Having Your Cake and…

Remote Access Security:
Finding Balance in the Real World

Tim Newell, Bell Aliant
MSc, CISSP, ISSAP, GCIA, GCIH

Overview

- Intro
- Dynamics of Remote Access
- Security Threats
- Mitigation Strategies
- Case Study

Dynamics of Remote Access

- Conflict – Function vs Security vs Cost
  - Typical order of priorities in this region:
    1. Cost
    2. Function
    3. Security
- I've found my approach has "mellowed" accordingly
  - Find effective, affordable solutions that reduce risk to acceptable levels.
  - I used to worry about ensuring it's secure at all costs and dealing with the rest later.

Dynamics of Remote Access

- Increasing demand
  - More users
    - Users who didn't need remote access before
    - Teleworkers
    - Contingency plans – storms, pandemic, DR, etc.
    - Flexible hours, work/life balance…
  - Partners/vendors
  - More device types and locations
  - More functions to be accessed
    - ➢ Anytime, anywhere access

Dynamics of Remote Access

- Used to be “enter password and let’em in”
- Changing requirements
  - Scalable
  - Flexible
  - “Secure” – various policies, authentication, access restrictions
  - User experience simplicity
  - Easy to install / deploy
  - Multi-platform

Security Threats

- Remote access is often the Achilles Heel of corporate security
  - Why bother hacking a web site or spear phishing if you can just log in?
  - One of the most common malware vectors

Security Threats

- Three primary threat types
  - Unauthorized Access
    - Risk of letting an outsider “in”
    - Brute force, vulnerabilities, session hijack, etc.
  - Malware Infection
    - From exposed/unsecure external devices via “trusted” channel
    - Often “easiest” path in
  - Data Leakage
    - May be a consequence of the other two, but consider threat to data at rest after remote access
    - Infected remote devices
    - Home computers with file sharing / P2P apps

Mitigation - Prerequisite

- Organizations need more than in/out decisions.
- Things to look for in a remote access solution
  - A dynamic framework to implement policy
  - Support distinct user types (roles)
  - Scalable access control framework
  - Flexible authentication and endpoint security policies
  - Provide different “levels” of access – application, network
    - Application – browser-level access, various key specialized applications. Granular control and logging.
    - Network – “full” access, local arbitrary apps, etc.
  - User experience - Single Sign-On, user-specific “menus”

Mitigation - Basics

- Start with basic policy and strategy
  - What do you need to protect?
  - Are there any existing security requirements? (Policies, Compliance, …)
  - What kinds of usage scenarios do you have?
    - Who are your users?
    - What do they need access to?
    - Will you allow non-corporate devices to connect?
      - Under what circumstances?
      - Any specific requirements or restrictions?
  - What is your access control model?
    - Does everyone have the same access?
    - Application level access, network level, or both?
    - How far do / can you go with “least privilege” access?
      - This can drive a lot of complexity and support effort if it gets out of control.

Mitigation – Unauthorized Access

- Passwords are next to useless
  - Only as good as your weakest password – people are predictable
  - Complexity?
    - "Passw0rd!" anybody?
  - Account lockout?
    - Helps – but "invert" attack to use password and sweep accounts
  - Automated attacks are trivial
  - Keep honest people honest, implement "perception" of security
- Need to use two-factor authentication
  - Certificates
    - Good: user experience, maybe no physical device
    - Bad: installation / portability, ad-hoc access, compromised devices?
  - Tokens
    - Good: portable, device compromise not a major concern
    - Bad: physical device, provisioning / replacement, user experience
  - Pick your poison…

Mitigation – Unauthorized Access

- Access Control
  - Key security tool
  - Reduce the attack surface exposed to remote users
  - Mitigate some risk of unintended access
  - “Contain the damage” if initial access gained
  - Beware of “jump-off” attacks / consequences
    - Can attacker go A -> B, then B -> C?
  - Reality
    - Relatively open access for the 80% access by employee users with corporate assets
    - Apply tighter access control to the remaining 20%
      - Non-corporate assets
      - Third party access

Mitigation - Malware

- Limit the attack surface
  - Application versus Network level access
  - Access Control
- Largely a matter of determining / reducing risk – validate confidence in connecting device
  - How likely is it that device X is vulnerable?
    - Managed / Corporate device or not
    - AV present? Up to date? Date of last scan?
- Some on-demand dynamic AV scanners available
  - Don't seem to be widely used
  - Simpler to focus on managed corporate versus not

