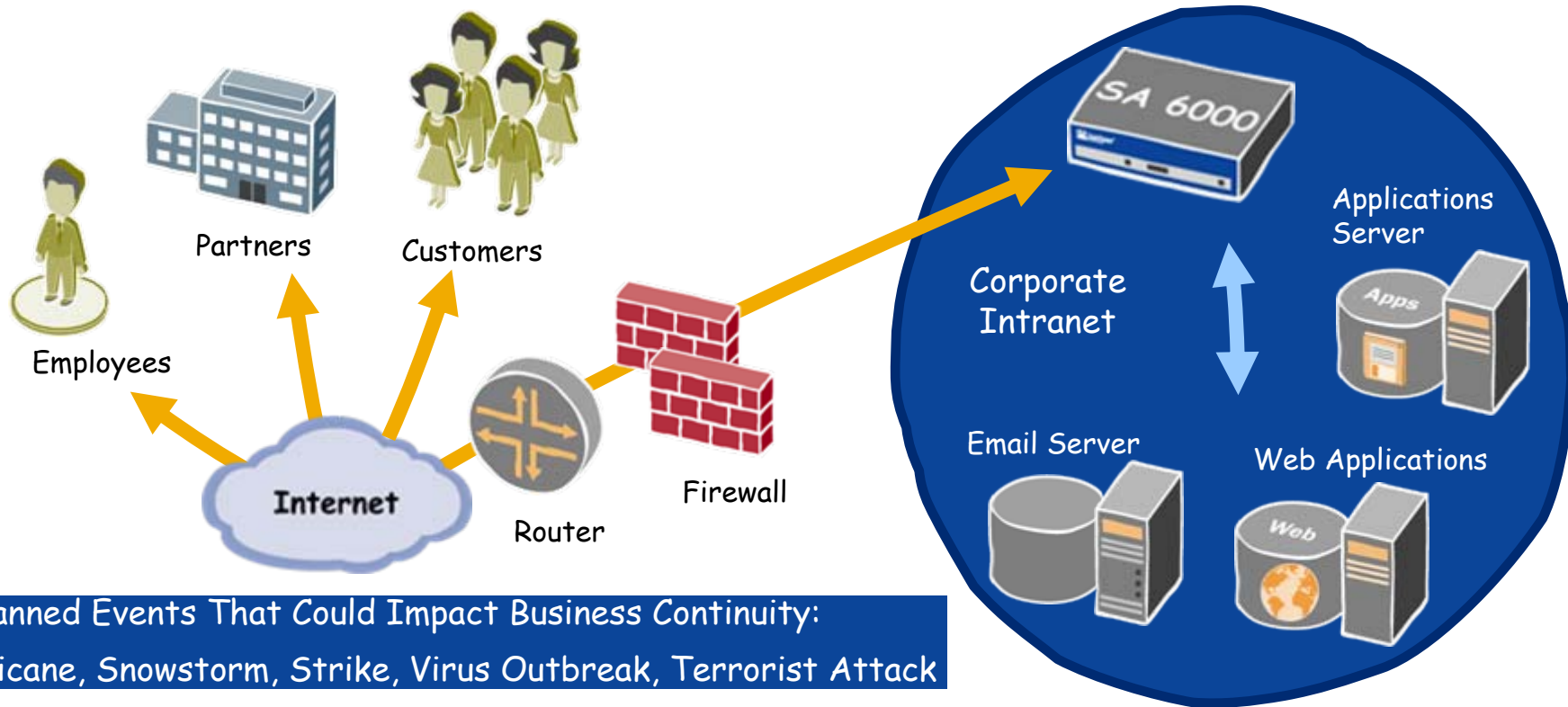
Flexibility with SSL VPN

- Rapidly add/drop access to partners, suppliers, & customers
- No client software required on devices
- Access from any Web-enabled device

SSL VPN Management

- Limit access to select applications or resources
- Ensure corporate security policy is met before granting access
- No need to maintain or configure users' devices

Use Case #3 - Disaster Recovery



Unplanned Events That Could Impact Business Continuity:
Hurricane, Snowstorm, Strike, Virus Outbreak, Terrorist Attack

Remain Operational with SSL VPN

- Meet peak in remote access demand during emergency
- Instant activation for increased demand
- Sustain access for partners and customers

Maintain Productivity with SSL VPN

- Enable users to work from home or any location
- Allow access from any Web-enabled device
- Assure employees' safety & minimize downtime at the same time



Unplanned Events - Impacting the Global Business

Disastrous Events

Pandemic

Avian/Bird Flu
SARS

Natural

Earthquakes
Hurricanes

Other

Terror attacks
Winter Storms

Social Distancing

Geographical isolation
Quarantines

Business Continuity Challenges

- Maintain **productivity**
- Sustain **partnerships**
- Continue to deliver exceptional service to customers and partners with **online collaboration**
- Meet **government mandates** for Disaster Recovery and compliance

