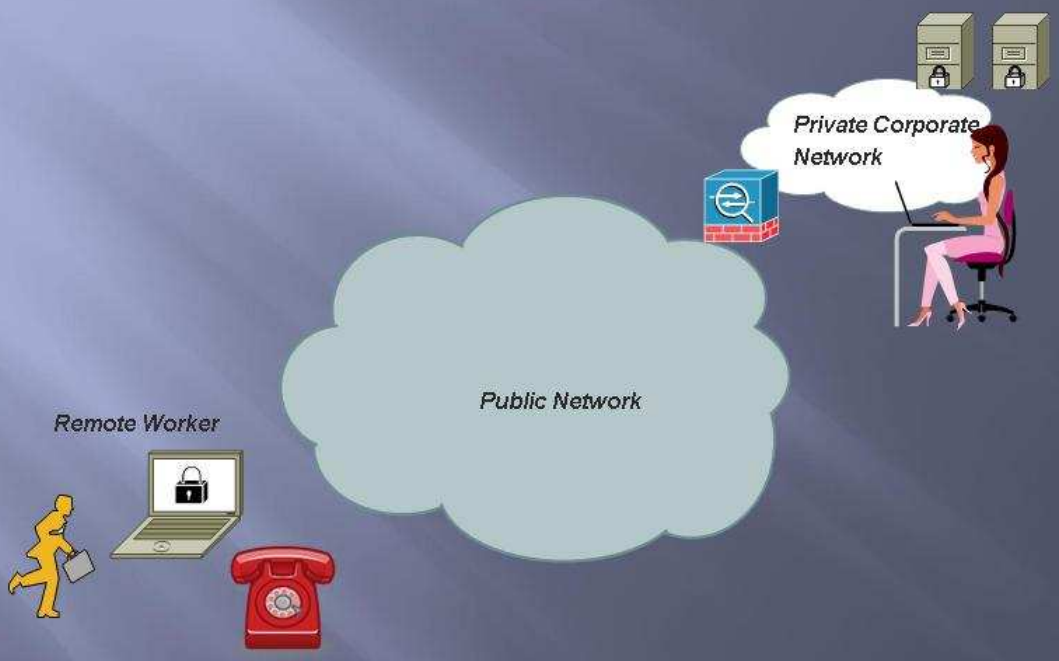
SSL VPN TECHNOLOGIES

By Igor Plotnikov

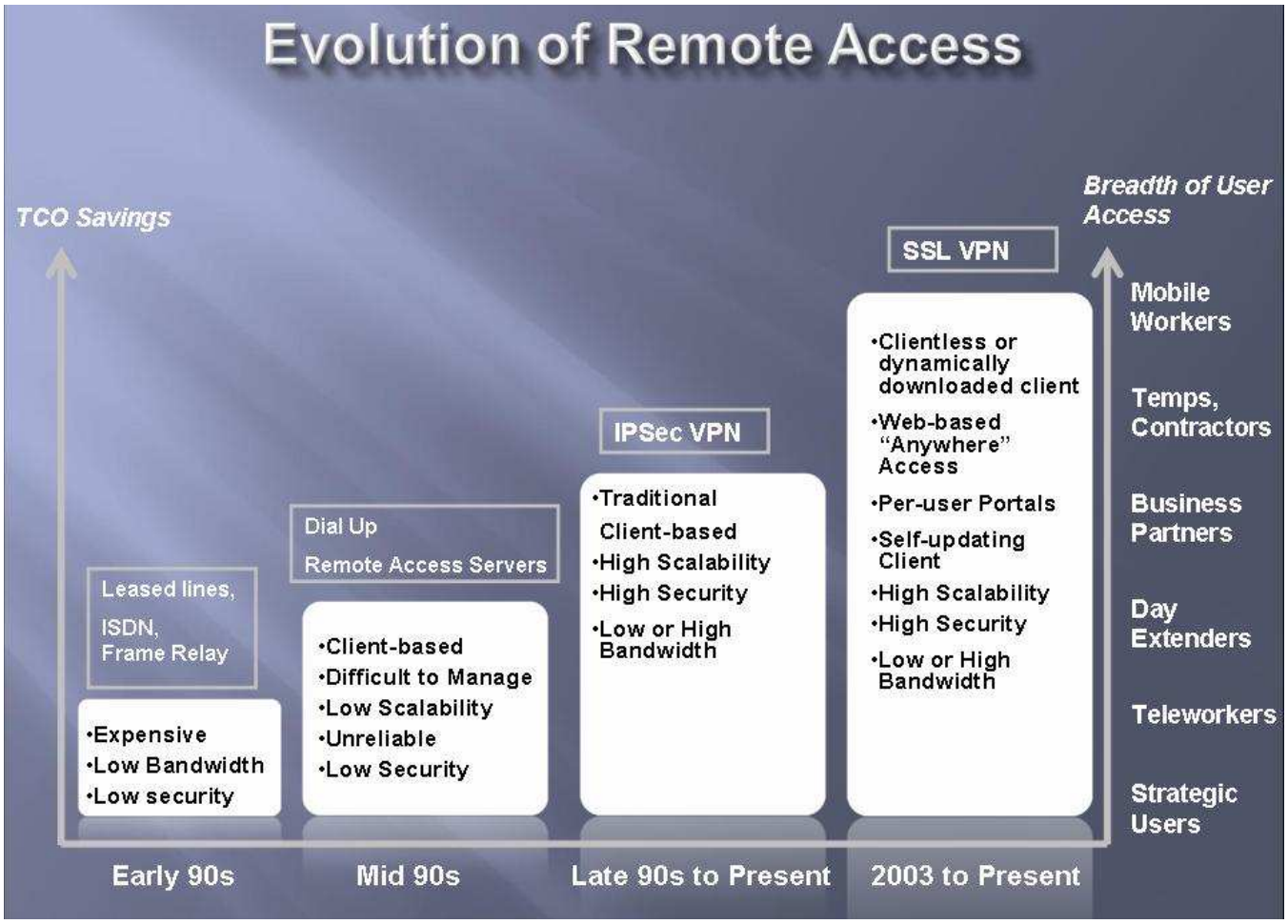
