



Cisco AnyConnect Secure Mobility Solution

György Ács

Regional Security Consultant

Agenda



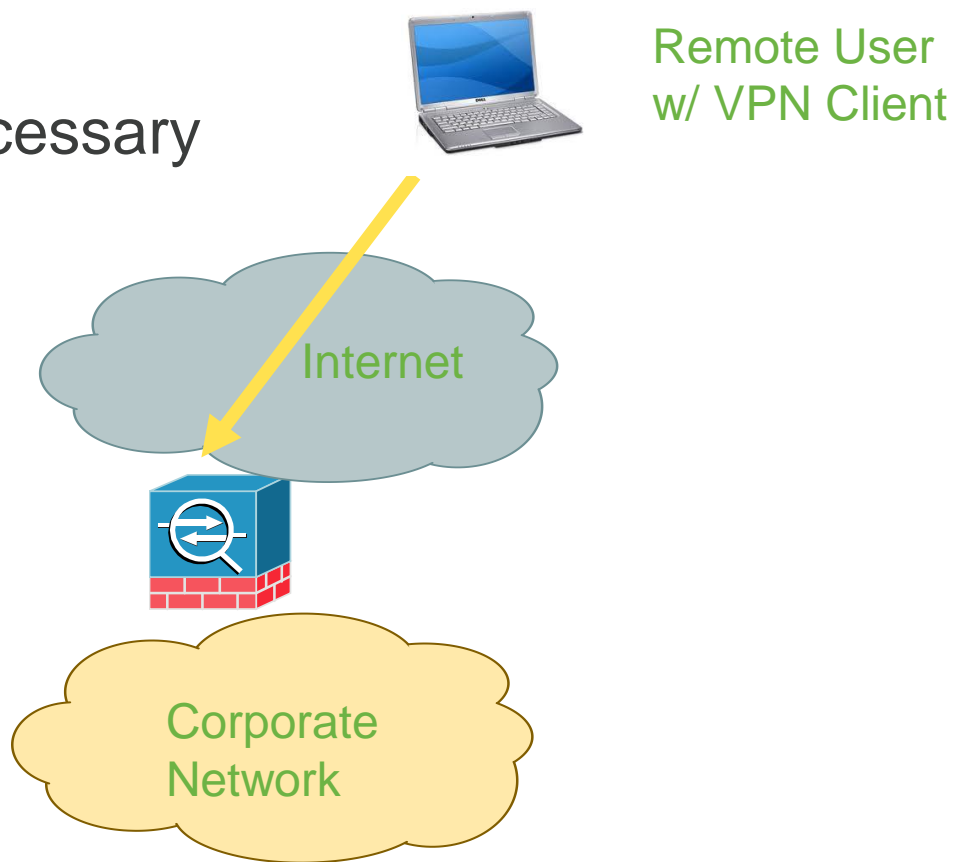
- Mobile User Challenges
- Mobile and Security Services
- Web Security Deployment Methods
- Live Q&A



Mobile User Challenges

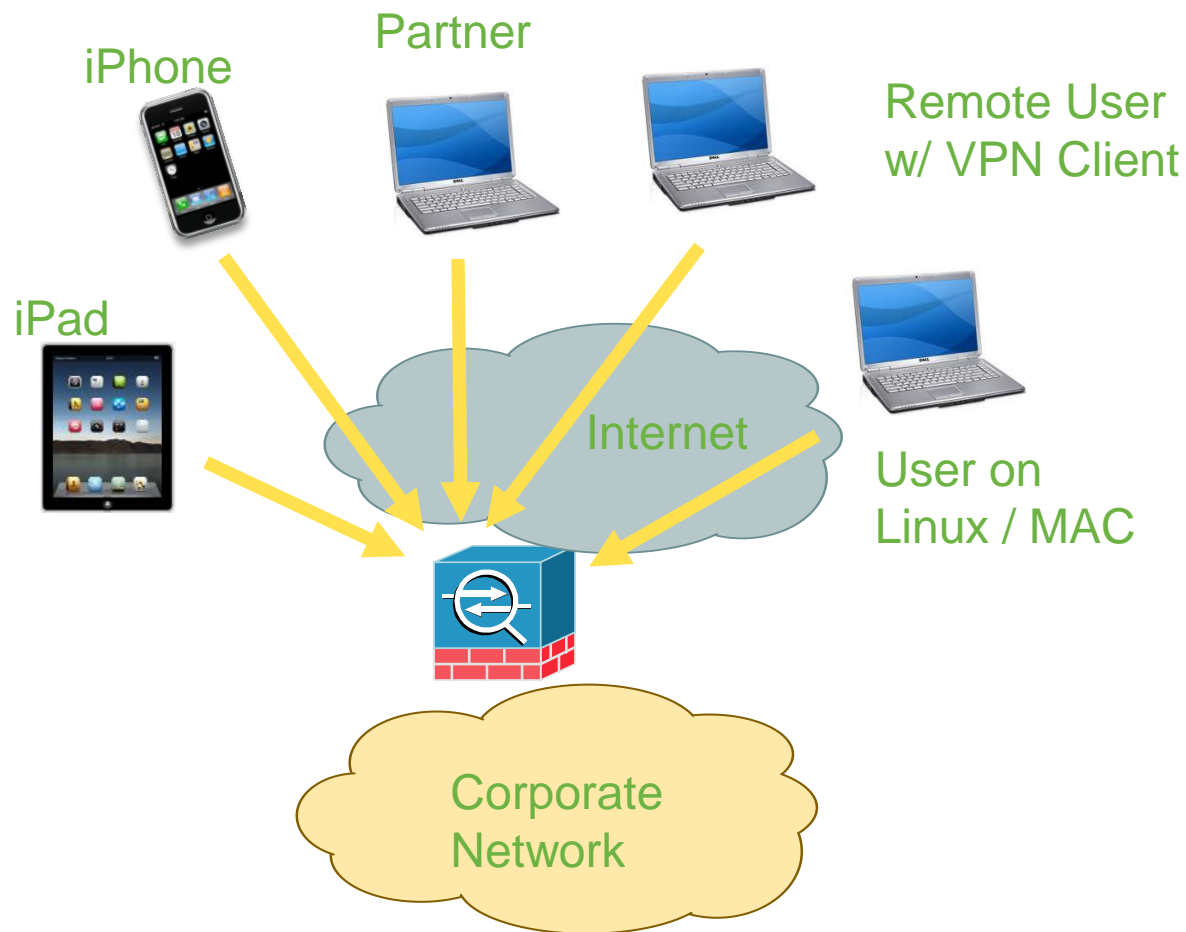
Traditional Remote Access

- Manual Tunnel Setup
- Limited Roaming
- Client only connected if necessary



Challenge Today - Consumerization

- Different Enduser Devices
- Different Levels of Access required

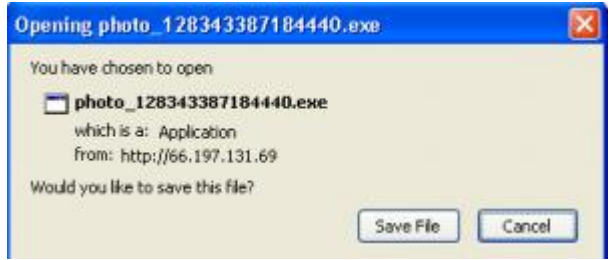
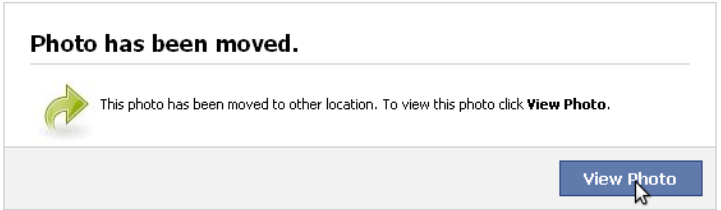
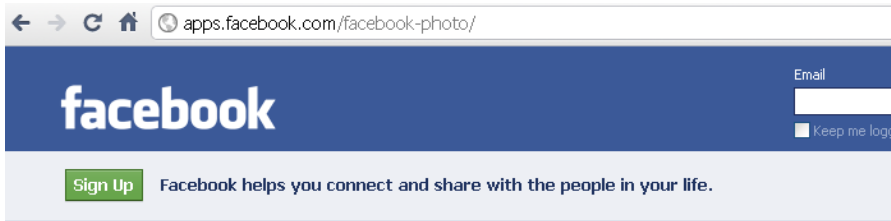


Challenge Today – HTTP as new TCP

- Many Applications use HTTP as the transport
- Applications can no longer be identified on Network Layer
- Communication with aggressive advertising sites or phishing sites




Criminals targeting Facebook



VirusTotal is a [service that analyzes suspicious files and URLs](#) and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 1 VT Community user(s) with a total of 1 reputation credit(s) say(s) this sample is malware.

File name: **photo_128343387184440.exe**
 Submission date: **2011-02-22 22:41:58 (UTC)**
 Current status: **finished**
 Result: **37 /43 (86.0%)**

VT Community

malware
 Safety score: 0.0%

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
AhnLab-V3	2011.02.23.00	2011.02.22	Win-Trojan/Ircbrute.140855
AntiVir	7.11.3.198	2011.02.22	TR/Crypt.XPACK.Gen
AntiV-L	2.0.3.7	2011.02.22	Trojan/Win32.Menti
Avast	4.8.1351.0	2011.02.22	Win32:VB-RCX
Avast5	5.0.677.0	2011.02.22	Win32:VB-RCX
AVG	10.0.0.1190	2011.02.22	Generic21.DQP
BitDefender	7.2	2011.02.22	Trojan.Generic.KD.127947
CAT-QuickHeal	11.00	2011.02.22	Trojan.Menti.f

Twitter as BotNet Command and Control Channel

The Register[®]
Biting the hand that feeds IT

Exclusive videos.

Original URL: http://www.theregister.co.uk/2009/08/13/twitter_master_control_channel/

Twitter transformed into botnet command channel

Victim becomes enabler

By **Dan Goodin in San Francisco**

Posted in [Security](#), 13th August 2009 20:50 GMT

[Free whitepaper – Avoiding 7 common mistakes of IT security compliance](#)

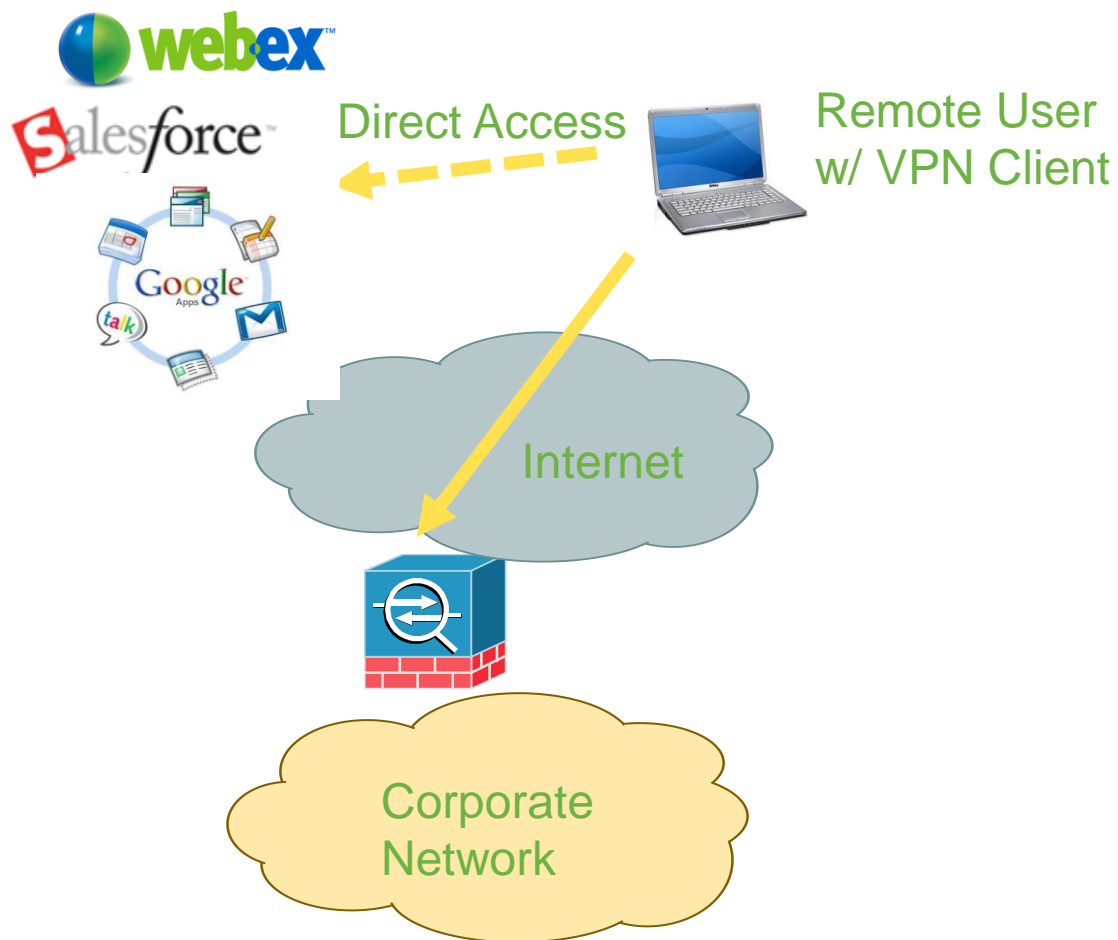
For the past couple weeks, Twitter has come under attacks that besieged it with more traffic than it could handle. Now comes evidence that the microblogging website is being used to feed the very types of infected machines that took it out of commission.

That's the conclusion of Jose Nazario, the manager of security research at Arbor Networks.