Hurricane Katrina (Aug 05)
Hurricane Stan- S.A. (Oct 05)

Seamless AAA Integration

- **Full Integration into customer AAA infrastructure**
 - AD, LDAP, RADIUS, Certificate, OTP, etc.
- **Password Management Integration**
 - User self service for password management
 - Reduced support costs, increased productivity
 - All standard LDAP, MSFT AD
- **Single Sign-On – Native Capabilities**
 - Leveraged across all web apps → seamless user experience
 - Forms, Header, SAML, Cookie, Basic Auth, NTLM
- **SAML Support – Web single sign-on, integration with I&AM platforms**
 - Standards-based Web SSO
 - Partnerships with leading AM Vendors (CA, Oracle, RSA, etc.)

Provision by Purpose

Three Different Access Methods to Control Users' Access to Resources

Dynamic Access Control based on User, Device, Network, etc.

<u>Network Connect</u>	<u>Secure Application Manager (SAM)</u>	<u>Core Access</u>
<ul style="list-style-type: none"> - IPSec-like experience with full network layer tunnel - Supports all client applications & resource intensive applications like VoIP & streaming media - Recommended for remote and mobile employees only as full network access is granted 	<ul style="list-style-type: none"> - Access to client/server applications such as Windows & Java applications - One click access to applications such as Citrix, Microsoft Outlook, and Lotus Notes - Ideal for remote & mobile employees and partners if they have application software loaded on their PCs 	<ul style="list-style-type: none"> - Access to Web-based applications, file shares, Telnet/SSH hosted apps, and Outlook Web Access - Granular access control all the way up to the URL or file level - Ideal for most users to access from any device on any network (corporate laptop, home PC customer or partner PC, kiosk, PDA, etc.)



LAN-like L3 access to Client/Server and web apps with Network Connect

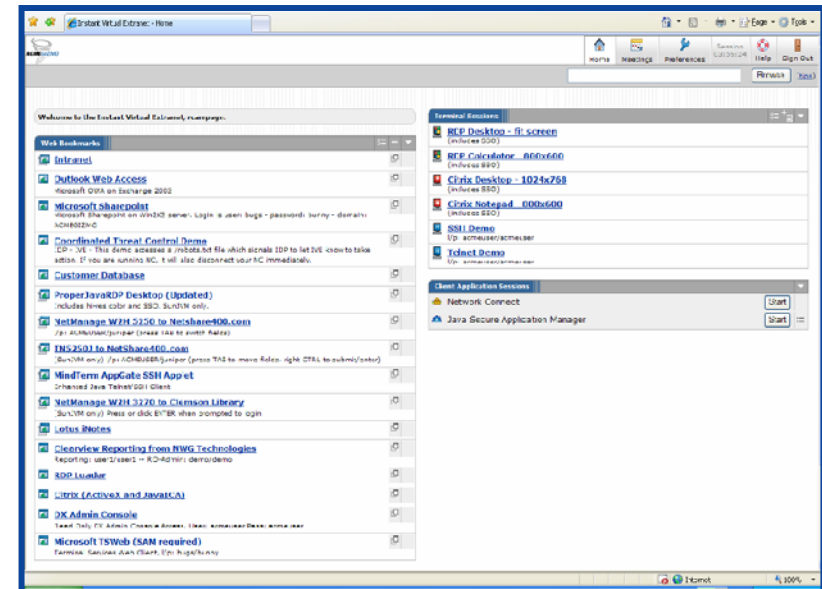
Granular client/server application access control with Secure Application Manager

Granular web application access control with Core Access method

Access Methods (Application & Resources)

- Core Access -

- Full cross platform/browser support
- Secure Web Application Access
 - Support for widest range of web-based content and applications
 - Sharepoint, OWA, iNotes, PDF, Flash, Java applets, HTML, Javascript, DHTML, VBScript, XML, etc.
 - Host & deliver any Java applet
- Secure File Share Access
 - Web front-end for Windows and Unix Files (CIFS/NFS)
- Integrated E-mail Client
- Secure Terminal Access
 - Access to Telnet/SSH (VT100, VT320...)
 - Anywhere access with no terminal emulation client



Access Methods (Application & Resources)

- Terminal Services -

- **Seamlessly and securely access any Citrix or Windows Terminal Services deployment**
 - Intermediate traffic via native TS support, WSAM, JSAM, Network Connect, Hosted Java Applet
- **Native TS Support**
 - Granular Use Control
 - Secure Client delivery
 - Integrated Single Sign-on
 - Java RDP/JICA Fallback
 - WTS: Session Directory
 - Citrix: Auto-client reconnect/session reliability
 - Many additional reliability, usability, access control options