Agenda

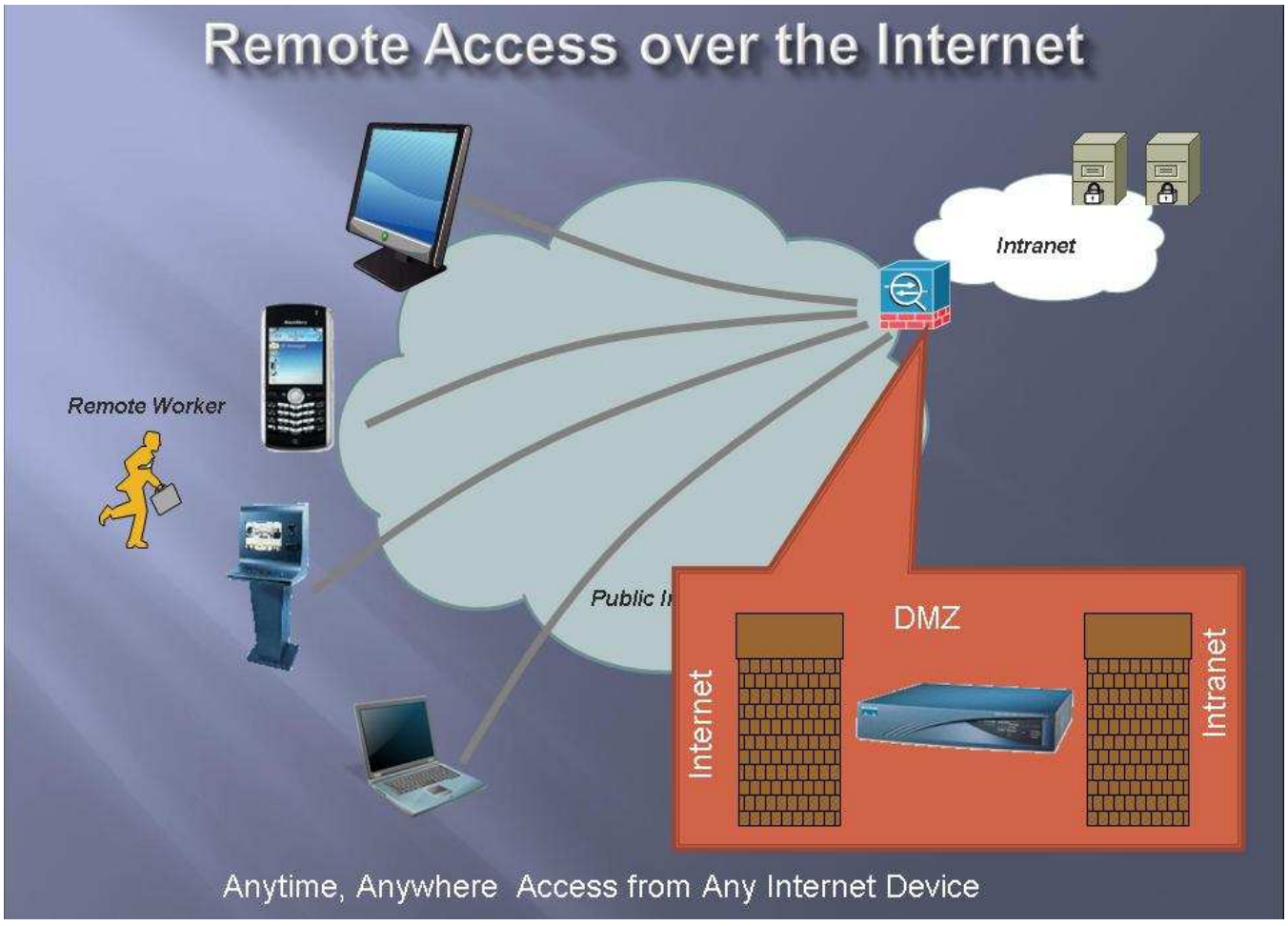
- Technology behind SSL VPNs
- The state of the market
- Personal experiences