On Thursday he stumbled upon a Twitter account that was being used as part

Challenge Today - Cloud

- Services are moving to the Cloud
- Can be access directly
- No Control from Corporate Policy



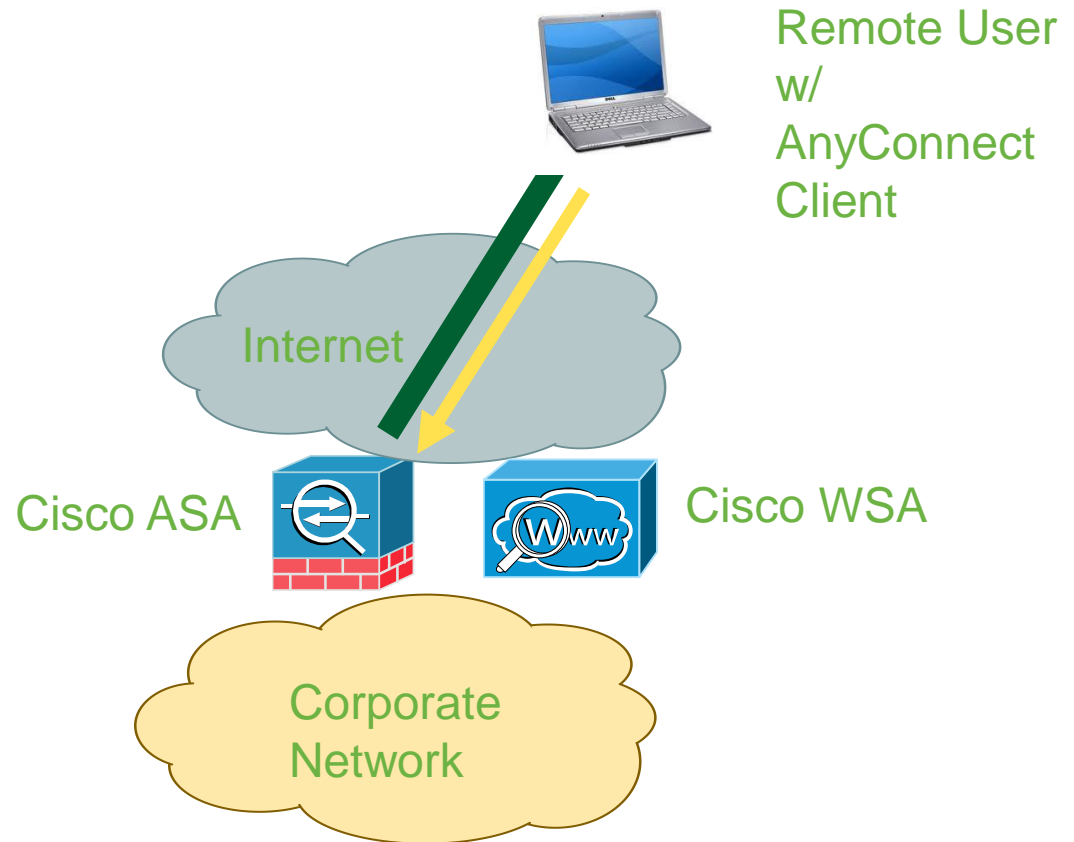
What we want to achieve

- Maximum of usability for the Enduser
Connect from anywhere, with any device, at any time
- Minimum of administration from corporate side
- Consistent control of security policy
Same policy if in the office or outside the office
Same policy regardless if connected Wired, Wireless
or via VPN



How we want to do it

- Tunnel is always on
User is always connected
- Anyconnect Client provides maximum usability
Easy, quick, transparent
- ASA and WSA can exchange user info for SSO
- WSA protects webtraffic