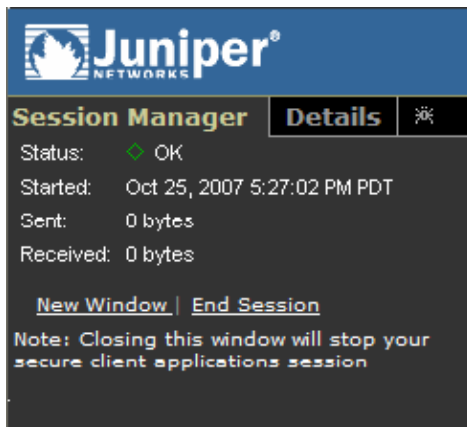


Terminal Sessions	
 RDP Desktop - fit screen (includes SSO)	
 RDP Calculator - 800x600 (includes SSO)	
 Citrix Desktop - 1024x768 (includes SSO)	
 Citrix Notepad - 800x600 (includes SSO)	
 SSH Demo l/p: acmeuser/acmeuser	
 Telnet Demo l/p: acmeuser/acmeuser	

Access Methods (Application & Resources)

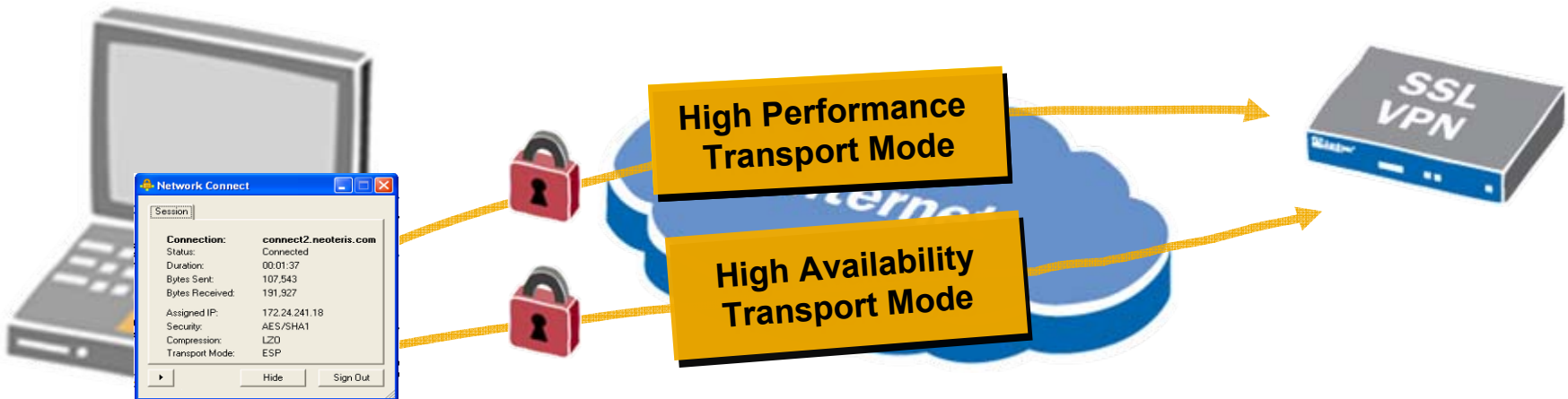
- Secure Application Manager -

- **Full cross platform support; Windows + Java versions**
- **Granular control – users access specific client/server applications**
 - Access C/S applications without provisioning full Layer 3 tunnel
 - Eliminates costs, complexity, and security risks associated with VPNs
 - No incremental software/hardware or customization to existing apps
- **WSAM – secure traffic to specific client/server applications**
 - Supports Windows Mobile/PPC, in addition to full Windows platforms
 - Granular access and auditing/logging capabilities
 - Installer Service available for constrained user privilege machines
- **JSAM – supports static TCP port client/server applications**
 - Enhanced support for MSFT MAPI, Lotus Notes, Citrix NFuse
 - Drive mapping through NetBIOS support
 - Install without advanced user privileges



Access Methods (Application & Resources)