The Problem of Remote Access to Your Data



Teleworking grown 40% since 2001 (Dieringer Research Group)


Evolution of Remote Access
TCO Savings
Breadth of User Access
Leased lines, ISDN, Frame Relay
•Expensive
•Low Bandwidth
•Low security
Dial Up Remote Access Servers
•Client-based
•Difficult to Manage
•Low Scalability
•Unreliable
•Low Security
IPSec VPN
•Traditional Client-based
•High Scalability
•High Security
•Low or High Bandwidth
SSL VPN
•Clientless or dynamically downloaded client
•Web-based "Anywhere" Access
•Per-user Portals
•Self-updating Client
•High Scalability
•High Security
•Low or High Bandwidth
Mobile Workers
Temps, Contractors
Business Partners
Day Extenders
Teleworkers
Strategic Users
Early 90s
Mid 90s
Late 90s to Present
2003 to Present


Remote Access over the Internet
Intranet
Remote Worker
Public I
DMZ
Internet
Intranet
Anytime, Anywhere Access from Any Internet Device

Two core ideas of SSL VPN

- Use the browser as a universal client
  - Create HTML applications to access some resources
  - Create generic mechanism to access Web servers
  - Use browser extensibility mechanisms – Java, ActiveX, plugins – for more
- Use https protocol in the browser as a security layer
  - The ciphersuites are comparable to IPSEC
  - Highly trusted security. More money is transferred every day over SSL than IPSEC or SSH
  - Always works! Internet, NAT, proxy-friendly

Architecture of SSL VPN

Portal – common unified user experience

Layer 7 VPN
Pure clientless

-Access to web apps:

-**HTML access to files:**
CIFS, FTP, NFS

-Web Mail

-Collaboration

Thin Client – L4 VPN
-Port Forwarder

Prepackaged Apps

- Citrix MetaFrame
- RDP (Windows Terminal Services)
- VNC
- Telnet/SSH
- X Windows