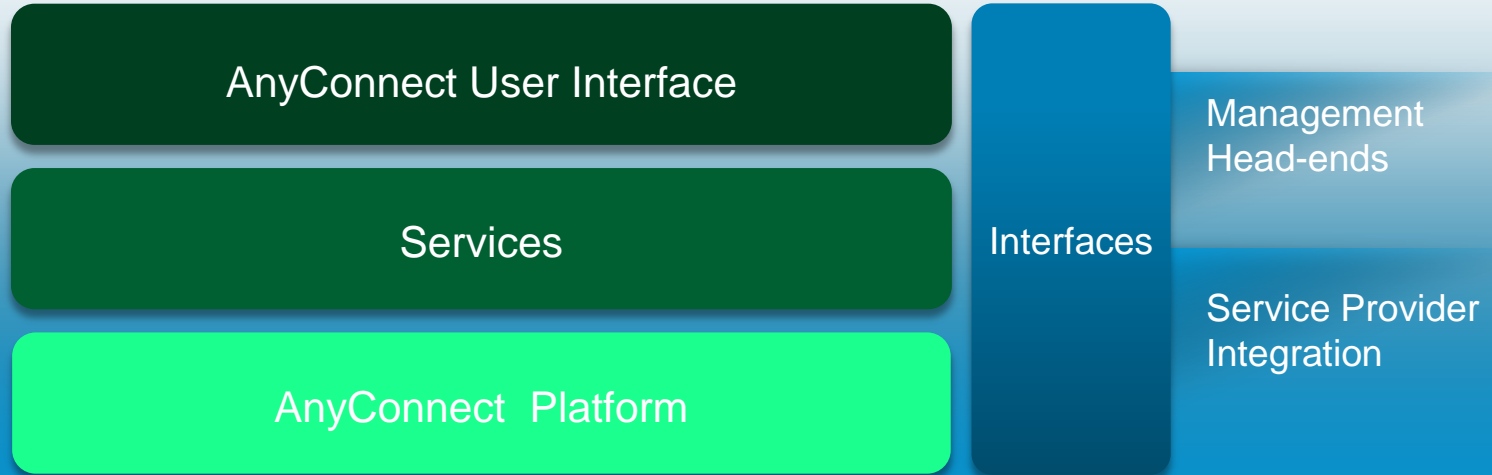




Mobile and Security Services

AnyConnect Secure Mobility Client

Architecture Overview



Architecture

Head End Devices



Wired switches and
Wireless controllers



NAC
Appliances



ASA Remote Access
ISRs



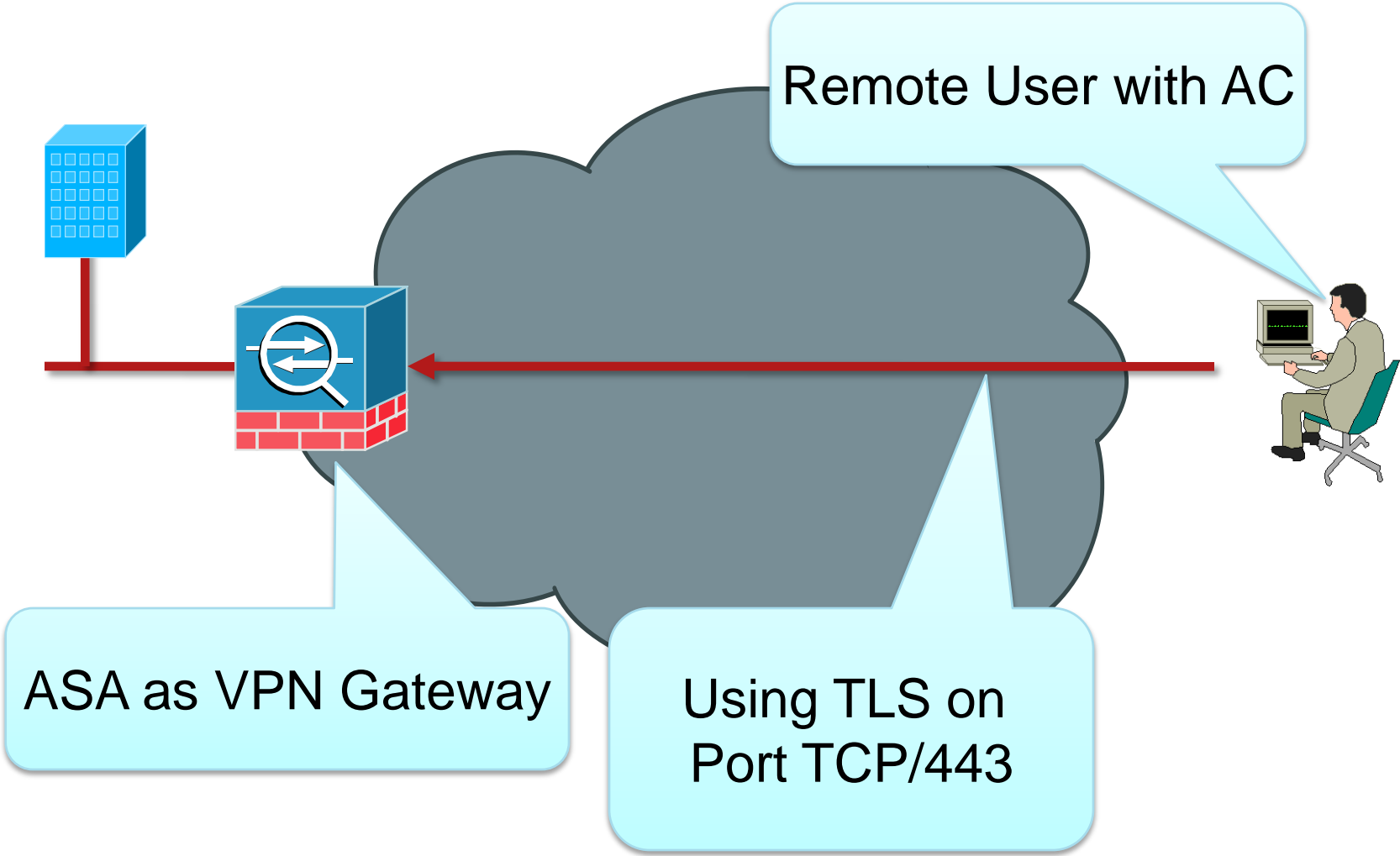
Web Security



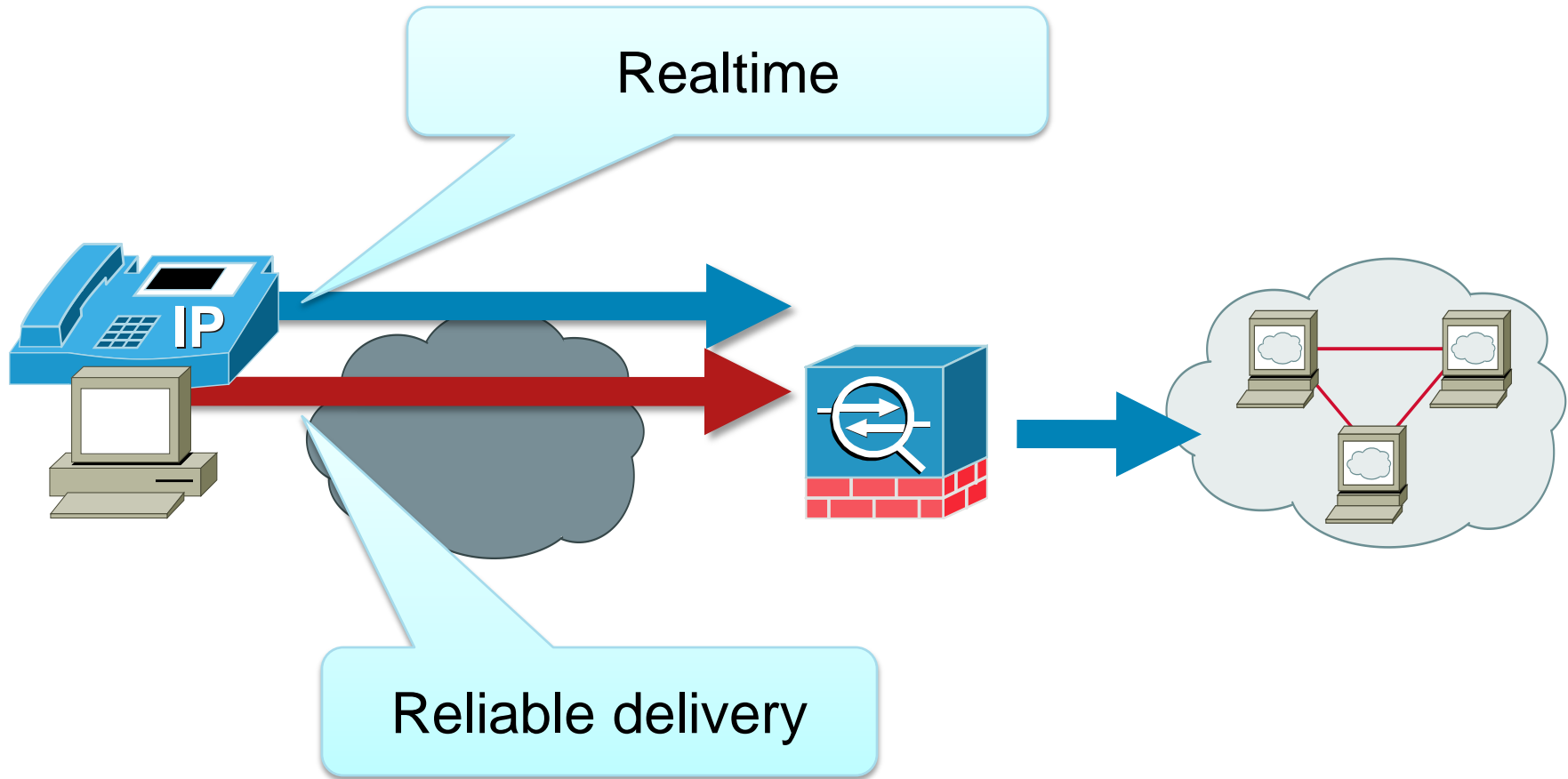
Cloud Web
Security

Trustsec
and Cisco
Medianet

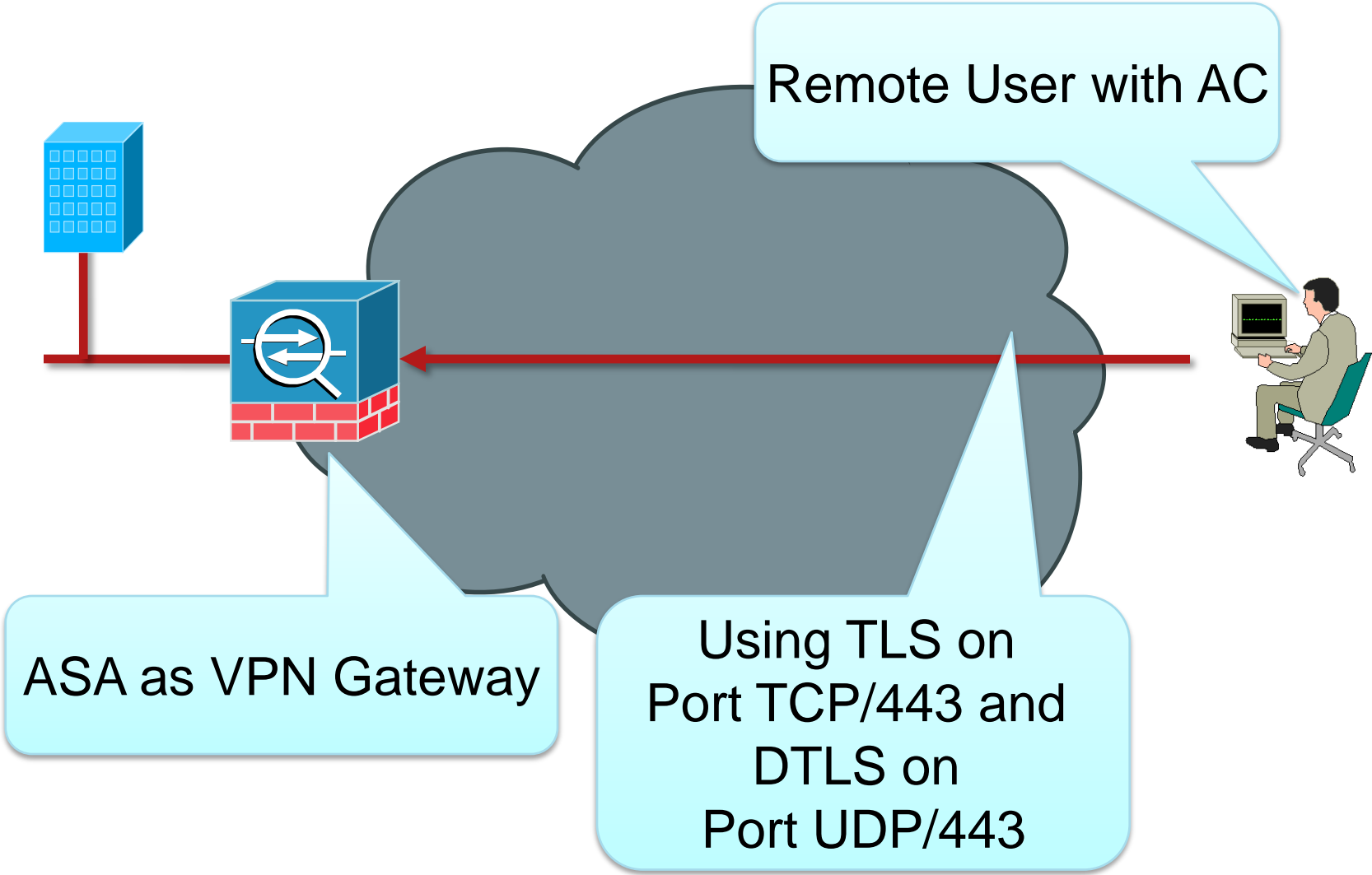
SSL VPN with AnyConnect



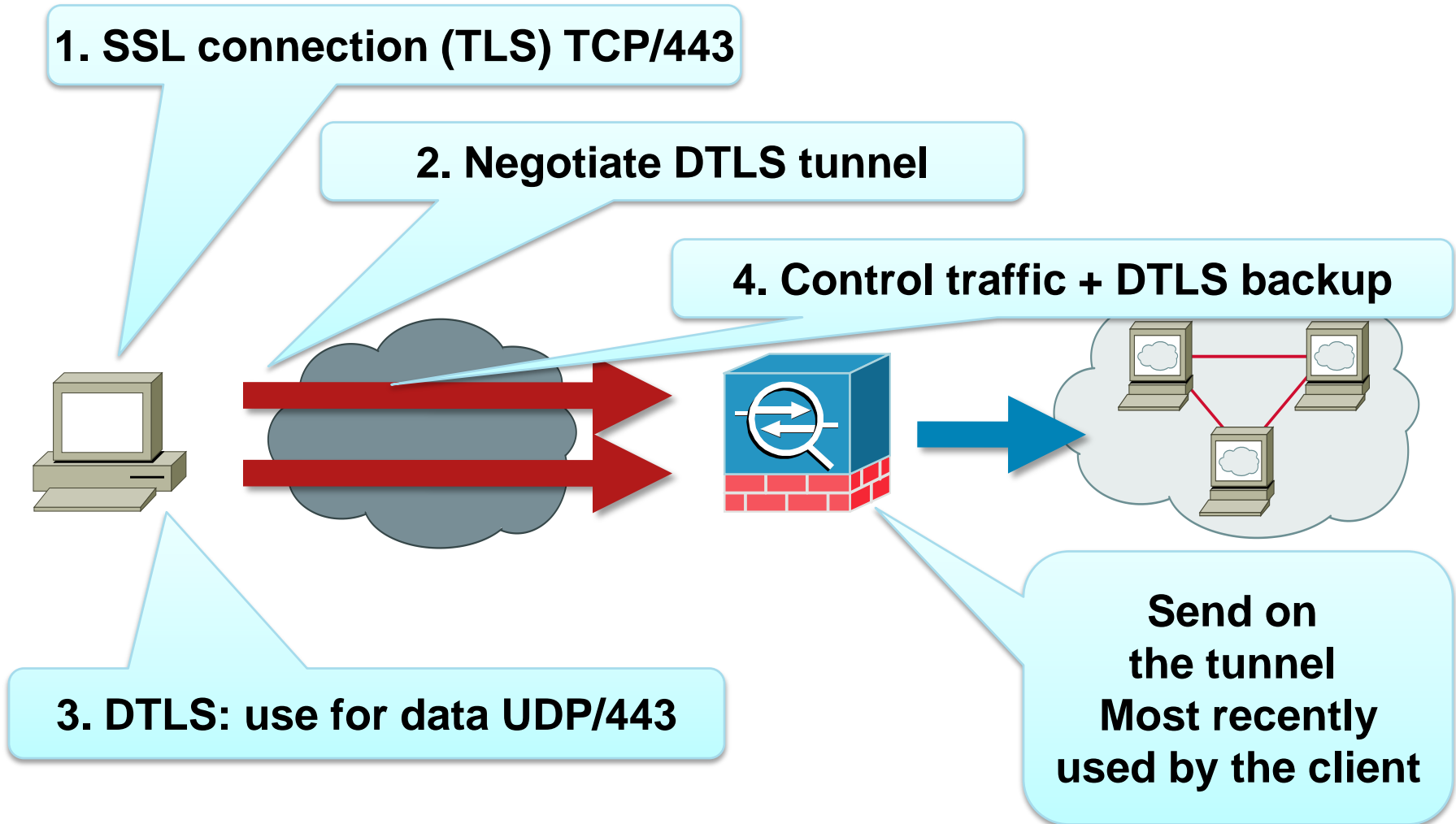
Why TLS Is Not Enough? Realtime Traffic



SSL VPN with AnyConnect

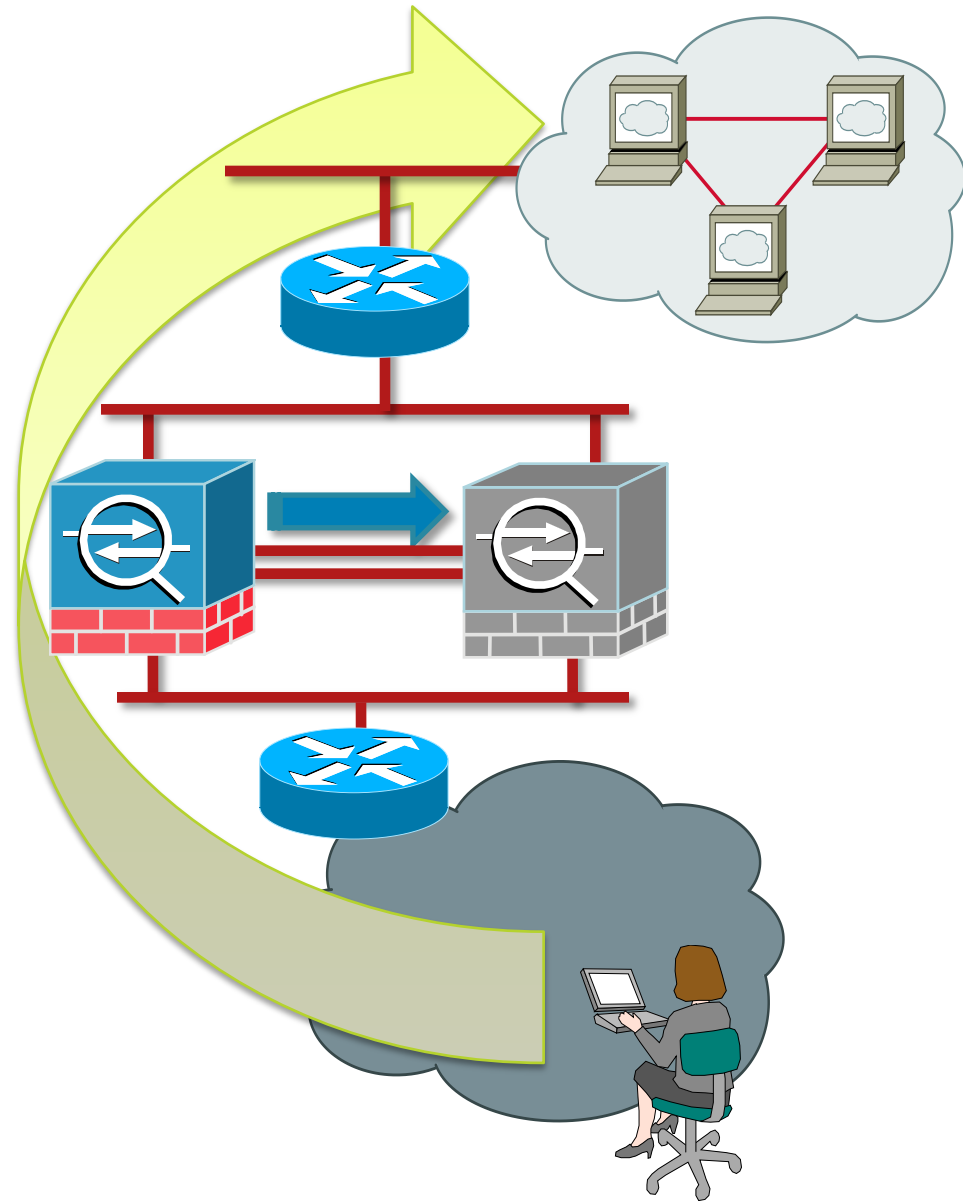


SSL + DTLS Tunnels