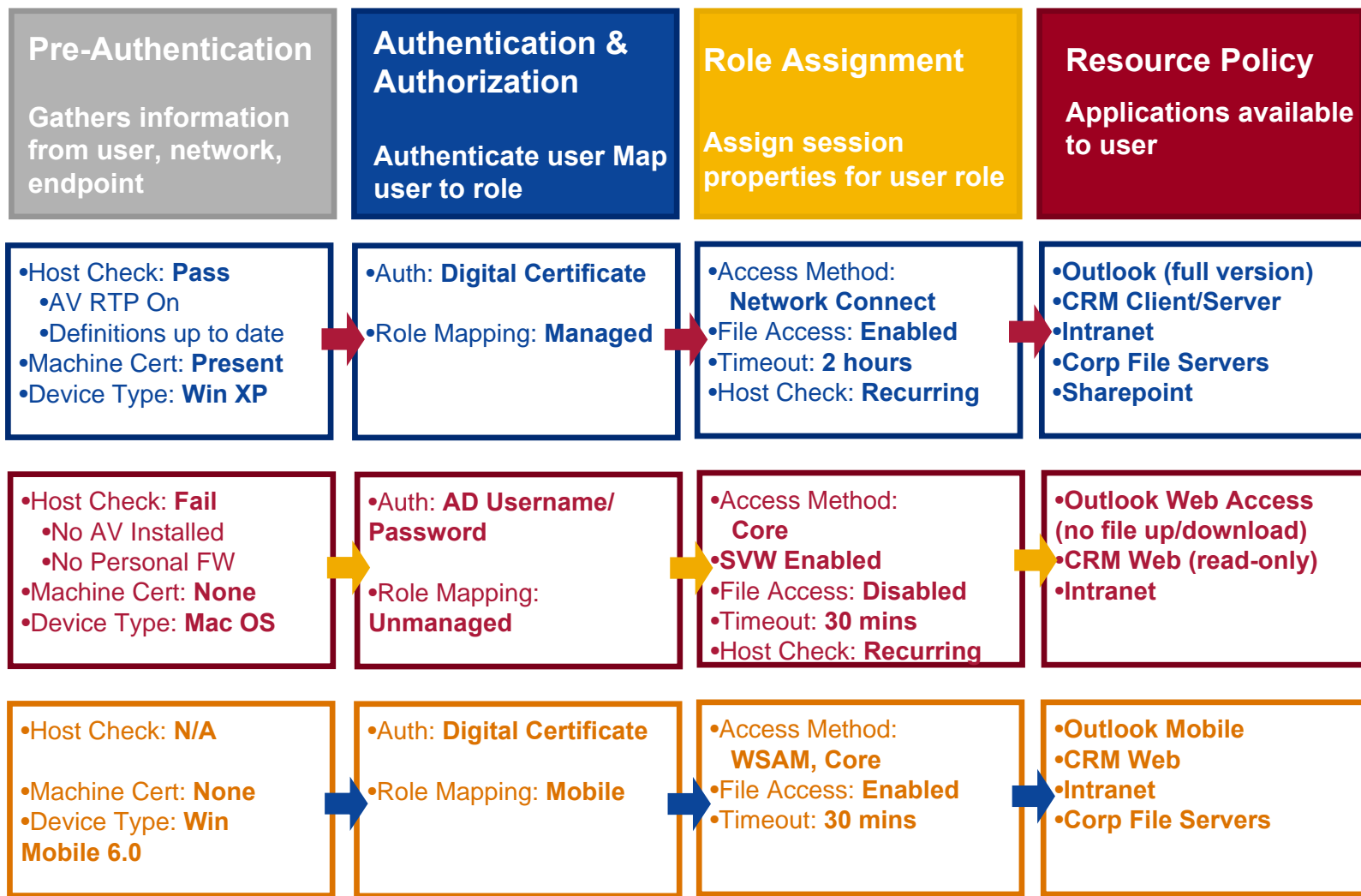
- Network Connect -



- **Full Layer 3 Access, similar to IPSec VPN**
- **Adaptive, Dual Transport Mode**
 - Initially attempts to set up high performance, IPSec transport
 - If blocked by network, seamlessly fails over to SSL
- **Cross Platform Dynamic Download (A|X or Java delivery)**
- **Range of options – browser launch, standalone EXE, scriptable launcher, MSFT Gina**
- **Client-side Logging, Auditing and Diagnostics**

Access Privilege Management – 1 URL

Same person access from 3 different locations



One Device for Multiple Groups

Customize policies and user experience for diverse users

partners.company.com



Welcome to the
Partner Extranet Site

Username Please sign in to begin your session

Password

employees.company.com



Welcome to the Employee & Contractor
Intranet Access Gateway

Username Please sign-in with your credentials

Password

Realm

customers.company.com



Welcome
WidgetsRU's Customers

Username Please sign in to access your account

Password

Realm



“Partner” Role

Authentication	Username/Password
Host Check	Enabled – Any AV, PFW
Access	Core Clientless
Applications	MRP, Quote Tool

“Employee” Role

Authentication	OTP or Certificate
Host Check	Enabled – Any AV, PFW
Access	Core + Network Connect
Applications	L3 Access to Apps

“Customer” Role

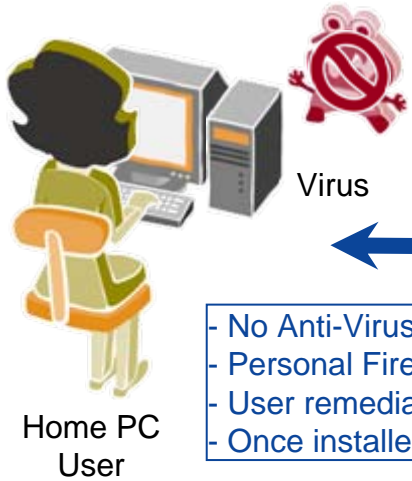
Authentication	Username/Password
Host Check	Enabled – Any AV, PFW
Access	Core Clientless
Applications	Support Portal, Docs

