Remote Access VPN
AnyConnect Secure Mobility

Abdullah Ahmed

Regional Security Consultant
Cisco Systems
Anywhere, Any Device Access

Mobility: Opportunity and Challenge

- New Devices
- Access Control
- Support Costs
- Data Loss
AnyConnect Secure Mobility
AnyConnect Secure Mobility Client
Network and Security Follows User—It Just Works

Broad Mobile Support
- Fixed and semi-fixed platforms
- Mobile platforms

Persistent Connectivity
- Always-on connectivity
- Optimal gateway selection
- Automatic hotspot negotiation
- Seamless connection hand-offs

Next-Gen Unified Security
- User/device identity
- Posture validation including Managed vs Un Managed Assets
- Integrated web security for always-on security (hybrid)
- Clientless and desktop virtualization
Secure Borderless Network Architecture
Enabling Mobility, Extending Security

Inside the Corp Environment
- 802.1X, TrustSec, MACsec
- Local Data Center
- Corporate Office
- Branch Office

Outside the Corp Environment
- Always-On Integrated Security and Policy
- CORP DMZ BORDER

SECURITY and POLICY

- Customers
- Coffee Shop
- Home Office
- Airport
- Mobile User
- Attackers
- Partners

Software as a Service, Platform as a Service, Infrastructure as a Service
AnyConnect Secure Mobility Client
Architecture Overview

Architecture

AnyConnect User Interface
Services
AnyConnect Platform

Management Head-ends
Interfaces
Service Provider Integration

Head End Devices

Wired switches and Wireless controllers
NAC Appliances
ASA Remote Access ISRs
Web Security
Cloud Web Security
ScanSafe

Presentation_ID

© 2010 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential
AnyConnect 3.0

Highlights

New Look and Feel

- Tile-based UI

Broad Protocol Support

- IPsec IKEv2 (+ SSL and DTLS)

Enhanced Security and Mobility

- Integrated connection management (L2 supplicant)
- Wired network identity/security (802.1x and MACsec)
- Support for ScanSafe cloud security
- Integrated posture assessment (HostScan)
- Endpoint telemetry feeds
## AnyConnect 3.0
### Operating System Support

<table>
<thead>
<tr>
<th>CAPABILITY</th>
<th>WINDOWS</th>
<th>MAC</th>
<th>LINUX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced User Interface</td>
<td>⬜</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPsec (IKEv2) and SSL (TLS and DTLS)</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Network Access Manager</td>
<td>⬜</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Security with ScanSafe</td>
<td>⬜</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated Posture (Host Scan)</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Telemetry</td>
<td>⬜</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-install</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Web-deploy and upgrade</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
<tr>
<td>Integrated Diagnostics and Reporting</td>
<td>⬜</td>
<td>⬜</td>
<td>⬜</td>
</tr>
</tbody>
</table>
AnyConnect 3.0 New UI
AnyConnect 3.0
New User Interface

- New User Interface for
  - Windows 7 and Vista (x86 and x64)
  - Windows XP (x86)
  - Windows 2003 Server (x86)
  - Network Access Manager

- Enhanced UI for other platforms to follow

Windows 7-style Tray Flyout Provides 95% Functionality
Advanced Window for...

...Statistics, Configuration, and Diagnostic Options
Customizable...

... Logo, background image, application icon, title, system tray icons
AnyConnect 3.0
IPsec (IKEv2) Benefits

- Mobility Friendly
- Increased Security (over IKEv1)
- Full suite of Authentication options
- Conforms to federal mandates
AnyConnect 3.0
IPsec (IKEv2) Implementation

Requires head-end upgrade to ASA 8.4

Can be selectively enabled for individual groups

Utilizes SSL for advanced features such as dynamic upgrade, Hostscan, Customization and SCEP etc.
AnyConnect 3.0
IPsec (IKEv2) Licensing

Existing AnyConnect licenses support IKEv2
AnyConnect 3.0
IPsec (IKEv2) Migration

- CLI support to migrate IKEv1 config to IKEv2
  
migrate <l2l | remote-access <ssl | ikev2>> <overwrite>

crypto ipsec transform-set ddd esp-3des md5-hmac

crypto map abc 1 set ikev1 transform-set ddd

tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
  ikev1 pre-shared-key *
  ikev1 trust-point labca

group-policy DfltGrpPolicy internal
  group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ikev1 l2tp-ipsec

crypto ipsec ikev2 ipsec-proposal ddd
  protocol esp encryption 3des
  protocol esp integrity md5

crypto map abc 1 set ikev2 ipsec-proposal ddd

tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
  ikev2 local-authentication certificate labca
  ikev2 remote-authentication pre-shared-key *
  ikev2 remote-authentication certificate

group-policy DfltGrpPolicy internal
  group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec
AnyConnect 3.0
IPsec (IKEv2) - Protocol Selection