Mitigation – Data Leakage

- Prevent unauthorized information disclosure
- Authentication, access control, malware protection are key elements, but…
- What if all those check out? Is there still risk?
  - Data at rest after remote access session?
  - Unmanaged (e.g. home) computers – file sharing software, malware
  - How much to trust non-managed devices?
- Keep the data off if you don't trust the device
  - Reduced or no access for untrusted device
  - Limit functions (e.g. no downloads / attachments)
  - Cache scrubbers

Mitigation – Data Leakage

- At the extreme, get into virtual / secure desktop environments
  - No access to the “real” client device while connected
  - Can’t copy files down or access outside the session
  - No printers, screenshots, CLI, system config, etc.
  - Significant user impact
  - Lots of potential hassles
  - Best suited for very specific, “closed” environments

Customer Scenario - Background

- Medium-sized customer, ~50 users
- Increasing demand for remote email access and other “basics”
- Sensitive database with marketing data, private consumer information
- Managers, Sales, and IT staff with laptops
- Sales and Managers need access to database
- IT need fairly full access for support and admin

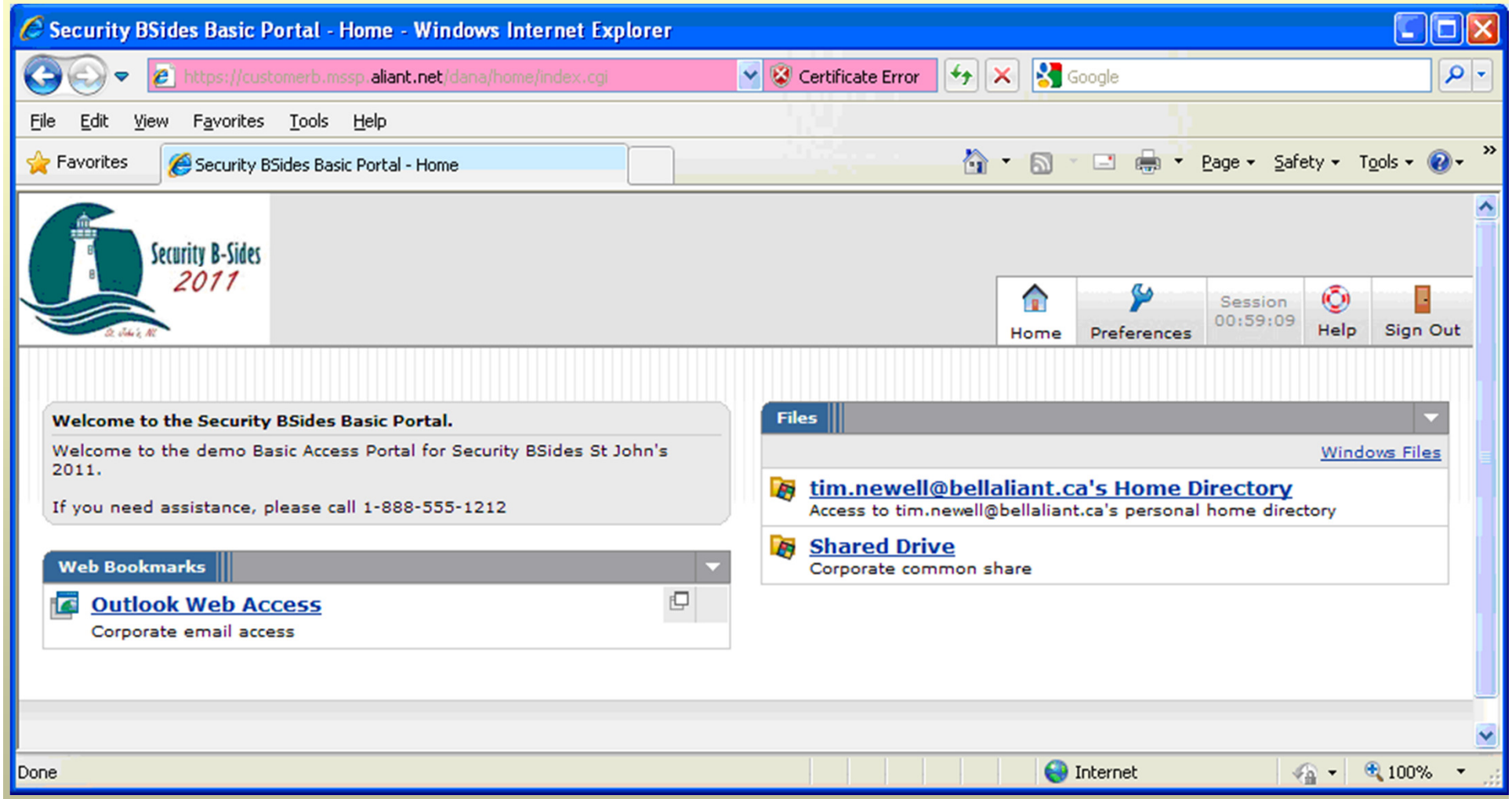
Customer Scenario - Solution

- Two tiers of access
  - Basic – lower security, minimal access
  - Full – higher security requirements, broad access
- Separate “Portal” for each
  - Link to each other for convenience
  - Different authentication and endpoint requirements

Customer Scenario - Solution

- Basic access portal – access to limited services from home or the road
  - Username/password (Active Directory)
  - Need a current, recognized AV product
  - Cache scrubber required
  - Limited to application-level, restrictive access
    - Can only access “bookmarked” menu items, ACL’s to enforce
  - Outlook Web Access, some web-based file shares
    - Single Sign-On (SSO) for convenience
  - Main residual risk is exposure of email attachments and/or sensitive files from shares
    - Compensating control - staff receive security awareness training