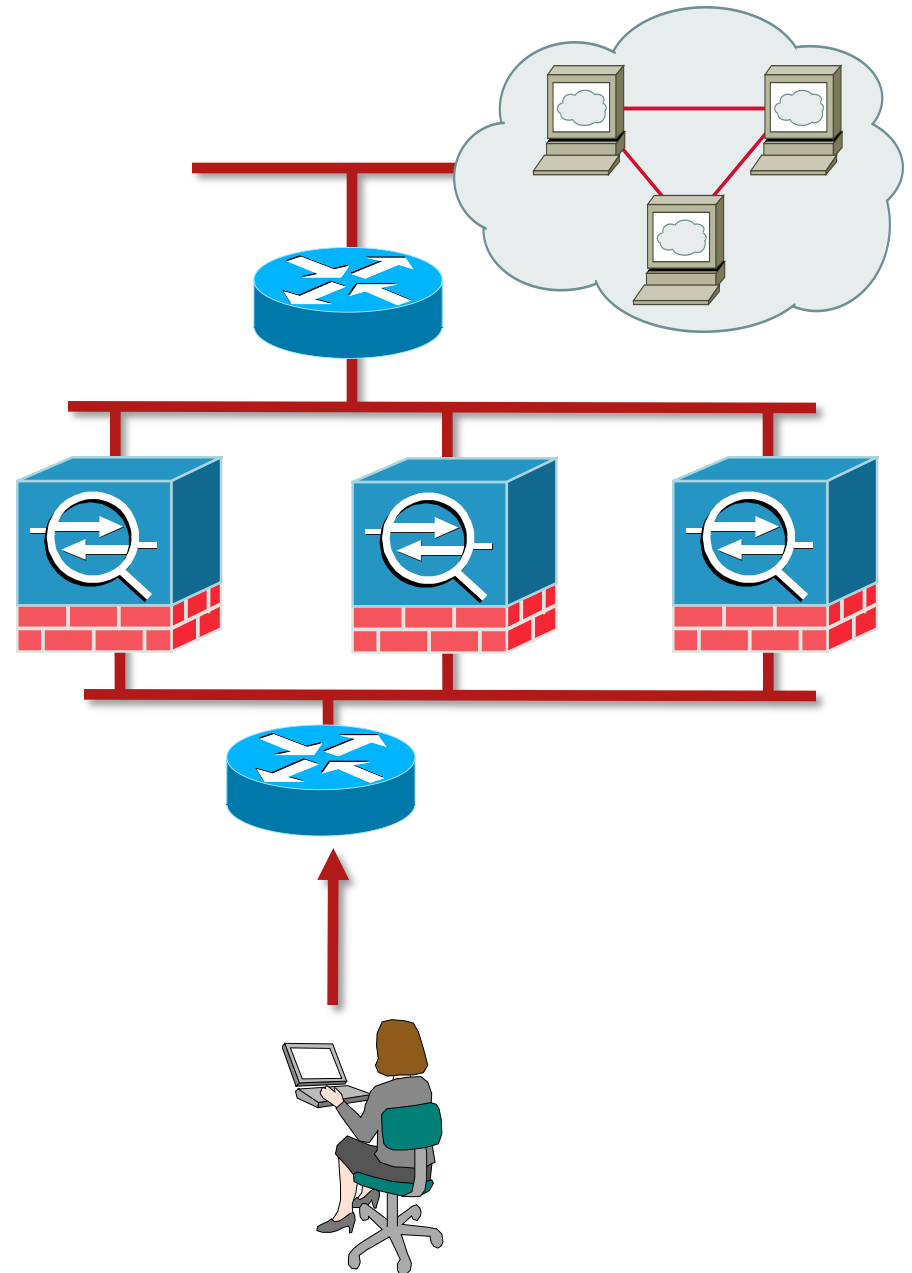
Failover

- AnyConnect with SSL and VPN Client with IPSec failover is stateful



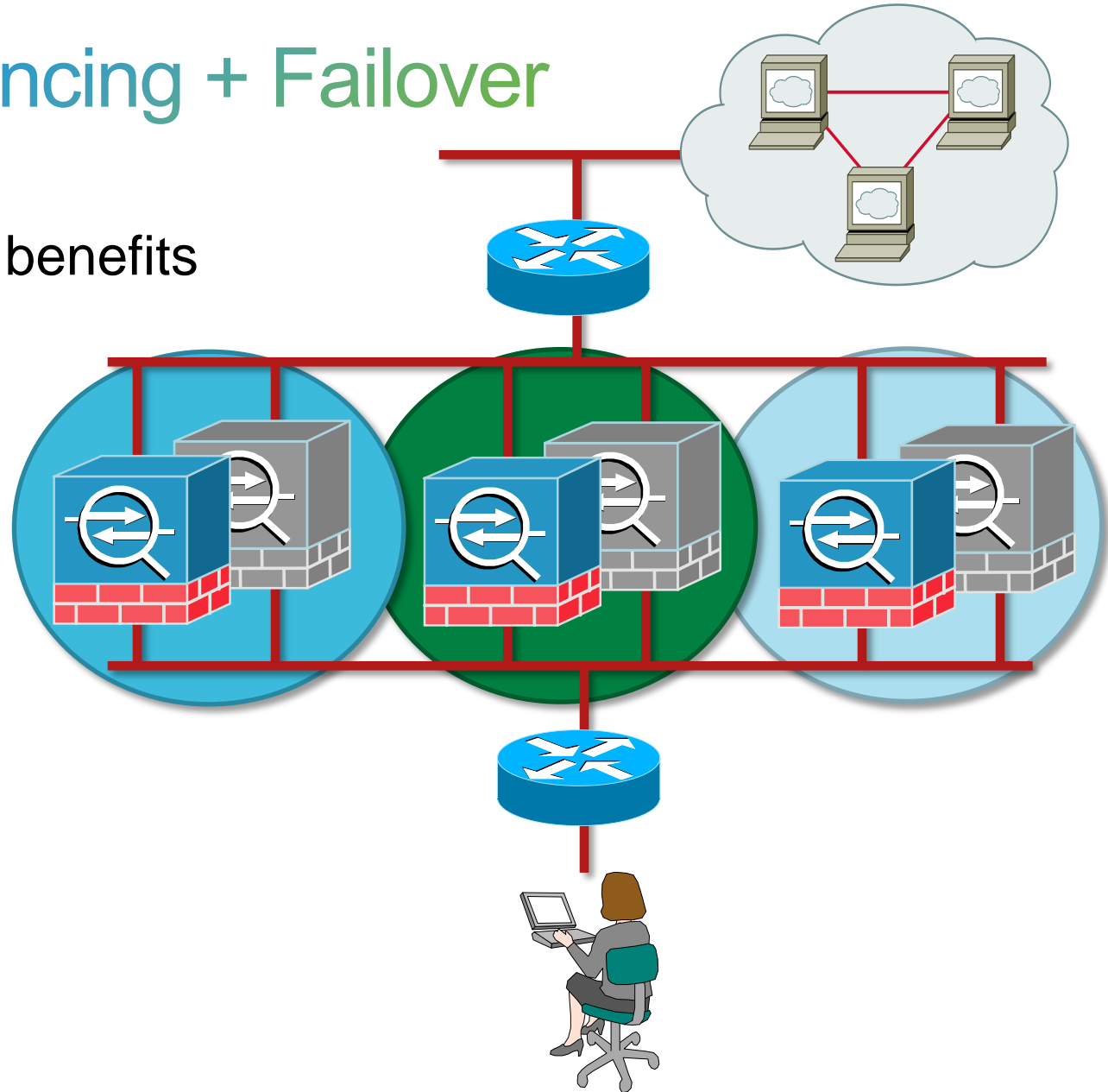
Load-Balancing

- Master ASA redirects the connections
- Distribute the load in 1% increments



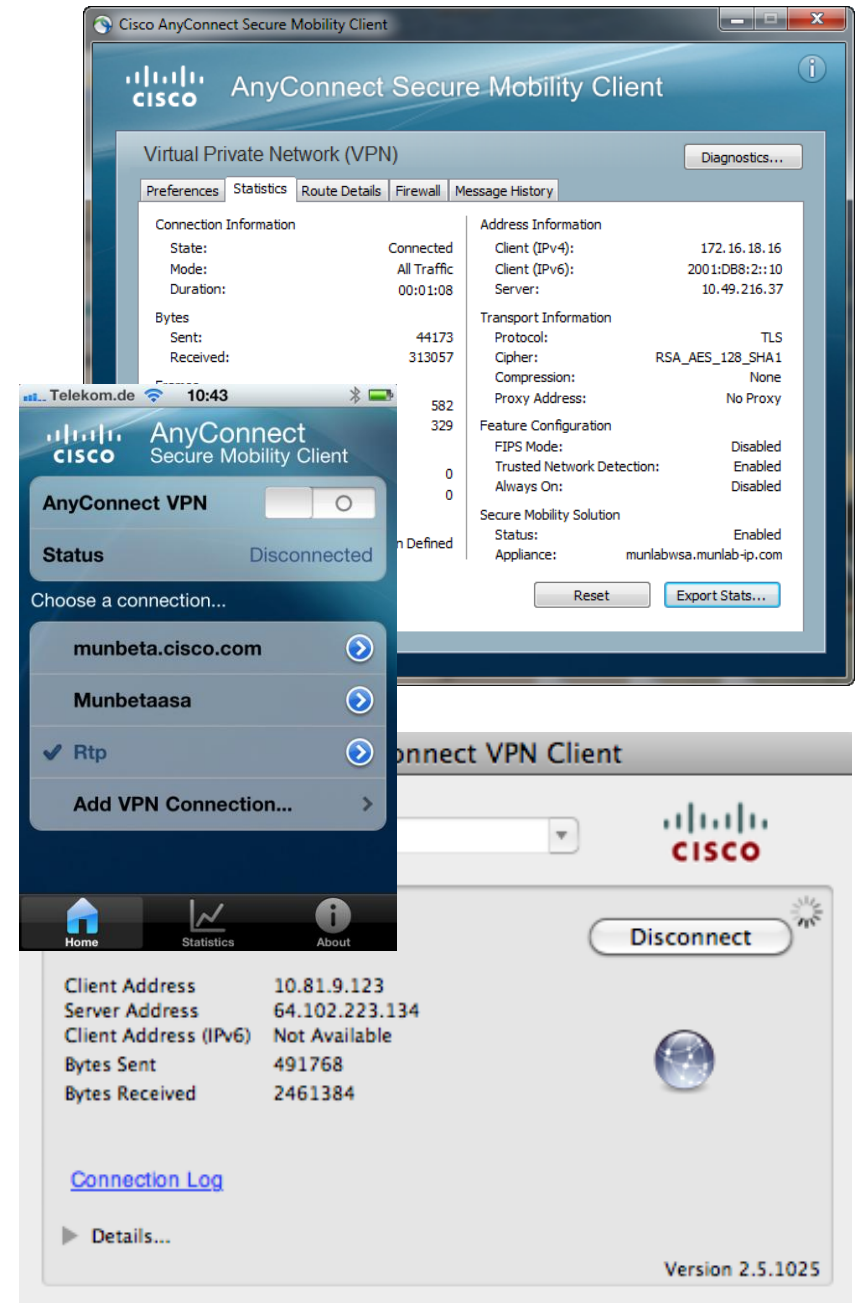
Load-Balancing + Failover

- Combine the benefits



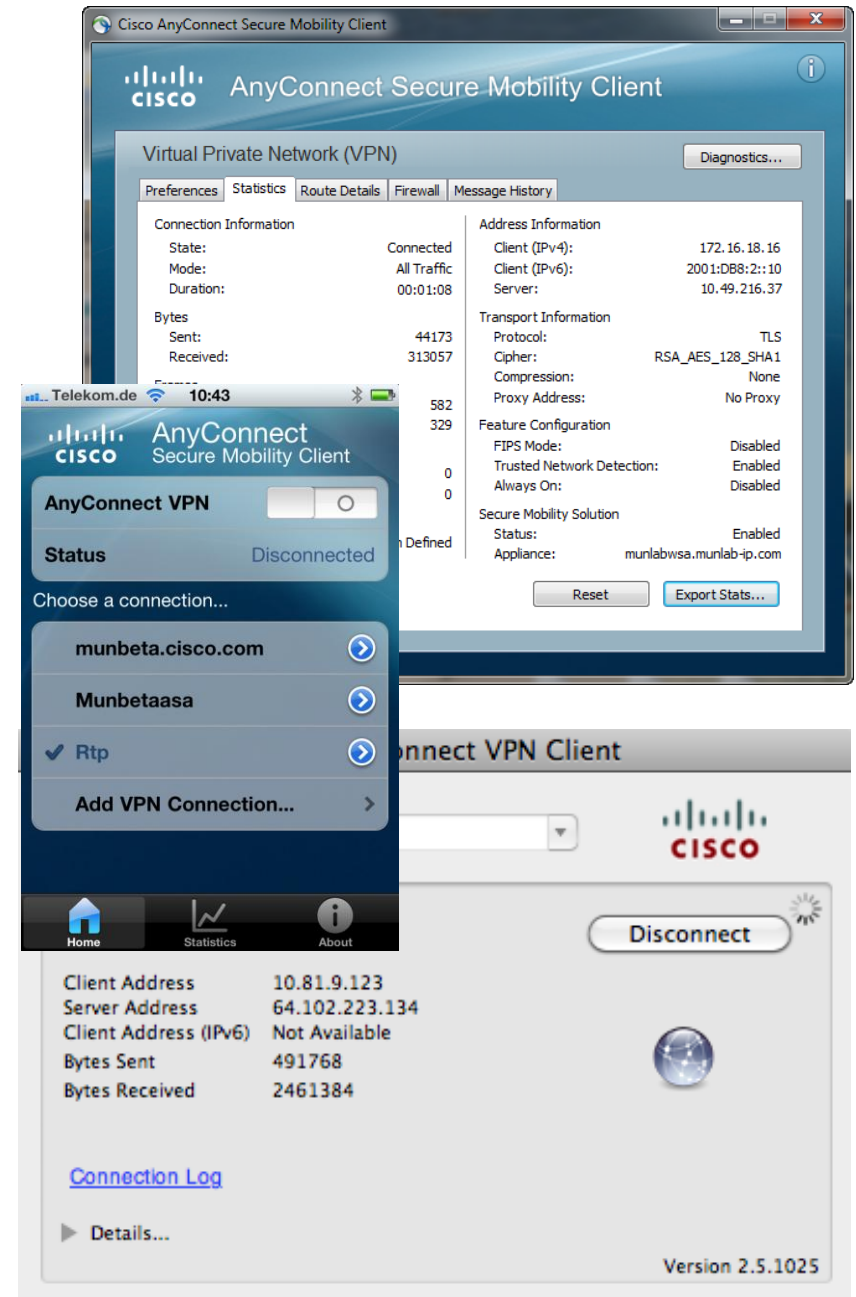
AnyConnect 3.0

- Supported on
 - Windows 32-bit & 64 bit, XP, Vista , W7
 - Linux w 2.6 Kernel
 - Mac OSX 10.5 & 10.6
 - Windows Mobile 5,6 & 6.1
 - iPhone OS 4.1 (version 2.4)
 - iPad OS 4.2
 - Samsung Galaxy S II - Android***
- Encryption
 - SSL with DTLS
 - IPSEC with IKEv2