End-Point Security

- Host Checker -

Host Checker

- Check devices before & during session
- Ensure device compliance with corporate policy
- Remediate devices when needed
- Cross platform support



- No Anti-Virus Installed
- Personal Firewall enabled
- User remediated → install anti-virus
- Once installed, user granted access



- No anti-virus installed
- No personal firewall
- User granted minimal access



- AV Real-Time Protection running
- Personal Firewall Enabled
- Virus Definitions Up To Date
- User granted full access



End-Point Security

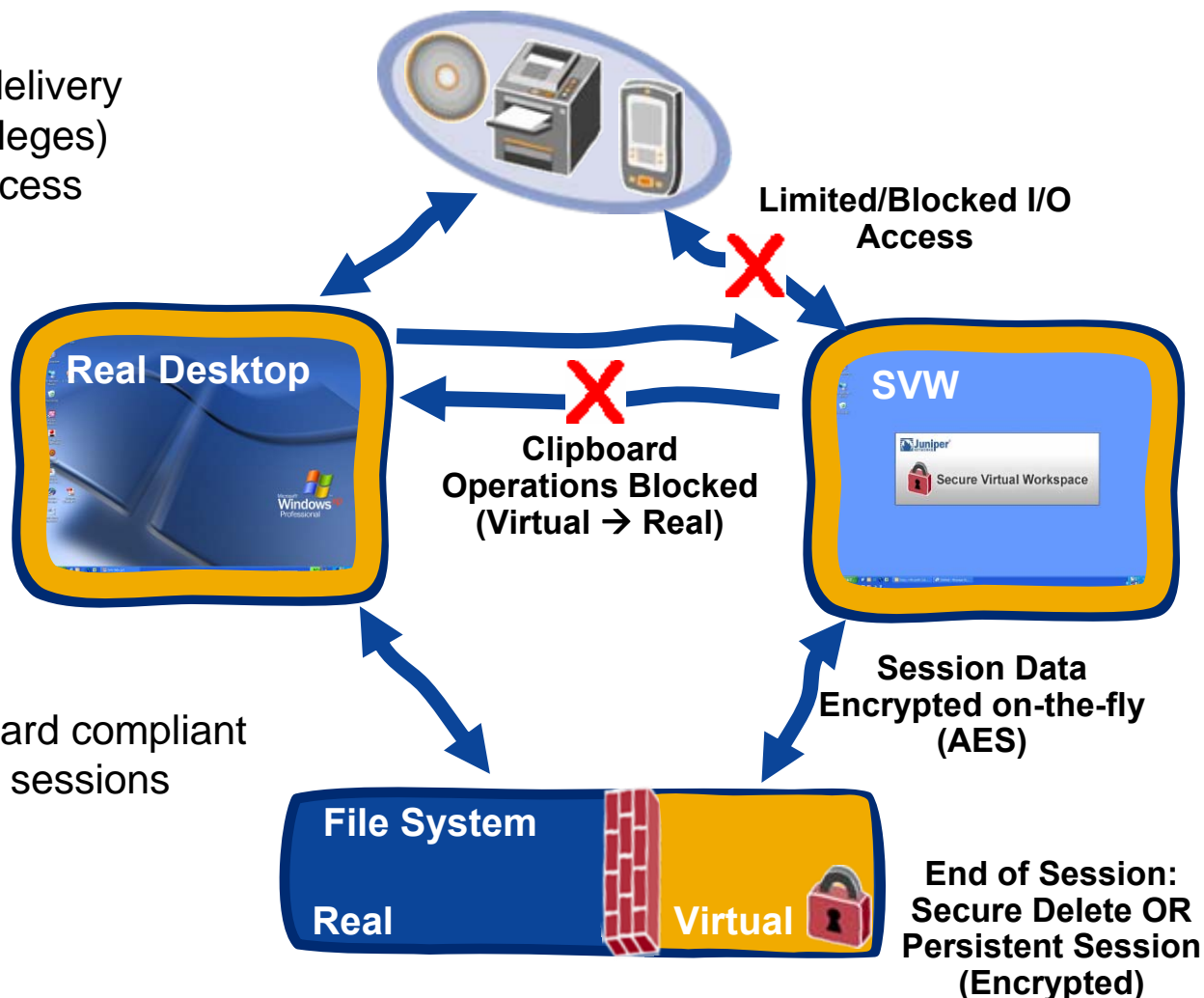
- Host Checker -

- **Point-and-click policy configuration with support for hundreds of leading applications**
 - AV, Personal Firewall, Anti-Spyware, Anti-Malware + Custom policy definition for maximum policy definition flexibility.
 - Scan prior to and during authenticated sessions
 - Embedded update mechanism to add new applications with no software upgrade
 - Devices automatically learn latest signature versions from AV vendors
 - Check for AV installation, real-time protection status, definition file age
- **Varied remediation options to meet customer needs**
 - Custom/standard remediation, quarantine, Secure Virtual Workspace, 3rd party policy remediation, etc.
- **Trusted Network Connect (TNC) architecture for seamless integration with all TNC compliant endpoint security products/vendors**
 - Leverage existing endpoint security application deployments
- **HC policies similar to Juniper's UAC offering, for common endpoint security across local and remote access deployments**