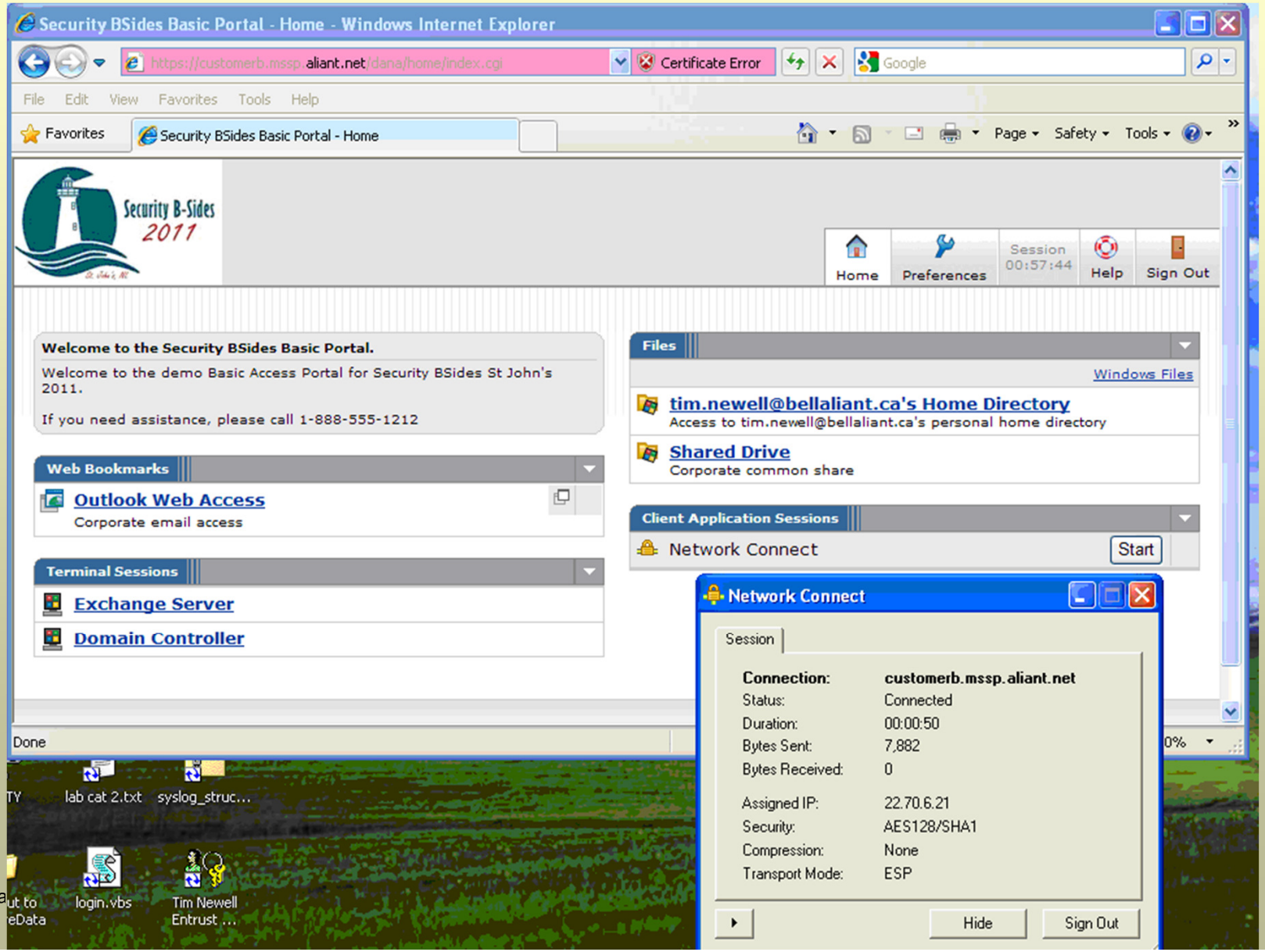
Customer Scenario – Basic Access



Customer Scenario - Solution

- Full access portal – network access, database, server management
  - Strong auth – Hardware Token plus Active Directory
  - Corporate machines only – watermark devices
  - Cache scrubber still required
  - AV must be specific corporate standard
  - Get all the functions of the Basic Access portal
  - Addition of open network-level access
  - RDP links to key servers as convenience for IT staff
- Essentially – set the bar higher – trusted device, known and trusted user – and open up access accordingly to keep things simple

Customer Scenario – Full Access



Things to Keep in Mind…

- Easy to overcomplicate!
  - Some products allow great deal of customization
  - Usually multiple ways to do things, and trade-offs with each
  - Enough rope to hang yourself…
- Understanding the options and how to apply them, and paradigm changes, can be hard at first
- Decide what you want out of your remote access solution
  - Security
  - Ease of use
  - Familiar user experience / easy transition
  - Cost (whether cash, support effort, user disruption, etc.)
- Typically:
  - Application-level access simplest, most secure
  - Network level also simple, similar to traditional VPN, but less secure