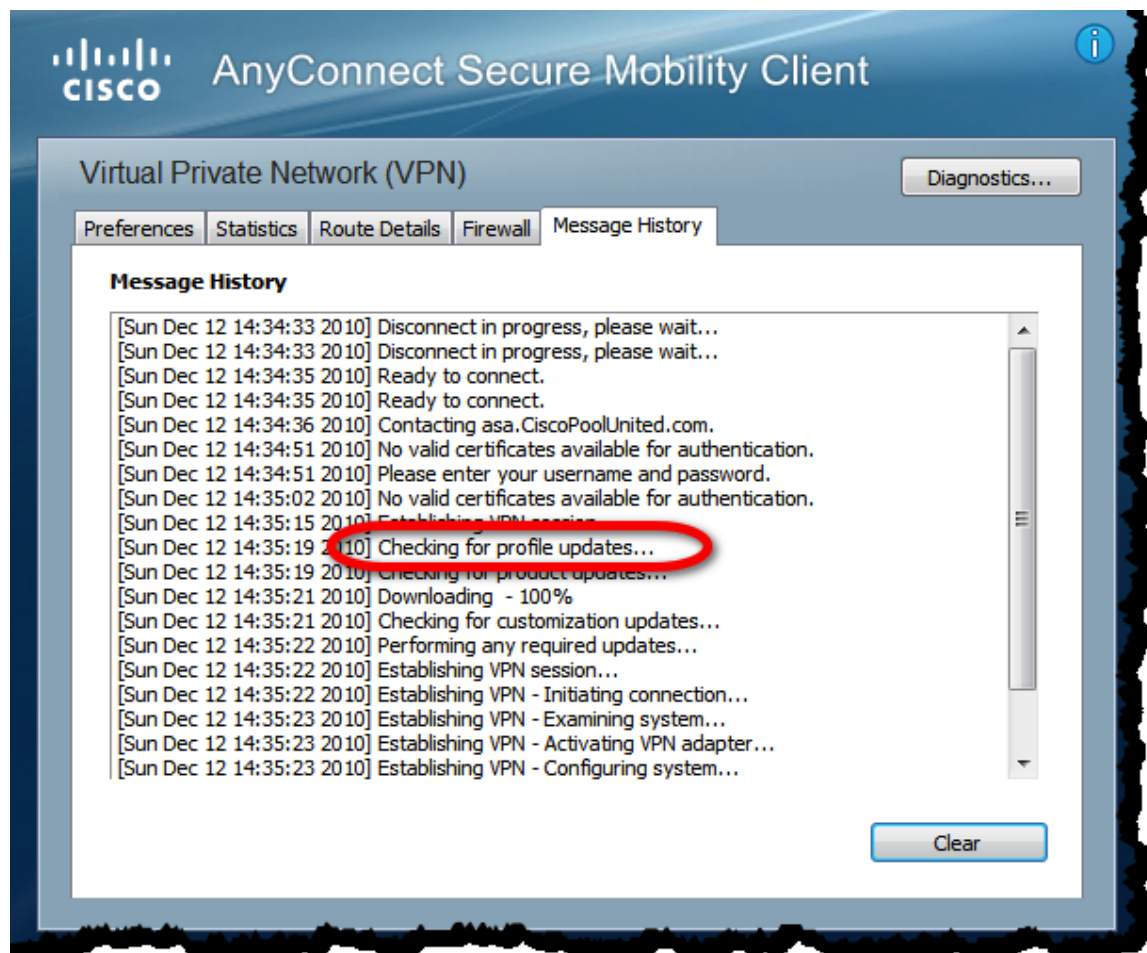
AnyConnect 3.0

- Features for Secure Mobility
 - Optimal Gateway Selection
 - AlwaysON
 - Location awareness
 - Captive Portal Detection
- Personal Firewalling
 - No Personal Firewall integrated
 - OS Firewalls can be configured & managed centrally through ASA
 - Windows & Mac



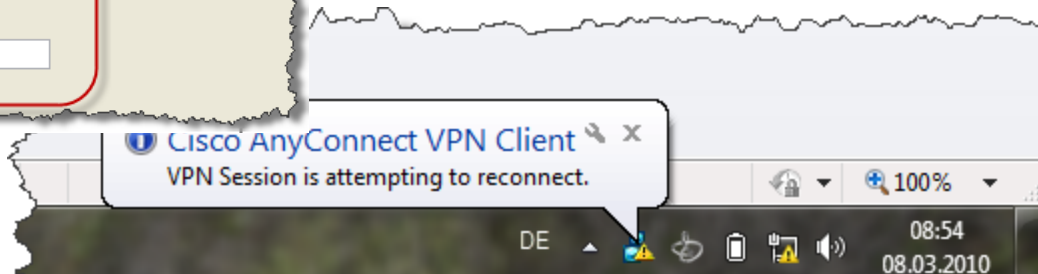
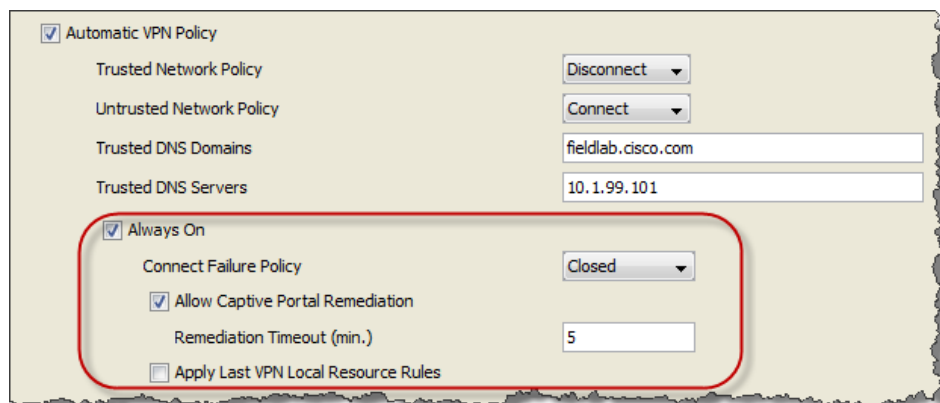
On the Client: AnyConnect Profile

- Profile is loaded automatically on the Client during connect
- At connect, checksum of profile is verified
- Tampered Profile gets replaced



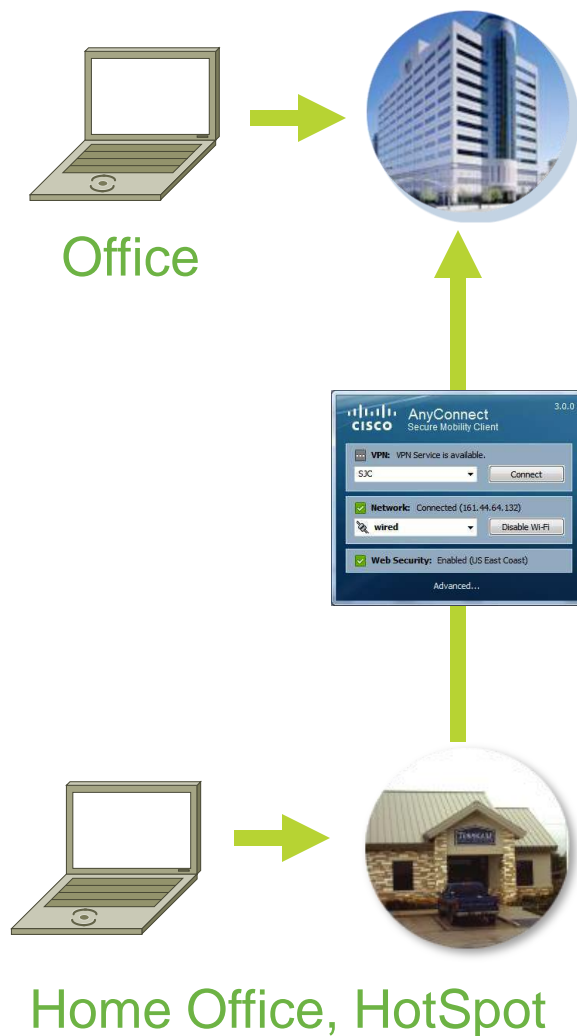
AlwaysOn

- Client Connection is kept both on ASA and on the Client
- If PC is coming back from Standby or is changing network, Client re-authenticates silently using a signed Cookie
- User does not need to manually reconnect



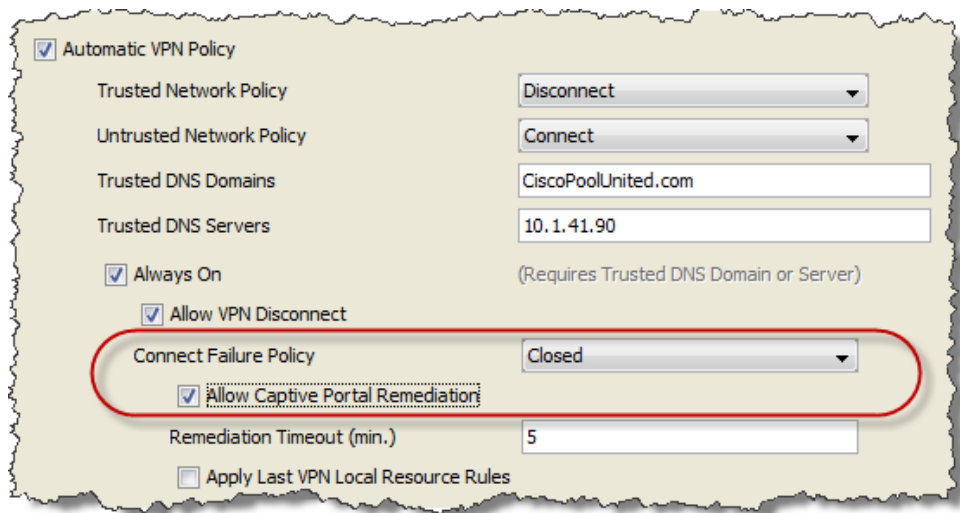
Trusted Network Detection (TND)

- Trusted Network Detection is Configurable via the AnyConnect Profile
- Trusted Networks can be Defined as DNS Suffixes or DNS Server IP Addresses
- DNS Suffixes and DNS Server IP addresses must be defined dynamically (DHCP) on the client
- If both, the trusted DNS Suffix and DNS Server IP address are defined, the entries will be ANDed to determine the Trusted Network



Captive Portal Detection

- Captive Portal Detection allows User to authenticate to a HOTSPOT Portal
- AnyConnect discovers CaptivePortal
- User has option to authenticate via Browser
- Connection of AnyConnect is resumed after successful authentication



Optimal Gateway Selection (OGS)

- Administrator Managed Feature
- Client determines the “nearest” ASA (a.k.a fastest response)
- OGS will initiate upon the following conditions:

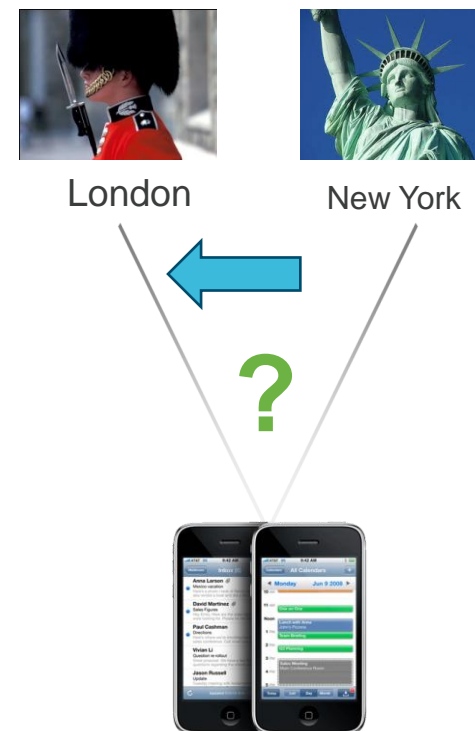
Prior to initial connection

Upon reconnects (ex. coming out of standby)

4 hours have elapsed since last connection

Will not switch ASA's when results are not faster by > 20%

- If ASA switch occurs, this results in a disconnect/connect



Client Firewall: ASDM Configuration

■ Public

Any physical interface that has direct connectivity to a network other than the VPN

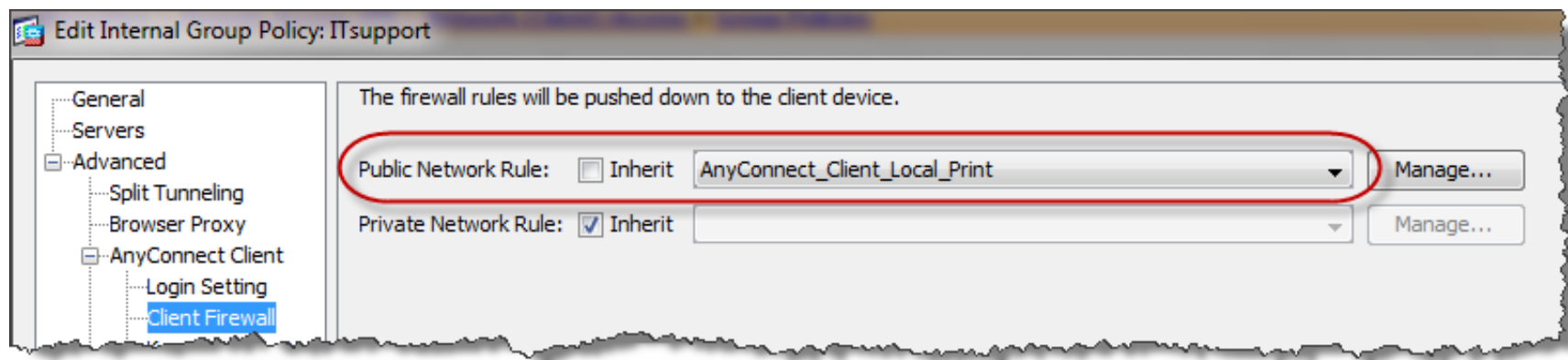
Only applied with a split tunneling configuration

If public rules can not be applied -> full tunneling will be applied.

■ Private

The Virtual Adapter interface

Rules are independent of the public interface



Client FW Rules



For Your Reference

Cisco AnyConnect Secure Mobility Client (beta)

AnyConnect Secure Mobility Client

Virtual Private Network (VPN) Diagnostics...