Endpoint Security

- Secure Virtual Workspace -

- Host Checker (Java/ActiveX) delivery
- Win 2k/XP Systems (user privileges)
- Admin-specified application access

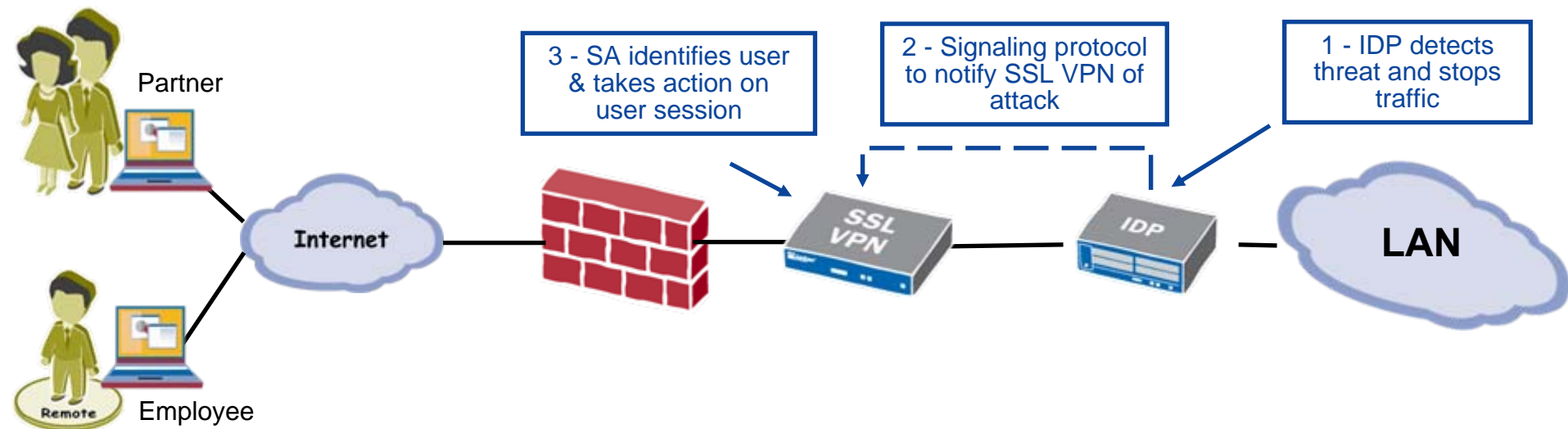


- DoD Cleaning/Sanitizing standard compliant
- Password-protected persistent sessions
- Controlled I/O Access
- Configurable look/feel

System Security

- **“Security First” approach to development**
 - Hardened OS based on Linux variant
 - Protection against many known attacks
 - AES encrypted hard disk on every appliance
- **In-Transit Data Protection**
 - Data trapping
 - URL obfuscation
- **Numerous 3rd party security audits**
- **Juniper Security Incident Response Team (SIRT) to quickly investigate any potential vulnerabilities**

Juniper's Coordinated Threat Control



Correlated Threat Information

- Identity
- Endpoint
- Access history
- Detailed traffic & threat information

Coordinated Identity-Based Threat Response

- Manual or automatic response
- Response options:
 - Terminate session
 - Disable user account
 - Quarantine user
- Supplements IDP threat prevention

Comprehensive Threat Detection and Prevention

- Ability to detect and prevent malicious traffic
- Full layer 2-7 visibility into all traffic
- True end-to-end security