  - Favor application-only for less-trusted, open up network more for trusted users/devices

Thank you!

Supplemental – SSL VPN Functionality

SSL for Remote Access

- People equate SSL with HTTPS / browsers
- It's just an encrypted communication protocol
- "Tunneling" embeds one protocol's data as a package (payload) in another protocol
  - We think of IPSec, L2TP, PPTP, GRE
  - What about SSH port forwarding, HTTPtunnel, Loki?
  - NFS over SMTP anyone?
- SSL VPN uses SSL protocol in several ways, but isn't limited to just web apps / sites
  - Can offer full network access

Why bother? Sounds like my IPSec VPN

- Functional benefits of SSL versus IPSec
  - Application layer, rather than network
  - NAT type issues avoided – functions anywhere you can access a banking site
    - Hotels, WiFi hot spots
    - Corporate networks – firewall blocks IPSec (!?!)
  - Users happy, fewer help desk calls
- "Clientless" access [modes]
  - No client / minimal client / auto-install / auto-update
- ***A lot has to do with the "whole package" versus SSL as a protocol***

Typical Types of Access

- Web / proxy access
  - Simple, universal
  - Secure
  - Limited function
- Granular Client/Server
  - Good Security
  - Mid function
  - High complexity
- Full IP-level network access
  - Less Secure (IPSec?)
  - Full function
  - Simple
  - Familiar