-Desktop access

Layer 3 VPN
Drivers behind the scenes

- **Full network access**

-**SSL** over port 443
-
Seamless install via browser

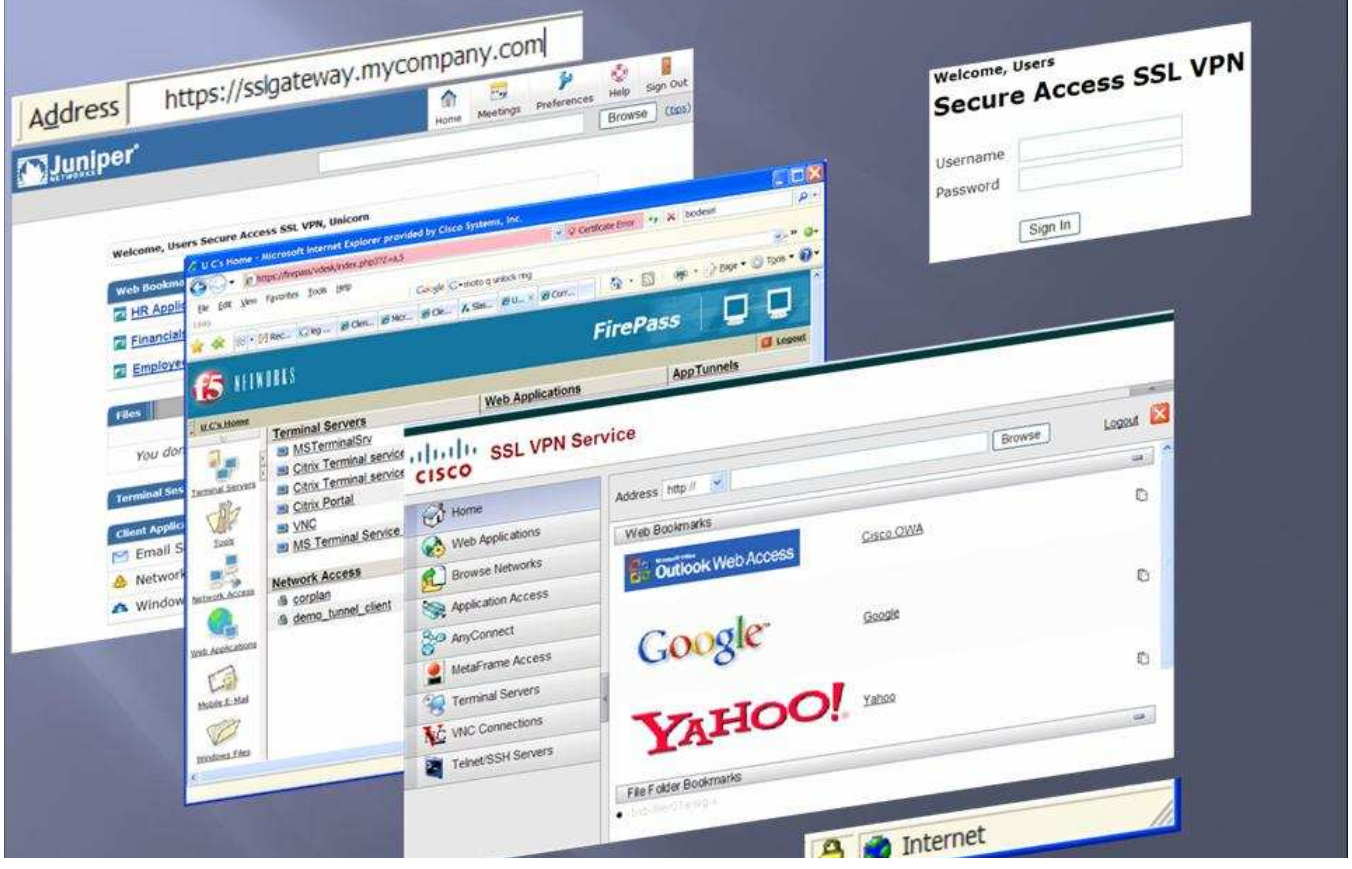
Browser-based logon, posture assessment, endpoint protection

SSL as a transport security layer

SSL Protocol

- Pioneered by Netscape in 1994
- Now in its 4th version, called TLS
- Highpoints:
  - Uses **public key crypto** to establish bulk symmetric keys
  - Has built-in **trust infrastructure** for accessing servers ad hoc, based on X.509 certificates
  - Provides **confidentiality, authentication and authenticity**
  - Typically used with **1024 bit** RSA keys, and **128 bit** symmetrical keys for 3DES, RC4 or AES ciphers
  - Extensive infrastructure for key revocation
- HTTP over SSL is called HTTPS

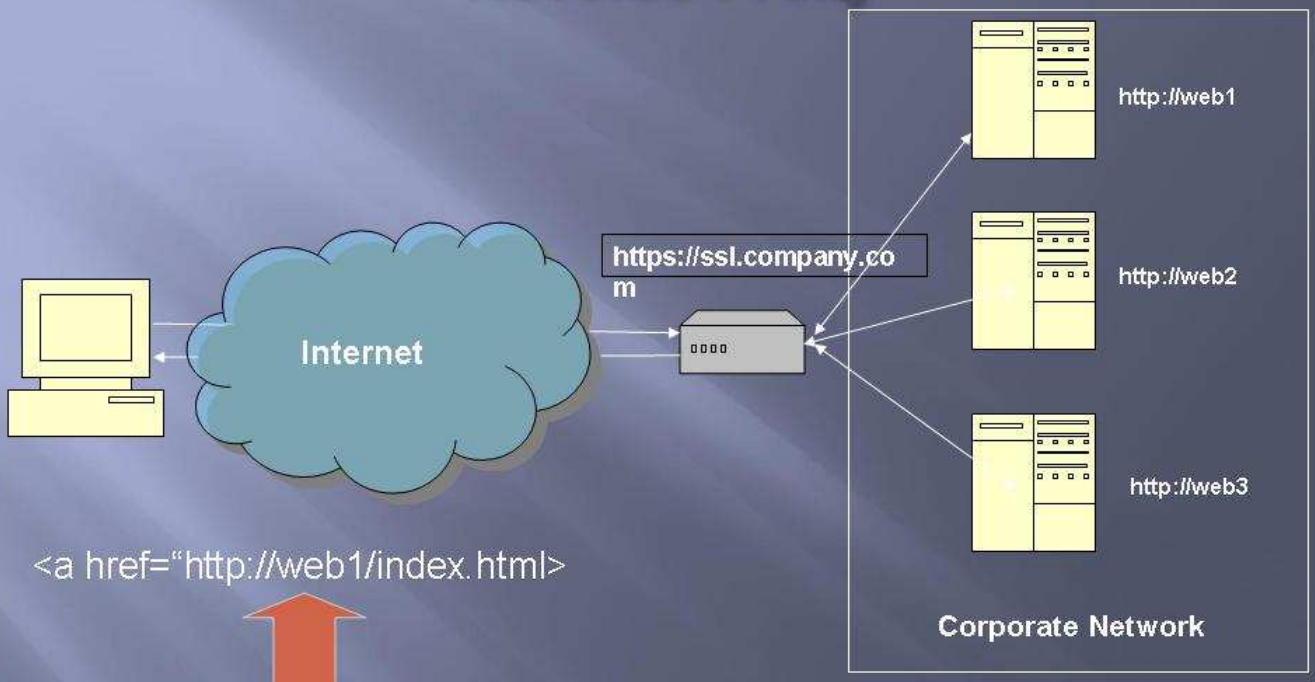
Browser as Application Delivery Platform