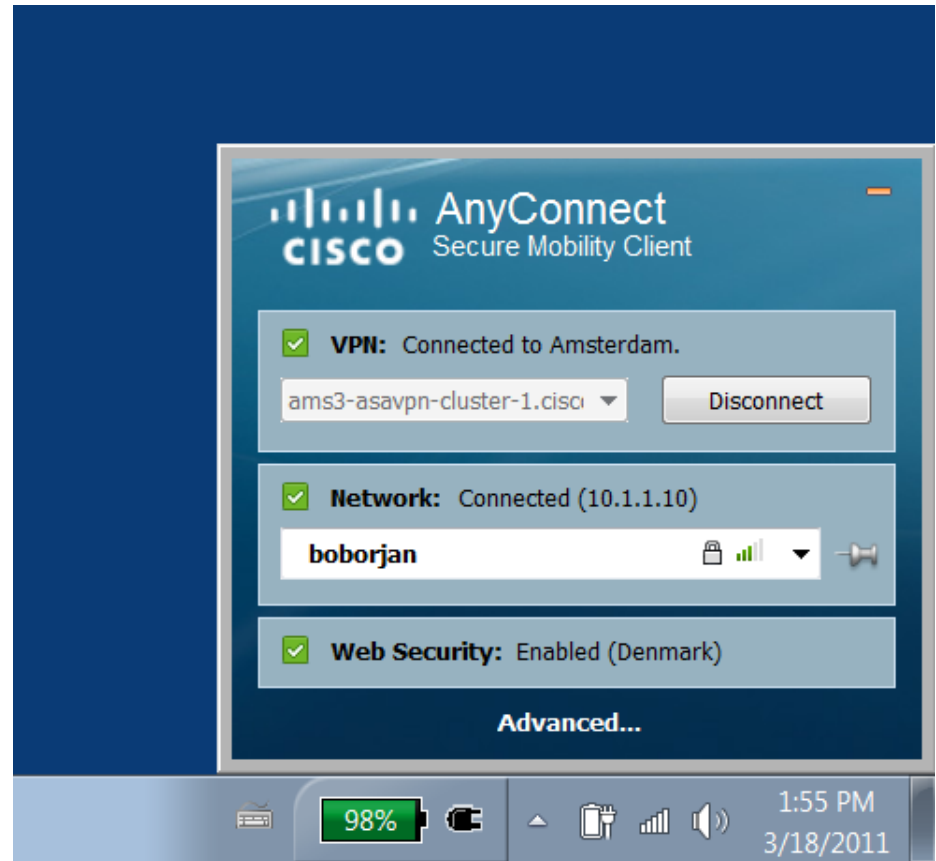
Preferences | Statistics | Route Details | **Firewall** | Message History

Firewall

Interface	Permission	Protocol	Source Port	Dest Port	Dest Address
Public	Allow	TCP	1-65535	515	0.0.0.0/0
Public	Allow	TCP	1-65535	631	0.0.0.0/0
Public	Allow	TCP	1-65535	9100	0.0.0.0/0
Public	Allow	UDP	1-65535	5353	224.0.0.251...
Public	Allow	UDP	1-65535	5355	224.0.0.252...
Public	Allow	TCP	1-65535	137	0.0.0.0/0
Public	Allow	UDP	1-65535	137	0.0.0.0/0
Public	Deny	ANY	1-65535	1-65535	0.0.0.0/0

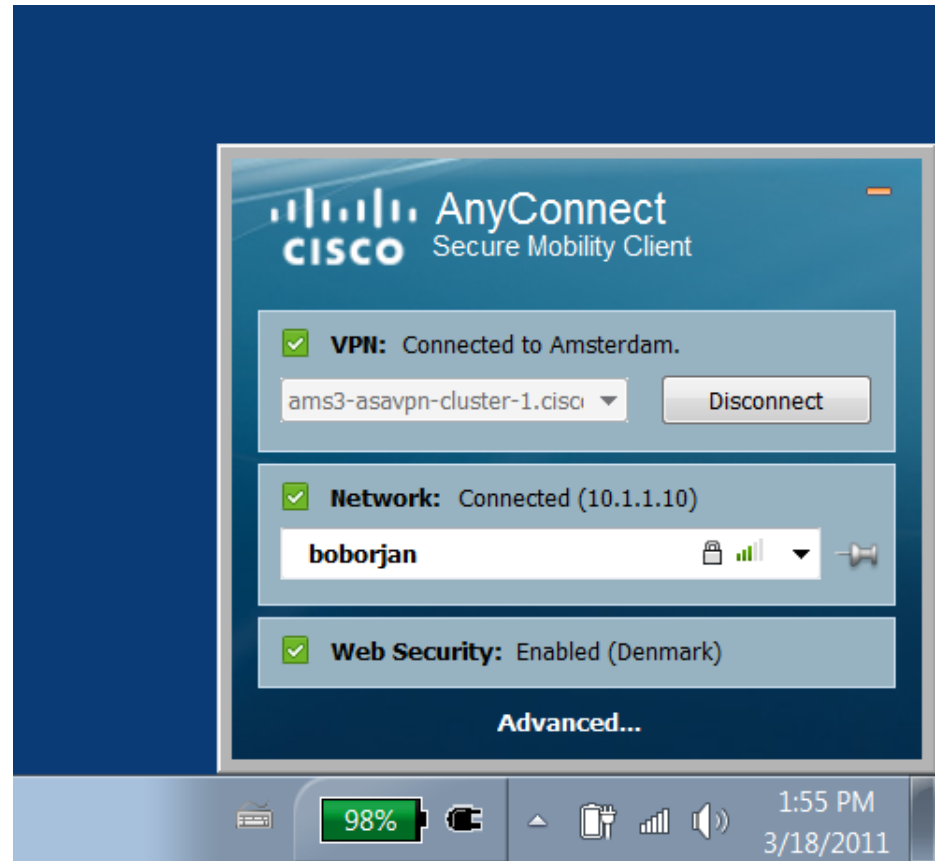
AnyConnect 3.0 GUI

- Windows-7 style GUI floating from right side of taskbar
- Supported on Windows 32-bit and 64-bit OS Versions (XP, Vista, W7, 2003/2008)
- Other OS Versions don't have new GUI, but still have AC 3.0
Mac OS X, Linux



AnyConnect 3.0 GUI

- Components displayed are modular
- Components can be centrally distributed from ASA, at initial install or at later point of time
- Some Components are OS dependant
 - Anywhere+
 - Telemetry
 - Network Access Manager



Profile Editor

Integrated in ASDM on ASA

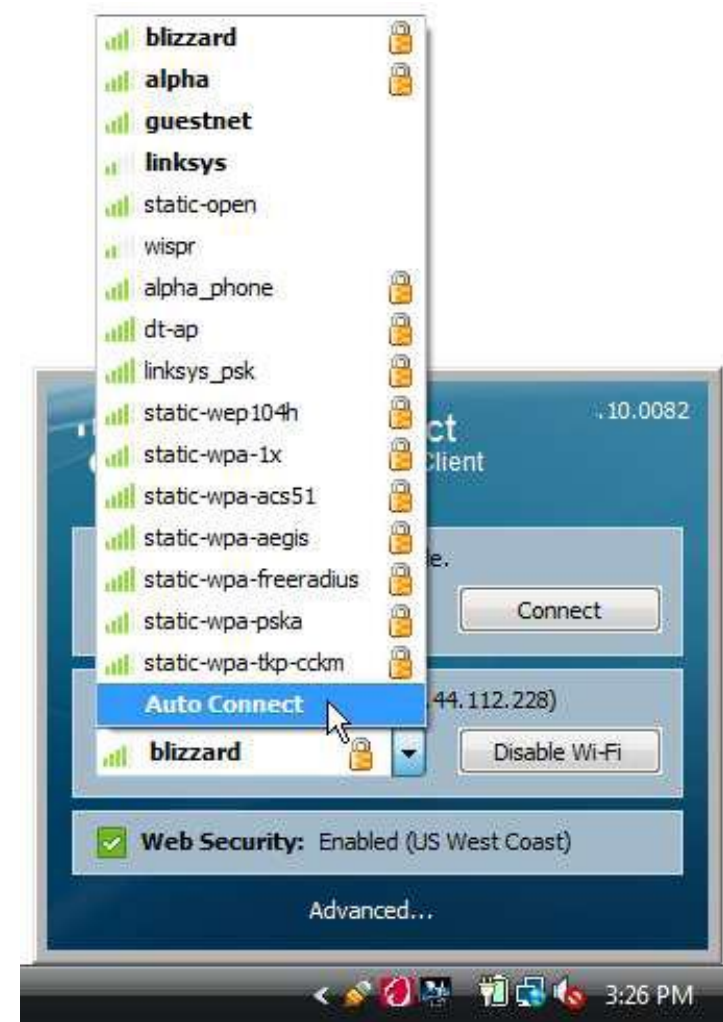
- Profile for VPN is ported from previous Versions
- Profiles for ScanSafe, NAM and Telemetry are new

The screenshot shows the Cisco ASDM 6.4 for ASA interface. The breadcrumb trail indicates the current location: Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. The main content area contains a table of AnyConnect Client Profiles.

Profile Name	Profile Usage	Group Policy	Profile Location
joe-tele	Telemetry		disk0://joe-tele.tsp
joe	Web Security	DfltGrpPolicy	disk0://joe.wsp
joe-vpn	VPN	DfltGrpPolicy	disk0://joe-vpn.xml
joe-nam	Network Access Man...		disk0://joe-nam.nsp

AC 3.0 with Network Access Manager

- Connection Management for Layer 2
 - Windows XP (32 bits)
 - Windows Vista and 7 (32/64 bits)
- Wired (802.3) and wireless (802.11) connectivity
- 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 with MACsec

- AnyConnect 3.0 provides
 - Unified access interface for SSL-VPN, IPSec and 802.1X for LAN / WLAN
 - Supports MACsec / MKA data encryption in software (Performance CPU-dependent)
 - MACsec capable hardware (network interface) enhances performance

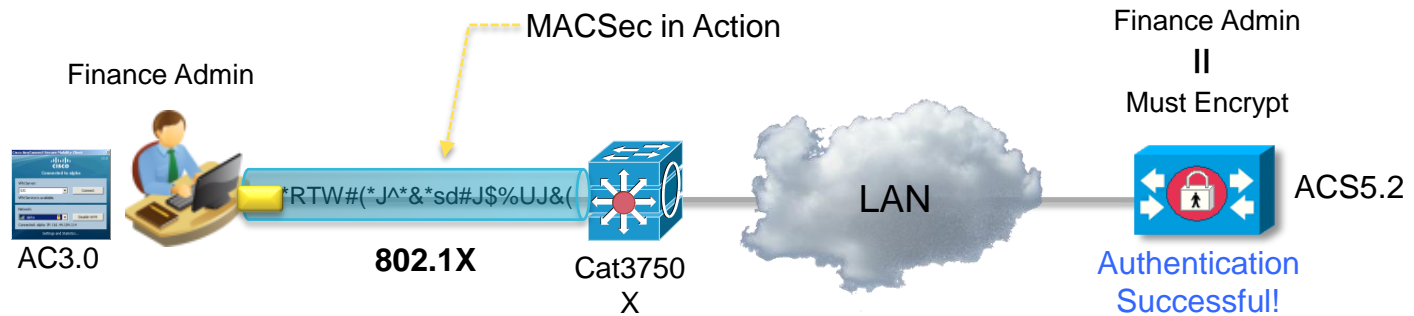


MACsec-ready hardware:

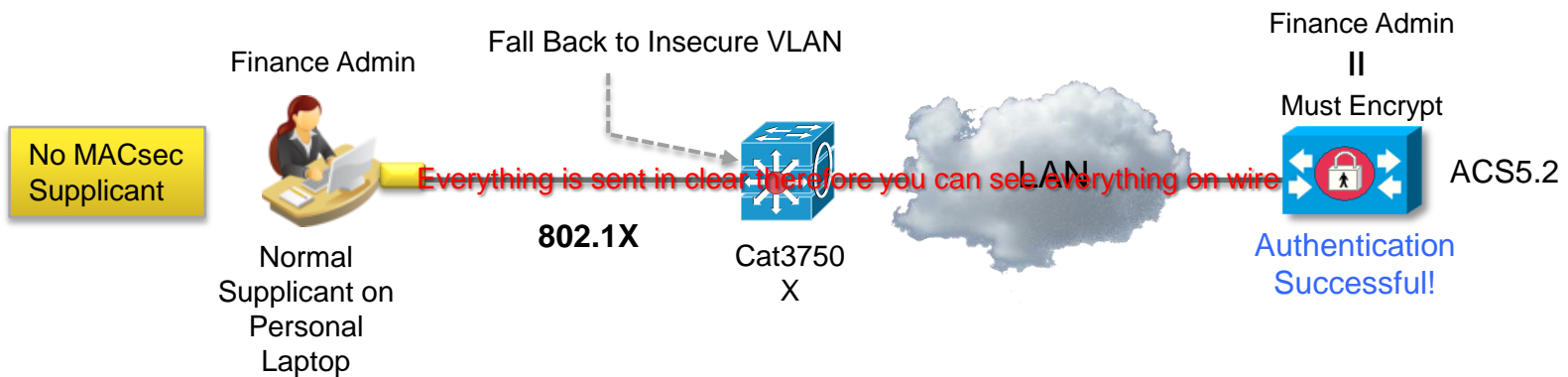
Intel 82576 Gigabit Ethernet Controller
Intel 82599 10 Gigabit Ethernet Controller
Intel ICH10 - Q45 Express Chipset (1Gbe LOM)
(Dell, Lenovo, Fujitsu, and HP have desktops shipping with this LOM)