- Profile specifies which protocol the client should use

SSL VPN is the default protocol.
Explicit configuration required to connect with IPSec
There is no protocol fallback
Network Access Manager
AnyConnect 3.0
Network Access Manager—Key Features

- Enterprise-focused connection management
- Wired (802.3) and wireless (802.11) connectivity via single authentication framework
- Layer-2 user and device authentication:
  - 802.1X, 802.1X-REV (wired key establishment)
  - 802.1AE (MACsec: wired encryption)
  - Supports numerous EAP types
  - 802.11i (Robust Security Network)
- Supports both Admin (office) and User (home) network configurations
AnyConnect 3.0
Network Access Manager—Highlights

- Intelligently detects and selects ‘best’ layer 2 access network(s)
- Automatically connects to configured networks. Automates user-experience.
  - Wired is preferred over WiFi in automatic mode.
  - Override with manual mode.
- One connection at a time
  - All other connections are blocked
- Post-connection script launch:
  - Script runs on user context
  - Can be defined by admin or user (if allowed)
- Enterprise-class Server Validation
  - Multiple validation rules per connection
- Remote desktop support
  - Extend User Connection beyond Logoff
AnyConnect 3.0
Network Access Manager—User Interface

- **Network Tile**
  Available when NAM is installed, inactive when service is disabled.

- **Network State Information**
  Indicates authentication progress
  Connected state shows IP address

- **Network Selection (Combo) Box**
  Defined Networks (bold face)
  Scan-list (ordered from open to most secure)
  Signal strength and security indicators
  Allows user to add new network profiles
  Connection mode - automatic vs. manual
AnyConnect 3.0
Network Access Manager — Specifications

General
- 802.1X – Authentication Security
- 802.1AE (MACsec) – Link Encryption

Operating Systems
- Windows XP – 32-bit
- Windows Vista – 32-bit & 64-bit
- Windows 7 – 32-bit & 64-bit
- Windows Server 2003 – 32-bit

EAP Types
- Non Tunneled EAP Methods:
  - EAP-TLS
  - EAP-MD5
  - EAP-MSCHAPv2
  - EAP-GTC
  - LEAP
- Tunneled EAP Methods:
  - EAP-PEAP (EAP-MSCHAPv2, EAP-TLS, EAP-GTC)
  - EAP-FAST (EAP-GTC, EAP-TLS, EAP-MSCHAPv2)
  - EAP-TTLS (EAP-MD5, EAP-MSCHAPv2, PAP, CHAP, MSCHAP, MSCHAPv2)
### AnyConnect 3.0

#### Network Access Manager — CSSC Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Secure Services Client</th>
<th>Network Access Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Controls</td>
<td>Management Utility</td>
<td>Profile Editor</td>
</tr>
<tr>
<td>VPN Support</td>
<td>Cisco VPN Client</td>
<td>AnyConnect VPN</td>
</tr>
<tr>
<td></td>
<td>Interaction</td>
<td>Integration (Always On and TND)</td>
</tr>
<tr>
<td>Diagnostic Utility</td>
<td>Log Packager</td>
<td>DART</td>
</tr>
<tr>
<td>Authentication Policy</td>
<td>Global</td>
<td>User-Enforced</td>
</tr>
<tr>
<td>Wired Link Encryption</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>One Connection at a Time</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Locked Profiles</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New* End User Groups</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Post-Connection Script</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>FIPS 140-2</td>
<td>Windows XP</td>
<td>Windows XP</td>
</tr>
</tbody>
</table>
- Controls auto selection of networks
- Attempts to make connections defined in currently active group.
- Disabling Auto-Connect enforces manual connection mode.
- User required to select network connection.
- Manual connection mode applies to both admin and user configured networks.
AnyConnect 3.0
Network Access Manager — Remote Desktop

- First remote or console user credentials used for network authentication

- Additional user logons are not authenticated and user does not have a system tray icon

- Extend user connection beyond logoff – when different user & machine VLANs are used
AnyConnect 3.0
Network Access Manager — Other New Features

- Limited or No Connectivity

- Not all defined networks are found in the UI network drop down list.

- Auto-connection algorithm enhanced to use scan list.
  - Hidden
  - Broadcasting

- Active group persists across reboot
AnyConnect 3.0 with MACsec

- Supports MACsec/MKA data encryption AES-GCM-128 in software (Performance CPU-dependent)

- MACsec capable hardware (network interface) enhances performance

- Requires Cisco Secure ACS 5.1+

MACsec-ready hardware:

- Intel 82576 Gigabit Ethernet Controller
- Intel 82599 10 Gigabit Ethernet Controller
- Intel ICH10—Q45 Express Chipset (1Gbe LOM) (Dell, Lenovo, Fujitsu, and HP have desktops shipping with this LOM)
Policy Based Encryption Using MACsec

Using AnyConnect 3.0

Finance Admin

MACSec in Action

802.1X Cat3750

LAN

Finance Admin

ACS5.2 Must Encrypt

Authentication Successful!