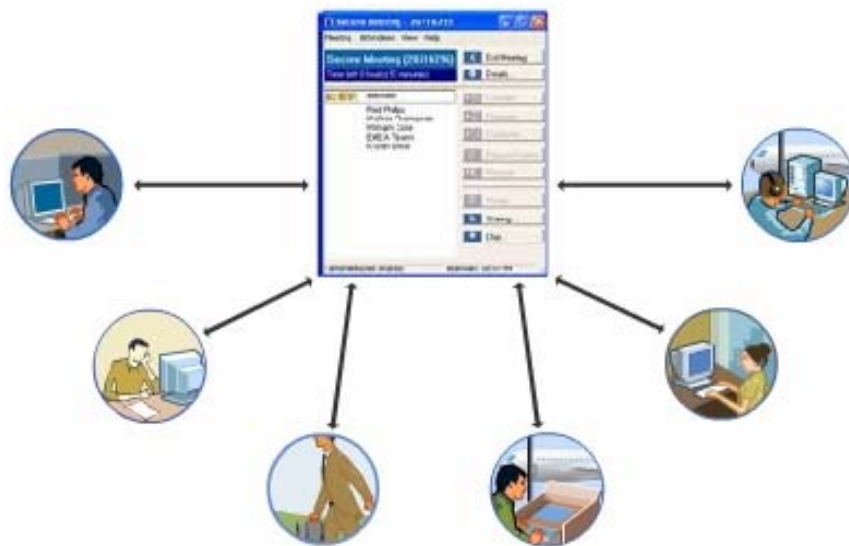
Secure Meeting

Instant Online Collaboration

- Secure Meeting -

- **Easy to Use Web Conferencing**
 - Share desktop/applications
 - Group and private chat
 - No training required
- **Easy to Deploy and Maintain**
 - No pre-installed software required
 - Web-based, cross platform
 - Personalized meeting URLs for users
 - <https://meeting.company.com/johndoe>
- **Affordable – No usage/service fees**
- **Secure**
 - Fully encrypted/secured traffic using SSL
 - No peer-to-peer backdoor
 - User credentials protected
 - Policy flexibility to meet authentication requirements