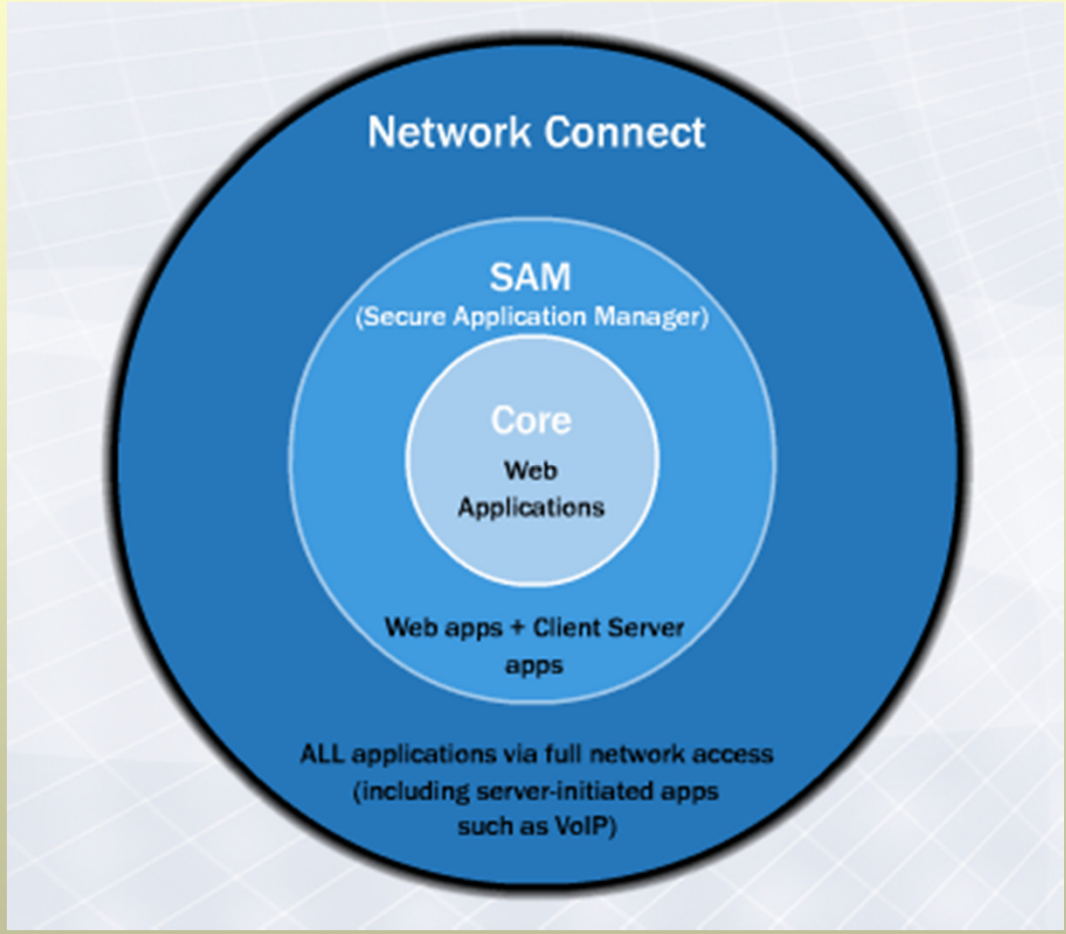


Figure courtesy Juniper Networks

SSL Access Type Comparison

	SSL Proxy	Client Server	Network Access
Benefits	• Very simple • Usually work with “any” browser • Clientless • (maybe Java applet / ActiveX) • Cross-platform	• Allow local apps – e.g. Outlook • Still access local network • “Lightweight” access	• Maximum Access • Familiar experience • Simple

Drawbacks	• Functionality limited – web apps
	  • (OWA but not Outlook)
	• Some add-ons allow e.g.
	  • Telnet / SSH
	  • RDP / Citrix
	  • Basic File Access
		• Configured app-by-app
		• Often limits on e.g. UDP, bi-dir
		• Can involve hoops
		  • E.g. DNS for loopback IP
		• Max complexity – Java / ActiveX, specific apps, more to go wrong
		• Different user experience
			• Greatest “client” footprint
			• Less control / logging usually

Security	• No IP Address on LAN • Application-level control • Detailed auditing	• “Pinhole” access – selective port forwarding	• IP on LAN – worms/malware • “No worse” than IPSec clients… • Can have good support for ACL’s
User Experience	• Web Portal and links • Accessible anywhere	• Web Portal and “helper” app • Run specific local applications	• Local VPN client and/or Portal • Log in, run ”any” local application

The whole package…

- Past few slides dealt with “core” frameworks
  - Common “bundled” features
    - Flexible authentication options
    - “Role based” access control
  - CAN be done with IPSec
    - Often aren’t as tightly integrated,
    - Harder to manage, and thus less common
- Remote access is often the Achilles Heel of corporate security (esp. authentication, malware)
- SSL VPN enables “anywhere access”, so also has to allow for that to be secured
  - Home users, vendors/partners, Public Kiosks, etc.

Security Add-Ons

- Most products offer a variety of extra features and options to protect and validate access
  - Usually licensed separately
  - Often third-party components or subscriptions
- These generally deal with validating or securing endpoints and protecting data
  - Cache scrubbers
  - Policy interrogation / enforcement
    - Reduced access and/or remediation zones
  - Sandbox environments
  - On-the-fly anti-malware agents/scans
  - On-screen keyboards