Encryption with MACsec

Using AnyConnect 3.0



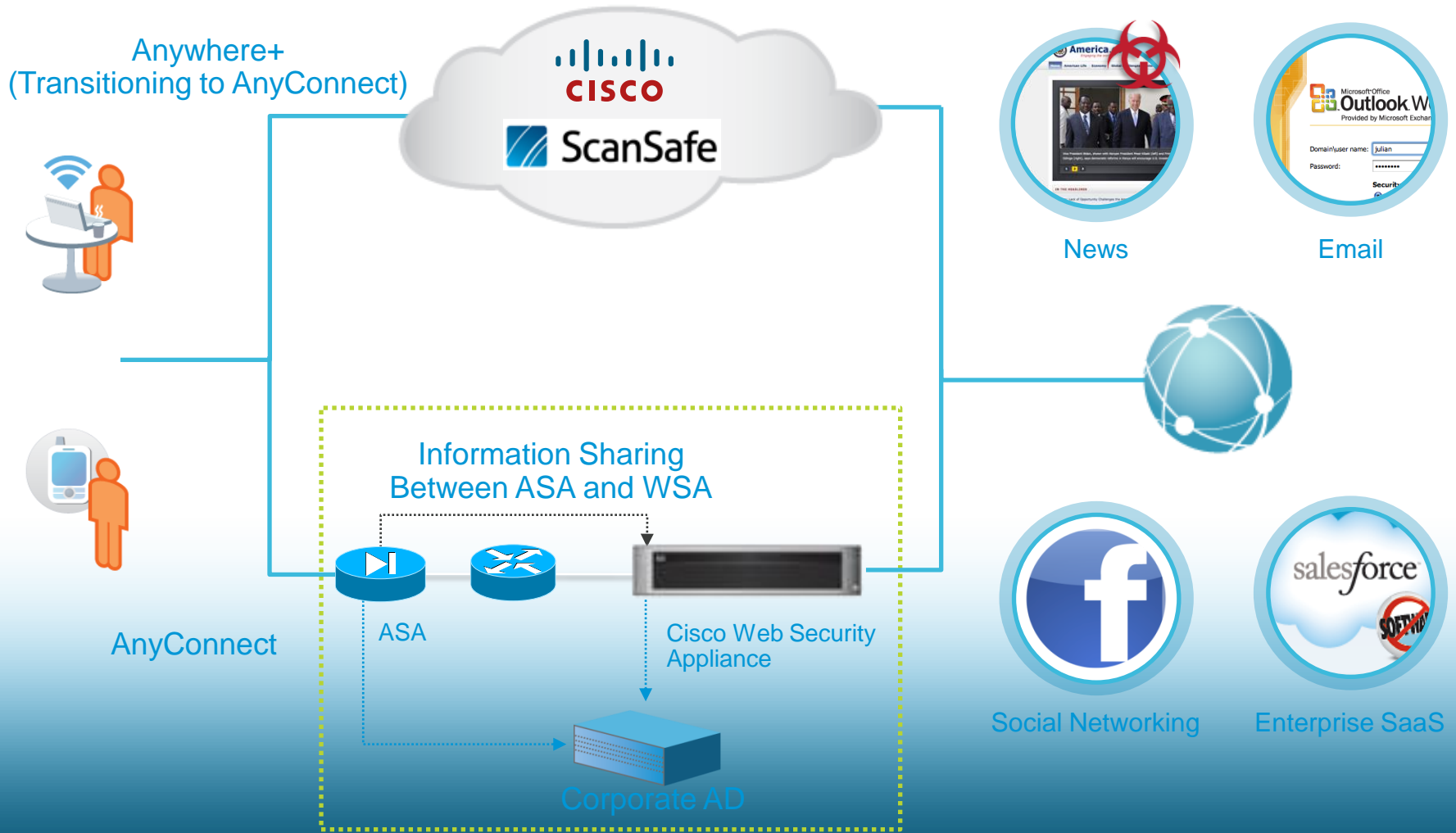
Using Normal Supplicant





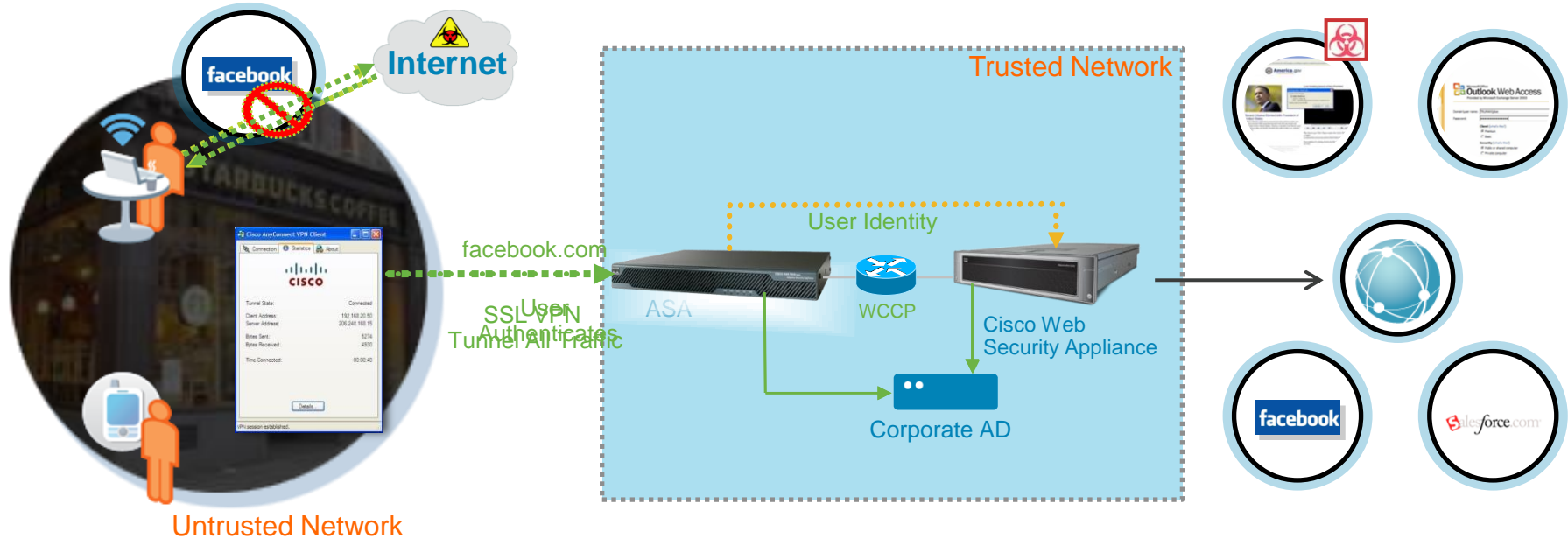
Web Security Deployment Methods

Flexible Delivery Appliance, Cloud & Hybrid



Persistent Security and Policy Enforcement Seamless User Experience

Always-On VPN



AnyConnect

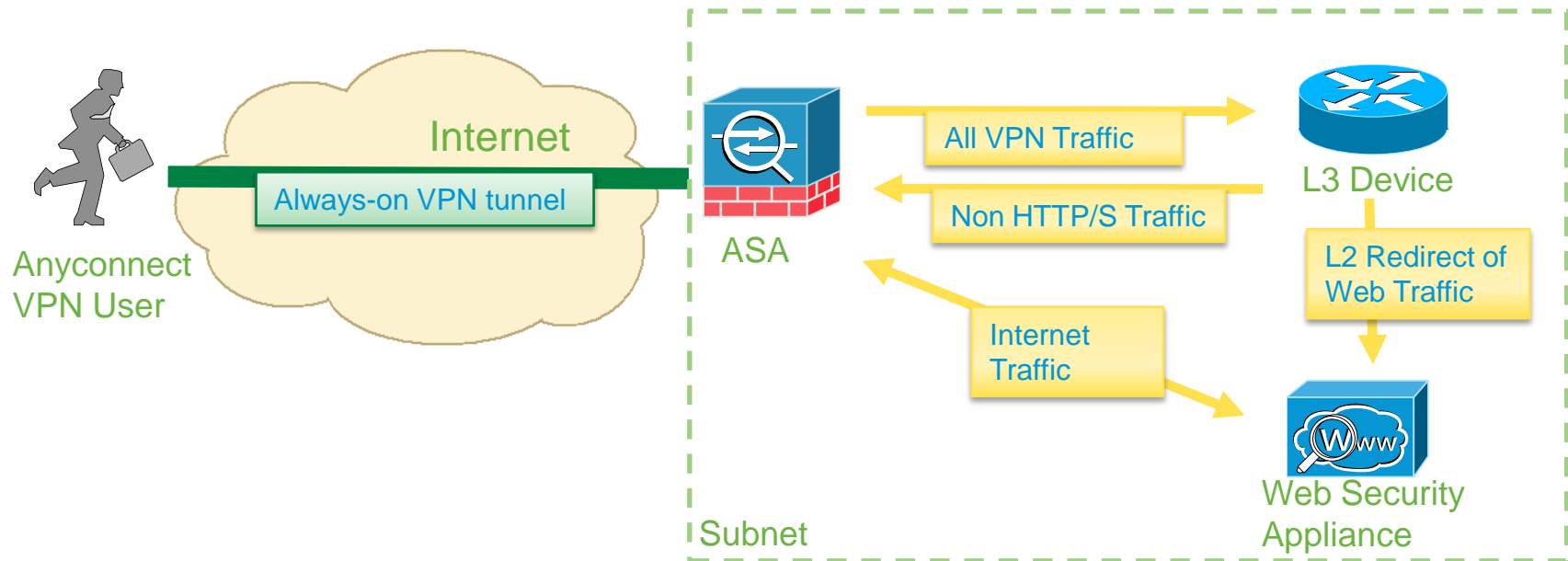
- Always-on VPN (admin configurable)
- Optimal head end auto-detect
- Transparent auth (certificate)

ASA → WSA

- Authentication handoff (SSO)
- Identity and location aware policy enforcement
- Location-aware reporting

Secure Mobility Architecture 1

easiest case



- ASA has „tunnel default gateway“ to WCCP Router
- ASA performs NAT, acting as Internet Gateway
- WCCP Router forwards WEB traffic to WSA
- Non-Web traffic is sent to ASA
- WSA must have route to VPN Client IP Pool

Cisco IronPort Web Security Appliance

- Web Proxy incl. caching

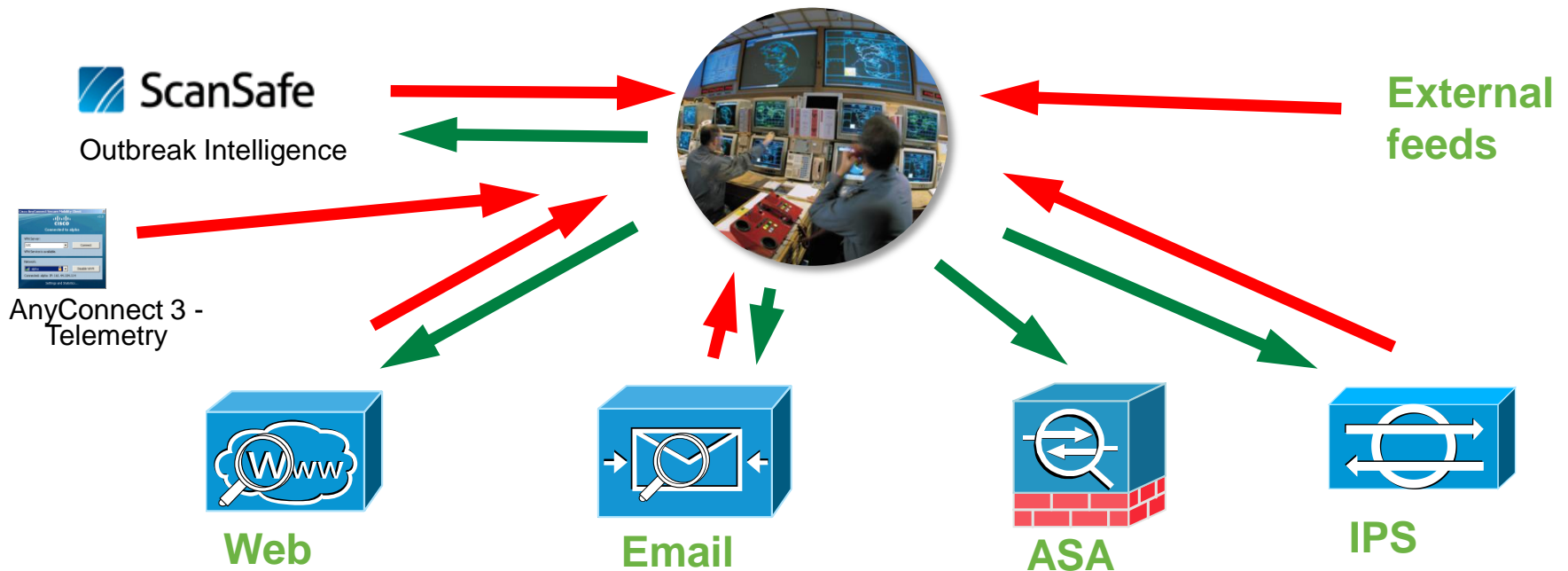


- Rich security functionalities
 - Reputation filtering
 - Malware scanning
 - Application visibility & control
 - HTTPS inspection
 - Authentication
 - Reporting and tracking



About Reputation

- Cisco SIO gathers statistical (telemetry) informations from Cisco Products and other resources
- Cisco SIO correlates informations
- Updated informations are delivered back to appliances
- Each IP / URL gets a score, ranging from -10 to +10



Examples: Reputation Values

- Known Botnet or Phishing Site

<http://tubezz.org/>

CONTENT TYPE: -

URL CATEGORY: Uncategorized
URLs

DESTINATION IP: No IP for this
transaction

DETAILS: PO.FIELDLAB "Access". WBSR: -8.8, Threat: Othermalware, Reason: Identified as a phishing or spam-related site. Domain reported and verified as serving malware.

- Agressive Advertising

http://pub.clicksor.net/newServing/js/show_ad.js

CONTENT TYPE: text/javascript

URL CATEGORY: Advertisements

(3)

DESTINATION IP: 64.102.255.40

DETAILS: PO.FIELDLAB "Access". WBSR: -5.8, Threat: Adware, Reason: Identified malicious behavior on domain or URI. Domain is associated with risky or of fensive content.