Request Authentication

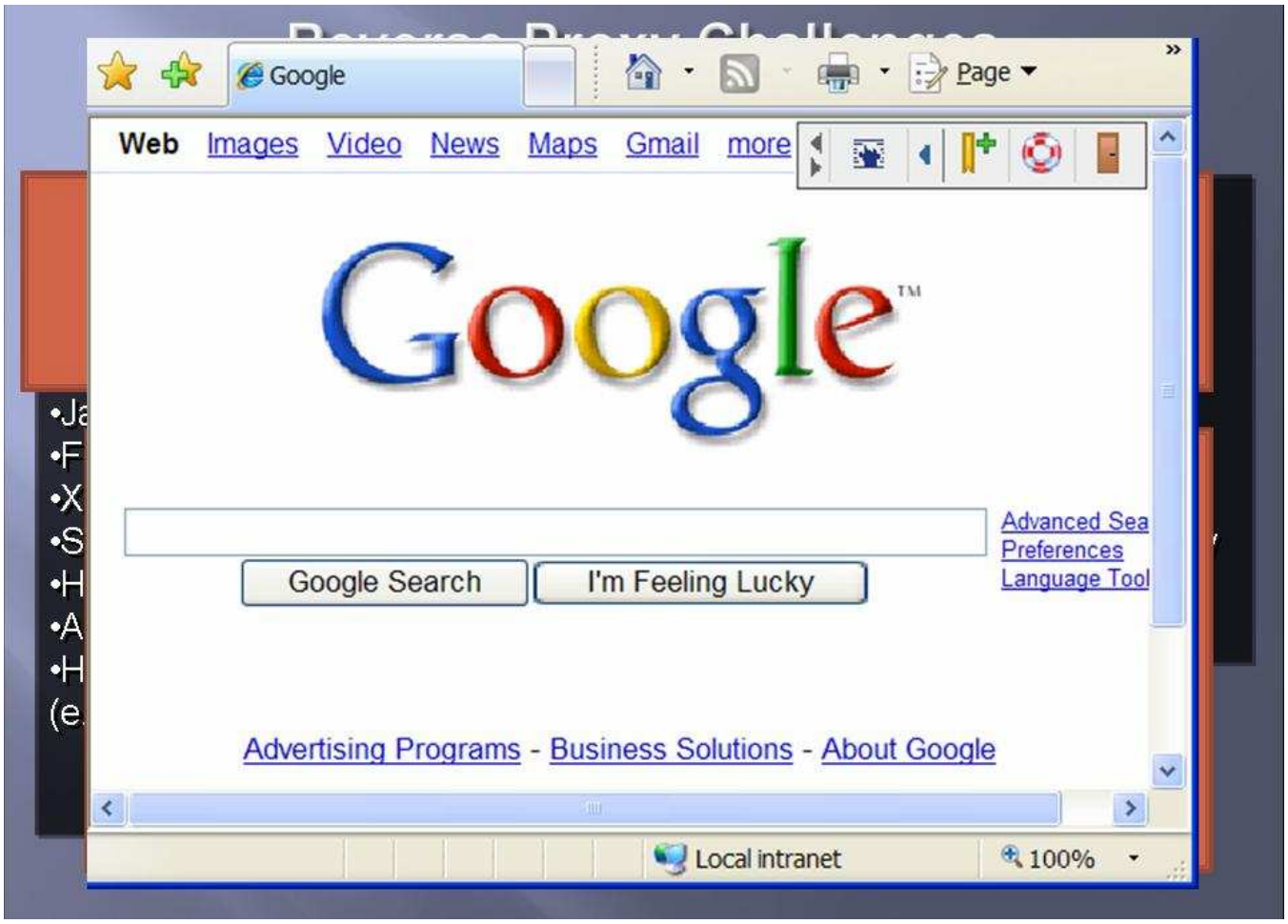
- HTTP is a stateless protocol
- State can be maintained via
  - Cookies
  - Query string parameters
  - Basic/NTLM authentication
- Usually the cookies are used
- It is possible to hijack a cookie

Reverse Proxy



<a href="https://ssl.company.com/http/80/web1/index.html>

Must transform: Anchors, Forms, StyleSheets, Meta tags, includes, etc.