Using Normal Supplicant

Finance Admin

No MACSec Supplicant

Normal Supplicant on Personal Laptop

Fall Back to Insecure VLAN

802.1X Cat3750

LAN

Finance Admin

ACS5.2 Must Encrypt

Authentication Successful!

Everything is sent in clear therefore you can see everything on wire
AnyConnect 3.0
Network Access Manager—Configuration (Admin)

- Profile Editor Launched from ASDM
  - Standalone version for non-VPN customers.

- Configure security policies, network profiles, groups, etc.

- Connections generated by the profile editor are locked
  - Protection against data tampering

- Deployable via AC downloader or SMS.
AnyConnect 3.0
Network Access Manager—Licensing

NAM is free when using with Cisco wireless AP, Wireless LAN controllers, switches and RADIUS servers

Support requires a current Smart Net contract on the related Cisco equipment
Web Security
AnyConnect 3.0
Web Security with ScanSafe
AnyConnect 3.0
Web Security with ScanSafe - Highlights

- Keeps malware from getting to your system in the first place
- Enforces Acceptable Use Policy
- Protects users even when VPN is disconnected
- Tunnels HTTP/HTTPS traffic through ScanSafe cloud
- Replacement for AnyWhere+ standalone client
AnyConnect 3.0
Web Security with ScanSafe – Key Features

- Trusted Network Detection
  Based on connectivity to beacon Server

- Optimal ScanSafe Tower Selection
  Based on round-trip latency
  **Fail-Open** if tower not reachable

- Exception List
  IP address, Domain and Host
  Wild-card (*.cisco.com)
AnyConnect 3.0
Web Security with ScanSafe Overview

ScanSafe offers consistent, enforceable, high performance Web security and policy, regardless of where or how users access the Internet.
AnyConnect 3.0

Web Security with ScanSafe - ScanSafe Scan Center

- Over 5000 customizable reports
- 75 reporting attributes
- 11 reporting categories
- Comprehensive Drill down analysis

- Cumulative, trending and forensic reports
- Automatic Scheduled reports
- Actionable Granular reports
AnyConnect 3.0  
Web Security Module - Details

- Includes Authentication and group information with the request
- The ScanSafe Tower enforces appropriate policies
- Request results are then scanned and returned to the client

Note: Exclude ScanSafe tower list from your VPN split-tunnel.
AnyConnect 3.0
Web Security with ScanSafe - Policy Management

- Centrally managed via the ScanSafe web portal
- Rule based policies allowing for a default policy while creating custom exceptions for particular users or groups
AnyConnect 3.0
Web Security with ScanSafe - Policy Management

- Filter – “What” content the Policy will match
  - URL Category
  - Custom domain and URL lists supporting sub-domains, request paths and wildcards.
  - MIME Content-type
  - MIME File-type
  - Protocol – HTTP, HTTPS, FTP over HTTP
  - Outbound content filters
AnyConnect 3.0
Web Security with ScanSafe and WSA - Hybrid

- When VPN is connected, all traffic is forwarded to ASA and web traffic is inspected by WSA at HQ.
AnyConnect 3.0
Web Security with ScanSafe and WSA - Hybrid

- If VPN is disconnected, user is still protected by ScanSafe as http traffic is now routed to the nearest ScanSafe tower.
AnyConnect 3.0
Web Security with ScanSafe and WSA - Hybrid

- When user enters Trusted Network, ScanSafe is disabled and user is protected by corporate WSA.
Licensing will be handled by existing ScanSafe license model. No additional AnyConnect license needed.
Posture Module
AnyConnect 3.0
Posture Module - Benefits

- Enables Host Scan integration with AC 3.0
- Provides elevated privileges for Host Scan
- Supports frequent updates to Hostscan
- Ensures Timely support for new AV, Anti Spy-Ware and Pers. Firewall releases.
AnyConnect 3.0
Posture Module – Multiple Host Scan Options

CSD Package
- Hostscan
- Vault (Secure Desktop)
- Key stroke logger
- Cache Cleaner

AnyConnect Package
- Hostscan
- Network Access Manager
- Web Security
- Posture and Telemetry

Independent

Independent hostscan takes precedence over the hostscan component in CSD.
Summary
Cisco AnyConnect Secure Mobility
From Remote Access to Secure Mobility

Seamless, Pervasive Access
- Advanced Connectivity Features
- SSL VPN, IPsec DTLS (voice/video)
- Always On VPN

Next Generation Security
- Strong authentication
- Posture Assessment and Secure Virtual Containers
- Hybrid Web Security

Broad Enterprise Mobility Support
- Windows, Mac and Linux
- iOS 4.1 (iPhone)
- Windows Mobile 6.1