Implementing Secure and Flexible Remote Access using SSL VPN

Ricky Elias
Security Architect
Advanced Technology (Security)
relias@cisco.com
Agenda

- The Need for Remote Access
- Deployment Considerations
- Endpoint Security
- Demo
- Q&A
Remote Access Market Evolution

Today
- IPSec?
- SSL?
- Client?
- Fixed Platforms?
- Video Apps?
- Mobile Security?
- Clientless?
- Mobile Platforms?
- Voice Apps?
- Data Apps?

Tomorrow

Convergence

Single Platform
Cisco ASA VPN Remote Access

Hardware Platforms

- Extensible across a broad range of enterprise networks
- Remote access and site-to-site VPN support
- Simple network integration
- Integrated load balancing (5510+) & HA
- Common criteria (EAL4) and FIPS certified

Capacity

ASA 5580
Up to 10000 VPN Sessions
1GB/s Max VPN

ASA 5550
Up to 5000 VPN Sessions
425Mb/s Max VPN

ASA 5520
Up to 750 VPN Sessions
225Mb/s Max VPN

ASA 5540
Up to 5000 IPsec Sessions
Up to 2500 SSL VPN Sessions
325Mb/s Max VPN

SOHO  ROBO  SMB  ENTERPRISE

Market Segment
SSL VPN is Different from eCommerce

Must fit into existing networks and application environments

Must support the same authentication mechanisms and often extensive application list as supported by IPSec

SSL VPN has multiple application support mechanisms
- Content rewriting and application translation (clientless/L7)
- Port forwarding (thin client)
- SmartTunnel (thin client)
- Dynamic VPN client (full network access/L3)
Handling Complex Content

Port Forwarding
  Local “thin” client acts as proxy
  Tunnels and forwards application traffic

Smart Tunnels
  Allows Winsock v2 TCP applications to use the VPN security appliance as a proxy gateway to the private side of a network

Plug-ins
  Citrix ICA, RDP, SSH/TELNET, VNC provided by Cisco
  Extensible framework for other popular protocols

Application Profile Customization Framework (Application Helper)
SSL VPN Tunneling: AnyConnect Client

Persistent “Thick”, “Full Tunneling”, or “Tunnel” Client

Traditional-style client delivered via automatic download
Access all applications
Supports 2K/XP/Vista (x86 & x64), Mac OS X 10.4 & 10.5, Linux x86, Windows Mobile 6
Can use TLS or DTLS as transport
Always up to date
  Automatic updates
  No admin privileges required for updates
Deployment Considerations
Deployment Considerations

Firewall placement and configuration
Routing
Address assignment
Client authentication
Resiliency
Firewall Placement and Configuration

Controlling Access to/from Public/Private Interfaces

Limit incoming traffic to IPsec and/or SSL for FW policy

Use firewall to inspect IP traffic after decryption

Parallel

Access Rule

Inline

Access Rule

DMZ
Routing - Interfaces/VLANs

User/Group Based Policies

Map users to group based on role

Use group policy to restrict egress VLAN

Potential VRF Integration
Routing: Address Assignment

Proxy-ARP
- IP pool/DHCP scope/static included within range of private interface subnet
- No changes required to router, no routing protocol required
- Transit network must have enough available IP space

Configured/Learned Routes
- IP pools are unique
- More scalable and can use unique per group IP pools
- Use static route(s) on downstream router pointing to private interface
- Use Reverse Route Injection (RRI), note IPsec only
- Use static route and route redistribution

VPN Security Appliance Uses Proxy-ARP

Downstream Router Requires a Specific Route
Split Tunneling

**Without** Split Tunneling

**Central Site**

**VPN Appliance**

**VPN Client**

**Maximum Security**

**With** Split Tunneling

**Central Site**

**VPN Appliance**

**VPN Client**

**Maximum Performance**
Client Authentication Design

VPNs can utilize many types of databases for centralized authentication

- Username and password
- Tokens
- Digital certificate/smartcards

Authenticated against:

- RADIUS
- Active Directory (AD)/Kerberos
- NT Domain
- RSA SecurID
- LDAP
- Other One-Time Password server (OTP) via RADIUS
- Single Sign-On (SSO)
Local/Geographical Failover/Load Balancing

Client Request Connection to 124.118.24.50
Virtual Cluster Master Responds with 124.118.24.33
(Least Loaded VPN Appliance)
Client Requests VPN Tunnel to 124.118.24.33

Virtual Cluster IP Address = 124.118.24.50

Master Selected Dynamically Based on:
- First to power up
- Priority (1–10)
- Lowest IP address
Endpoint Security
Security Concerns for SSL VPN

Before SSL VPN Session
- Who owns the endpoint?
- Endpoint security posture: AV, personal firewall?
- Is malware running?

During SSL VPN Session
- Is session data protected?
- Are typed passwords protected?
- Has malware launched?

After SSL VPN Session
- Browser cached intranet Web pages?
- Browser stored passwords?
- Downloaded files left behind?

Remote User
Customer Managed Machine

Supply Partner
Extranet Machine

Employee at Home
Unmanaged Machine
Cisco Secure Desktop
Comprehensive Endpoint Security for SSL VPN

Works with desktop guest permissions
No admin privileges required

Complete pre-connect assessment:
Location assessment—managed or unmanaged desktop?
Gathers data for Dynamic Access Policy
Specific applications running—defined by admin

Comprehensive session protection:
Malware detection
Data sandbox and encryption protects every aspect of session

Post-session clean-up:
Encrypted partition overwrite (not just deletion) using DoD algorithm
Cache, history and cookie overwrite
File download and email attachment overwrite
Auto-complete password overwrite
Dynamic Access Policy (DAP)

- Rulesets based on attributes
  - Can terminate connection based on any match
  - Can continue to evaluate against multiple rules

Access Policy Attributes:
- Network ACL and Web ACL Filters
- Portal Function Restrictions
- Port Forwarding and URL Lists
- Access Methods
- Dynamic Access Policy (DAP)
Key Takeaways

What Solution Fits Your Situation Best?

If your users carry their devices and installing a client is not an issue then focus on AnyConnect

    AnyConnect is the client for the future

If your users access corporate resources sporadically or you require access from non-employees then clientless SSL is best

    Good for partner and occasional guest access
    Good for employees that need basic services

If your users are telecommuters that work from home then a hardware based solution is ideal

    Integrates a wireless and IP hard phone solution
    Can accommodate spouse and child access