Clientless SSL VPN as imperfect technology

```
var wnd = window.open("http://www.google.com/")
```

```
var wnd = window.open("http://ssl.mycompany.com/http/80/www.google.com/")
```

?

Clientless SSL VPN as imperfect technology

```
var mywindow = window;
var wnd = mywindow.open("http://www."+"google.com/")
```

```
function  SSLWOpen(wnd, url) {
        if(RealWindow(wnd))
                return EncodeUrl(url);
        return url;
}
// …..
var mywindow = window;
var wnd = SSLWOpen(mywindow,"http://www.google.com/")
```

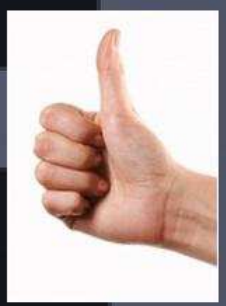
Window Objects and DOM objects methods, get and put for properties must be wrapped. Objects must be inspected.

Clientless SSL VPN as imperfect technology

JavaScript is a functional language.

It allows to call methods and access properties as associative arrays.

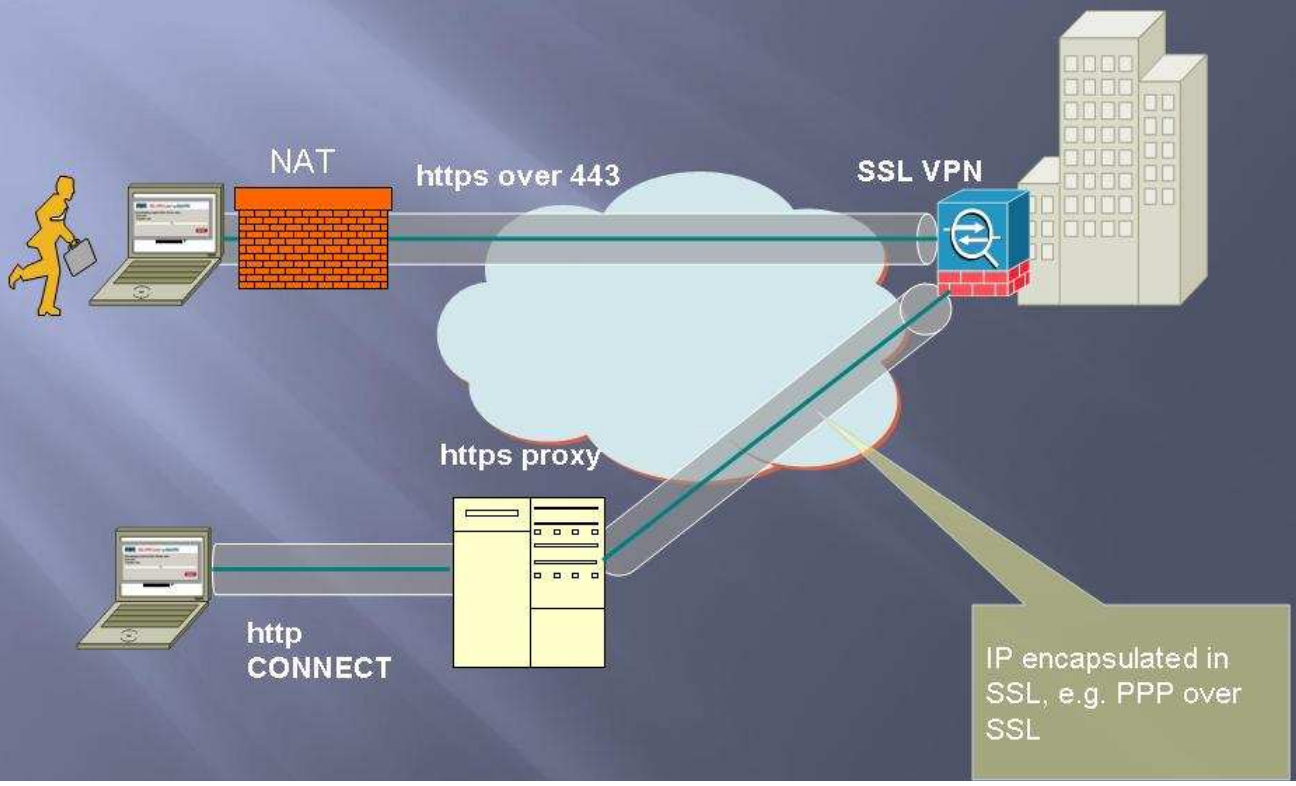
```
var _window = window;
var _open = "open";
var _url = "http://www.google.com/";
var wnd = _window[_open](_url);
```



How to address this imperfect nature?