Instant or scheduled online collaboration



Remote Helpdesk Functionality

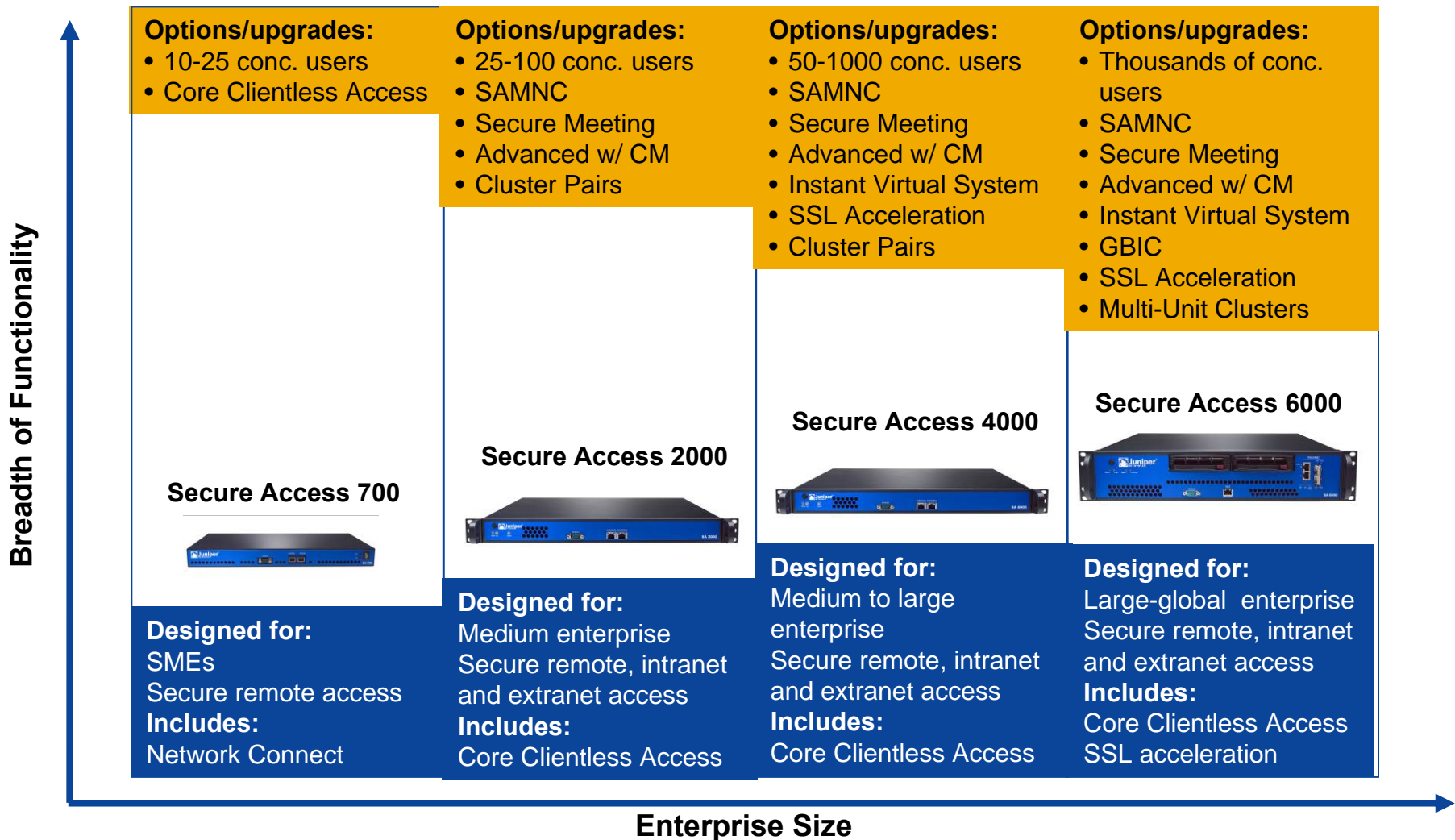
- *Secure Meeting* -

- **Reduce desktop/application support costs by speeding time to issue resolution**
 - Significant cost savings over phone-based troubleshooting
 - Improve helpdesk/technician productivity
- **Fast, easy setup with automatic setting configuration:**
 - Dynamic client delivery, cross-platform support
 - Automatic desktop sharing/remote control request
 - Secure Chatting disabled



Juniper SSL VPN Product Family

Functionality and Scalability to Meet Customer Needs



Introducing the Next Generation of Market-Leading SSL VPN Platforms

- **Secure Access 2500**



- **Secure Access 4500**



- **Secure Access 6500**



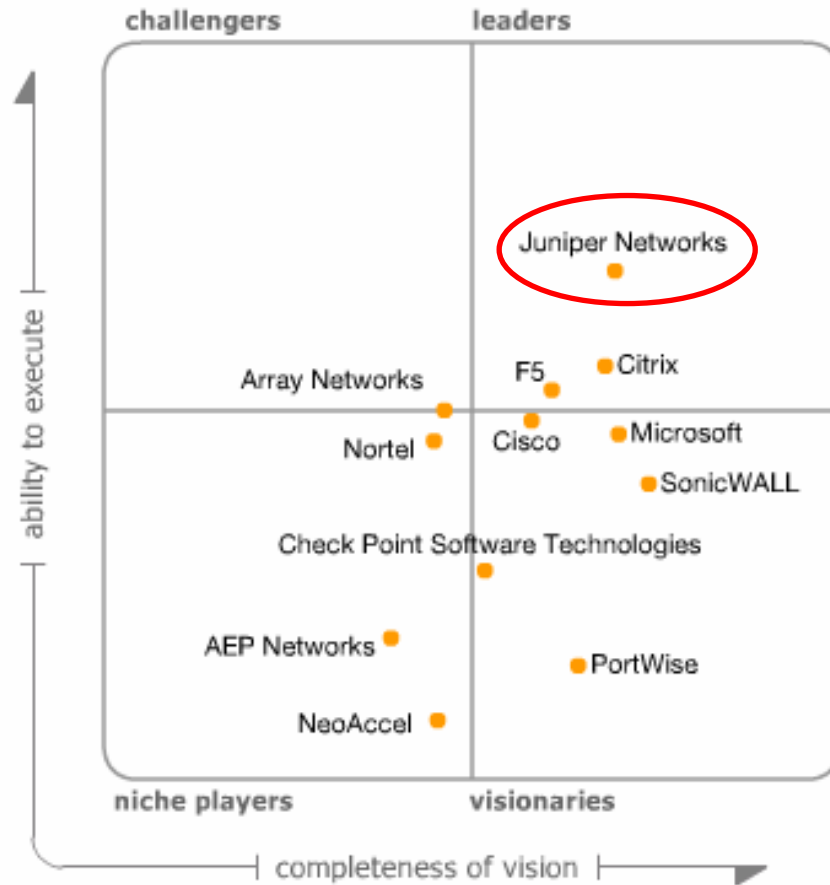
Why Juniper for SSL VPN?

- **Core Competence in SSL-based Access**
 - Proven in tens of thousands of customer deployments!
 - Market Leadership/Industry Awards
 - Product Maturity
- **Performance, Scalability & HA**
 - Differentiated hardware platforms
 - Global & local stateful clustering
 - Compression, SSL acceleration, GBIC connectors, Dual hot-swappable hard disks, power supplies, and fans
- **Single Platform for All Enterprise Remote Access Needs**
 - Support for complex Web content, Files, Telnet/SSH using only a browser
 - Client/Server applications
 - Adaptive dual transport method for network-layer access
- **Ease of Administration**
 - Centralized Management
 - Granular Role-based Delegation
 - Extensive integration with existing directories
 - Native endpoint remediation and password management integration
- **End-to-End Security**
 - Robust host checking capabilities
 - Dynamic Access Privilege Management
 - 3rd party security audits



Analyst Praise & Recognition

Gartner Magic Quadrant for SSL VPN, North America, 3Q07



As of November 2007

Full report can be found at <http://www.juniper.net/company/presscenter/awards/recognition.html>

Source: Gartner (November 2007)



Juniper *your* Net™