▶ RELATED TRANSACTIONS

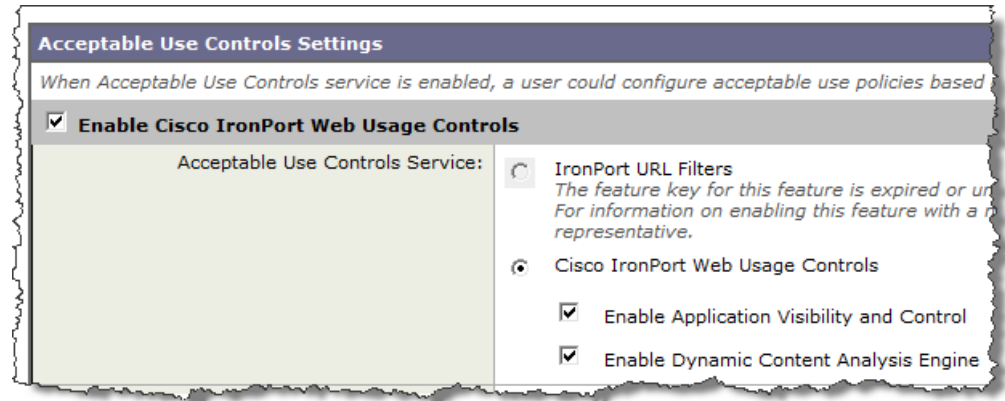
Filtering the URLs

- Filtering the URLs based on predefined Categories
- Possible Actions : Block, Monitor, Warn, Time-Based

Predefined URL Category Filtering					
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>					
Category	Use Global Settings	Override Global Settings			
		Block	Monitor	Warn	Time-Based
		Select all	Select all	Select all	(Unavailable)
Adult		<input checked="" type="checkbox"/>			—
Advertisements			<input checked="" type="checkbox"/>		—
Alcohol and Tobacco			<input checked="" type="checkbox"/>		—
Arts and Entertainment			<input checked="" type="checkbox"/>		—
Business and Industry			<input checked="" type="checkbox"/>		—
Cheating and Plagiarism			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	—
Child Porn		<input checked="" type="checkbox"/>			—
Computer Security			<input checked="" type="checkbox"/>		—
Computers and Internet			<input checked="" type="checkbox"/>		—
Cults			<input checked="" type="checkbox"/>		—
Dating		<input checked="" type="checkbox"/>			—
Dining and Drinking			<input checked="" type="checkbox"/>		—

Web Application Control

- Different Applications are detected by special Signatures
- Those Signatures are downloaded dynamically via SIO Updates
- No reboot or manual installation required!



twitter



facebook



Example from iPhone - Protection through WSA

Good Website



Benachrichtigung: Sicherheit: Malware-Risiko

Entsprechend der Zugriffsrichtlinien des Unternehmens (<http://www.full-antivirus-safety.com/>) wurde diese Website gesperrt, da sie laut der Web-Reputationsfilter ein Sicherheitsrisiko für Ihren Computer oder das Unternehmensnetzwerk darstellt. Diese Website kann Malware/Spyware enthalten.

Art des Sicherheitsrisikos: Othermalware

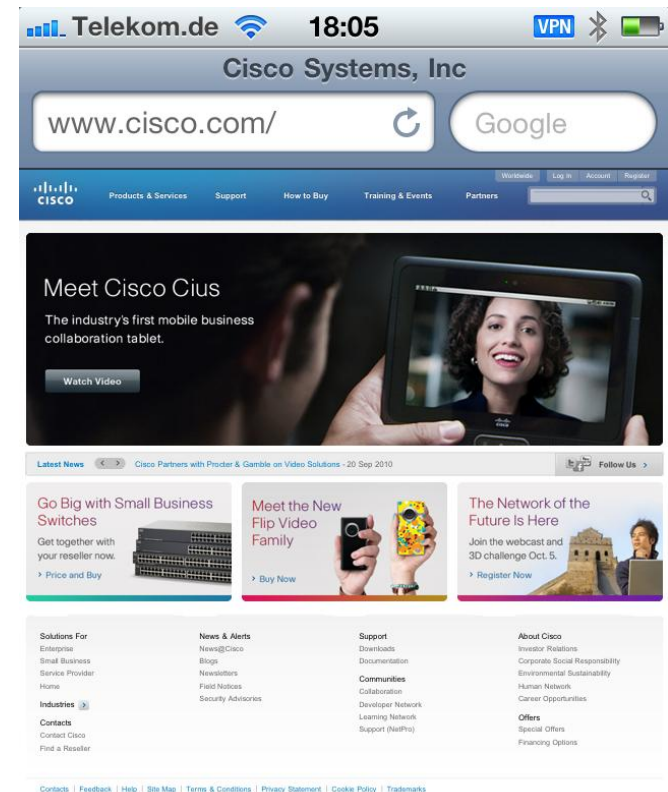
Grund für das Sicherheitsrisiko: Researchers or users identified possible threats.

Bei Fragen wenden Sie sich bitte an Maria Kron (cheers@prost.com), und geben Sie die unten aufgeführten Codes an.

Benachrichtigungscodes: (1, MALWARE, Othermalware, Researchers or users identified possible threats., BLOCK-MALWARE, 0x000035c5, [1285603539.452](#), AAAD6wAAAAAAAAAABf8ACP8AAAD/AAAAAAAAAAAAAAAAE=, <http://www.full-antivirus-safety.com/>)



Bad Website



Secure Mobility

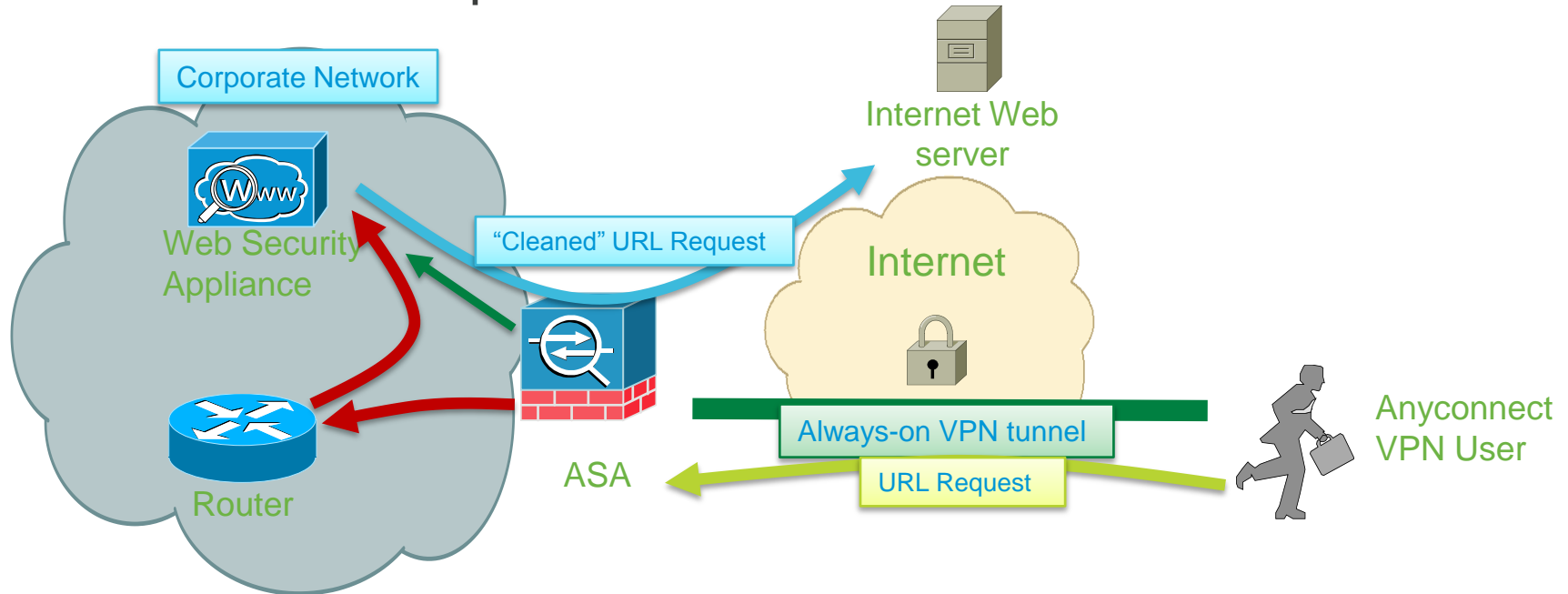
Functional Description

- Works with Cisco ASA and Cisco AnyConnect Client
- Cisco ASA authenticates the user at WSA
- WSA can use different policies for local and remote users
- WSA can use SAML 2.0 for Single Sign On to Webservices



Secure Mobility

Functional Description



ASA passes user information to WSA for authentication

AnyConnect user attempts to access internet webserver via always-on VPN

Traffic routed to inside router

URL Request redirected to Web Security Appliance (WSA). Traffic is checked by WSA against policy

"Cleaned" traffic forwarded to internet webserver

AnyConnect 3.0

Web Security for ScanSafe



- Keeps malware from getting to your system in the first place
- Tunnels HTTP/HTTPS traffic through ScanSafe cloud
- Fully localizable and translatable
- Fine-tunable web access policy management available
- Replacement for AnyWhere+ standalone client
- Does not need VPN connection!



ScanSafe Scalability & Reliability

Reliability

- 15 data centers
- Top tier certification
- Thousands of devices deployed
- 100% availability

Scale

- Billions of Web requests/day
- Highly Parallel processing
- Average <50 ms latency
- 10Gb connectivity
- Redundant network providers

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

Home Dashboard Web Virus Spyware **Web Filtering** Admin Reports Support

Management Notifications

Web Filtering > Management > Policy > Manage policy

Manage policy Edit a rule Create a rule

Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.

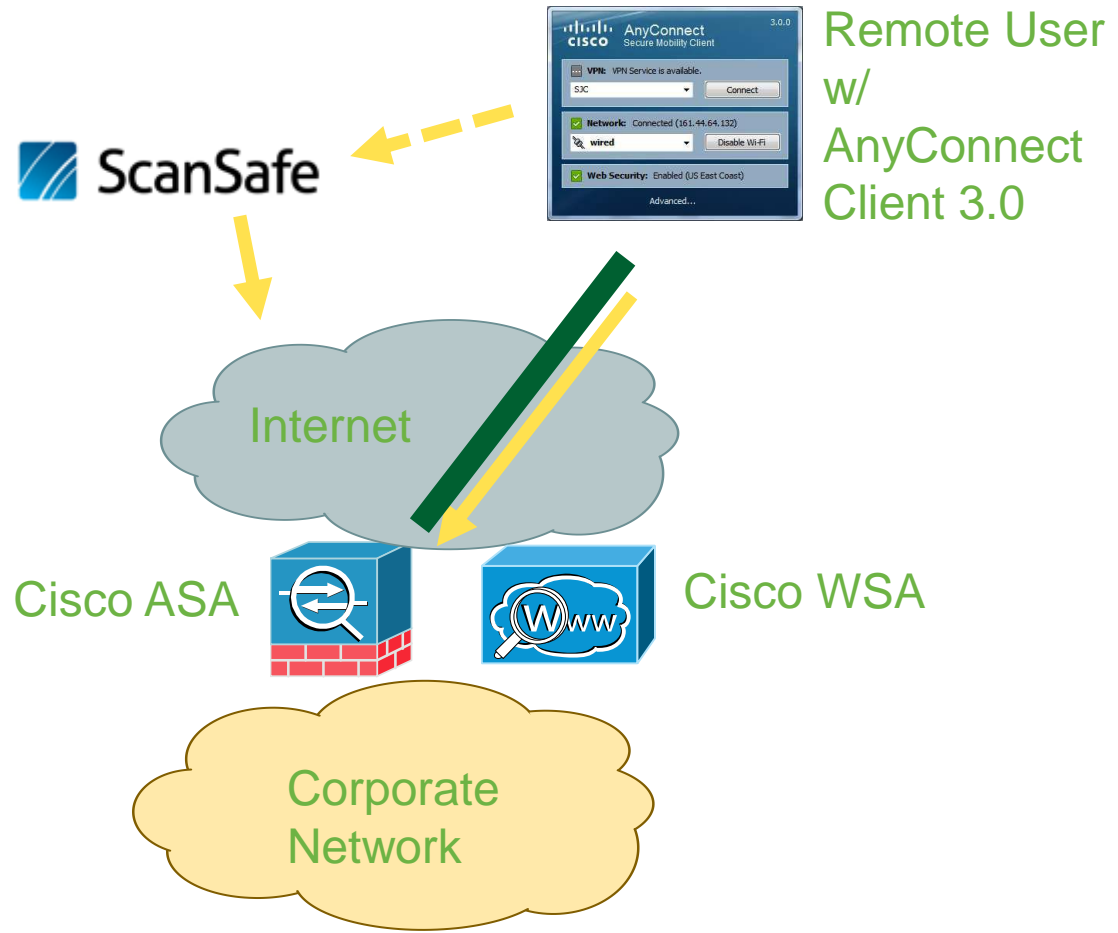
Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.

There is a maximum of 100 enabled rules allowed for the policy.

Company policy									
#	Move	Rules	Groups/Users/IPs	Filter	Schedule	Action	Active	Edit	Delete
1	↑ ↓	Colin-Foo-GPO	"Colin"	"Colin-Foo"	"anytime"	Block	<input checked="" type="checkbox"/>		
2	↑ ↓	shweta_rule_block	Anyone	"shweta"	"anytime"	Block	<input type="checkbox"/>		
3	↑ ↓	rpotts	"rpotts"	"rpotts"	"anytime"	Block	<input checked="" type="checkbox"/>		
4	↑ ↓	karan	"karan-group"	"karan"	"anytime"	Block	<input checked="" type="checkbox"/>		
5	↑ ↓	Domain	"WinNT://CISCO\" or "WinNT://CISCO\ Employees"	"Colin-Foo"	"anytime"	Block	<input checked="" type="checkbox"/>		
6	↑ ↓	websecurity-demo-rule	"websecurity-demo"	"websecurity-demo"	"anytime"	Block	<input checked="" type="checkbox"/>		
7	↑ ↓	finance-coach	"websecurity-demo"	"finance-coach"	"anytime"	Allow	<input checked="" type="checkbox"/>		
8	↑ ↓	automation	"automation"	"automation"	"anytime"	Block	<input checked="" type="checkbox"/>		
9		Default	Anyone	Anything	Anytime	Allow	<input checked="" type="checkbox"/>		

Secure Mobility Future – Hybrid Security

- Internet traffic secure through websecurity cloud service
- Corporate traffic secure through tunnel and WSA
- Consistent Policy and Monitoring





AnyConnect Demonstration



Live Q and A

Summary, AnyConnect provides

- Wide Operating Systems support
- Security and Mobility together
- Intelligent and seamless VPN (AlwaysON, DTLS, IKEv2)
- Context-aware policy and web security
- ScanSafe and Cisco IronPort collaboration
- Authentication (IEEE 802.1X supplicant) with data Confidentiality and integrity (IEEE 802.1AE, MACSec)