- Qualify common productivity applications
- Create point patch capabilities
- Use other tools in the SSL VPN toolset
- Standardize the rewriter

Full Network Tunneling over SSL



Full Network Tunneling over SSL

SSL Full Network Tunneling is functionally equivalent to IPSEC, but better!

Main Benefits:

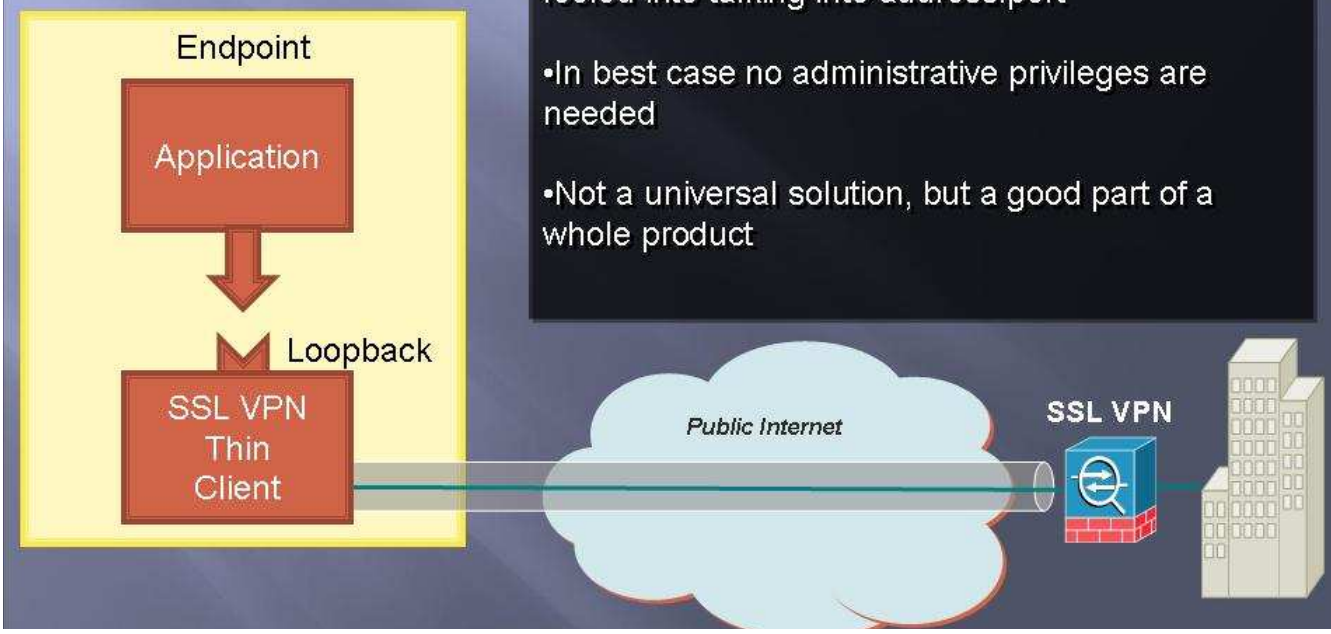
- Internet-friendly
  - https always tested
  - Traverses NAT
  - Traverses https proxies
- The client self deploys!
- Easy to use browser-based user experience

Limitations:

- IP over TCP/IP not good for VOIP
- Can be addressed via the use of DTLS (rfc 4347)
- Not completely standard

Port Forwarding – mini VPN for client-server apps

- Maps remote IP address:port to a local address:port
- The application needs to be reconfigured or fooled into talking into address:port
- In best case no administrative privileges are needed
- Not a universal solution, but a good part of a whole product



Endpoint Security Challenges

- Any endpoint can be used , not just a corporate asset
- Sensitive information may be left on a system, and recovered by an attacker
- The endpoint may have malware, spyware, rootkits

Solutions

- Mark all content non-cacheable
- Use cache cleaners
- Use sandboxing and virtualization
- Build access policies around posture assessment

Technology Summary

- SSL VPN is an application delivery platform
- Genetically closer to a web server than to a network device
- Ease of use, and low cost of deployment and support are the key differentiators
- Tight policy controls are essential

What makes it a product?

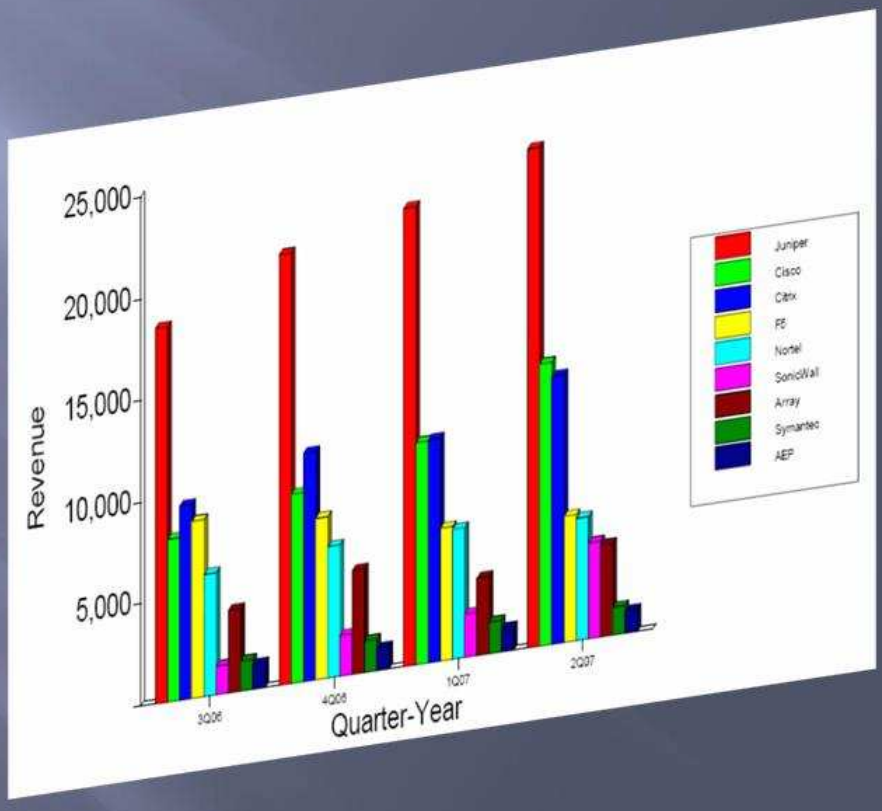
- AAA infrastructure
- Logging and monitoring
- High availability and clustering
- Enterprise class hardware
- Single Sign On
- Multilanguage support
- Multiplatform support

State of the SSL VPN market

- $631M addressable enterprise market CY09 *
- $91.7M worldwide revenue in 2Q07**
- 5-year CAGR of 21% *

Revenue Market Share Q207**

1.	Juniper	29.64%
2.	Cisco	16.78%
3.	Citrix	15.92%
4.	F5	07.50%
5.	Nortel	07.22%
6.	SonicWall	05.69%



*Sources: * Infonetics, ** Synergy*

Market trends

- Remote access SSL VPN replacing IPSEC
- The user base is growing, from under 20% of employees to 50%
- Managed services are growing
- Many companies invest into disaster recovery
- SSL VPN is often used to solve NAC problem
- More multifunctional devices with SSL VPN functionality

SSL VPN – active M&A space

- F5 acquired uRoam
- Juniper acquired Neoteris via NetScreen for ~$300M
- Symantec acquired SafeWeb
- Citrix acquired Net6 and Netscaler
- SonicWall acquired enKoo, Aventail
- BlueCoat acquired Permeo
- Microsoft acquired Whale
- Netilla merged with AEP
- Cisco, Nortel, Fortinet, Array - developed SSL VPN technology in house

Sharing a uRoam story

- uRoam founded in 1998 by Michael Herne, Alexander Sokolsky and Igor Plotnikov
- Very humbling experience
- Started off as a service for remotely accessing home desktops over SSL
- Really wanted to be a dot com initially
- Got naturally pulled into the enterprise remote access space in 2000 (agreement with RCN)

Sharing a uRoam story

- The timing was always wrong, up until 2002 we were contrarian
- We did not have a complete management team
- From *dot.com service* to *enterprise desktop access* to *mobile solution* to *peer to peer* to *next generation remote access* to *SSL VPN*
- The core technology stayed and evolved throughout the history, the marketing pitch kept changing
- The term SSL VPN was invented very late, in 2002. We intentionally avoided being compared with IPSEC

Sharing a uRoam story

- First to pioneer the full Network Access over SSL
- … but have not realized the importance
- "If you have all this technology how come we haven't heard of you?"
- Went through a reverse merger with Filanet
- Assets acquired by F5 Networks