

# What You Make Possible



# Understanding Secure Remote Access for Jabber

BRKUCC-2662

# BRKUCC-2662

- Jabber Solution Architecture
- Secure Remote Access
  - ASA / Anyconnect
  - VCS expressway
- Secure Remote Access Roadmap

# Jabber Solution Architecture



# Cisco Jabber Solutions

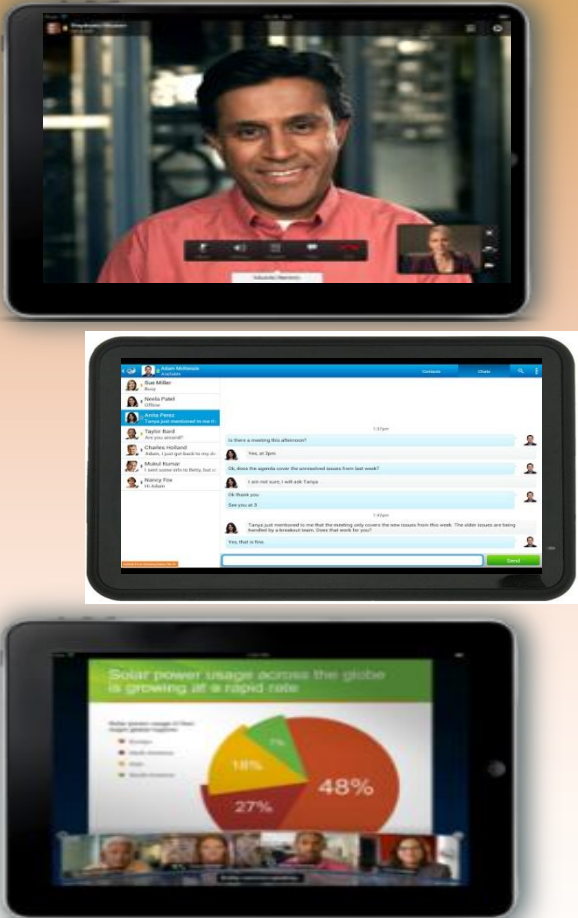
## Jabber Portfolio



### Win, Mac



### Tablet



### Smartphone

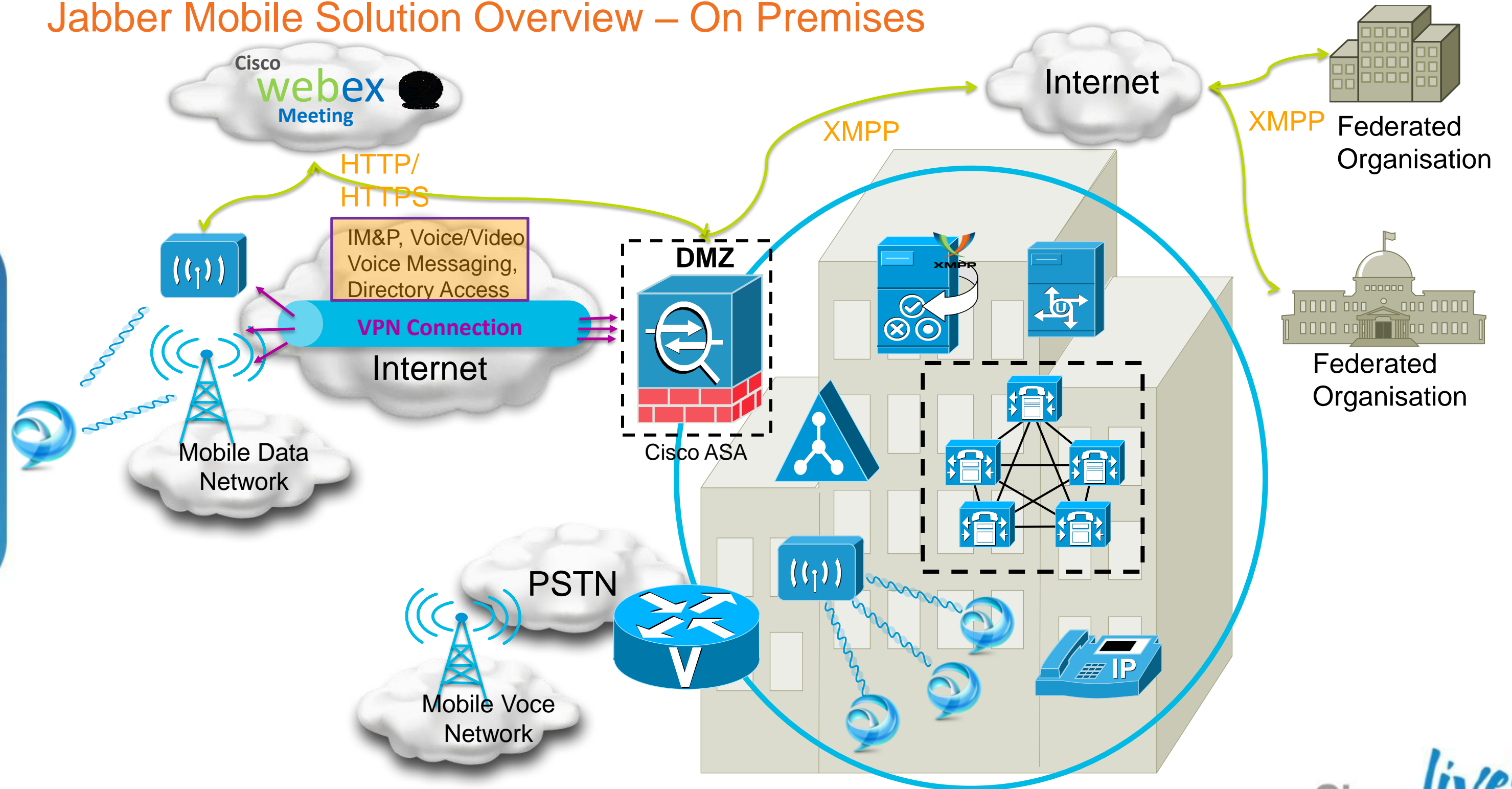


### Web SDK



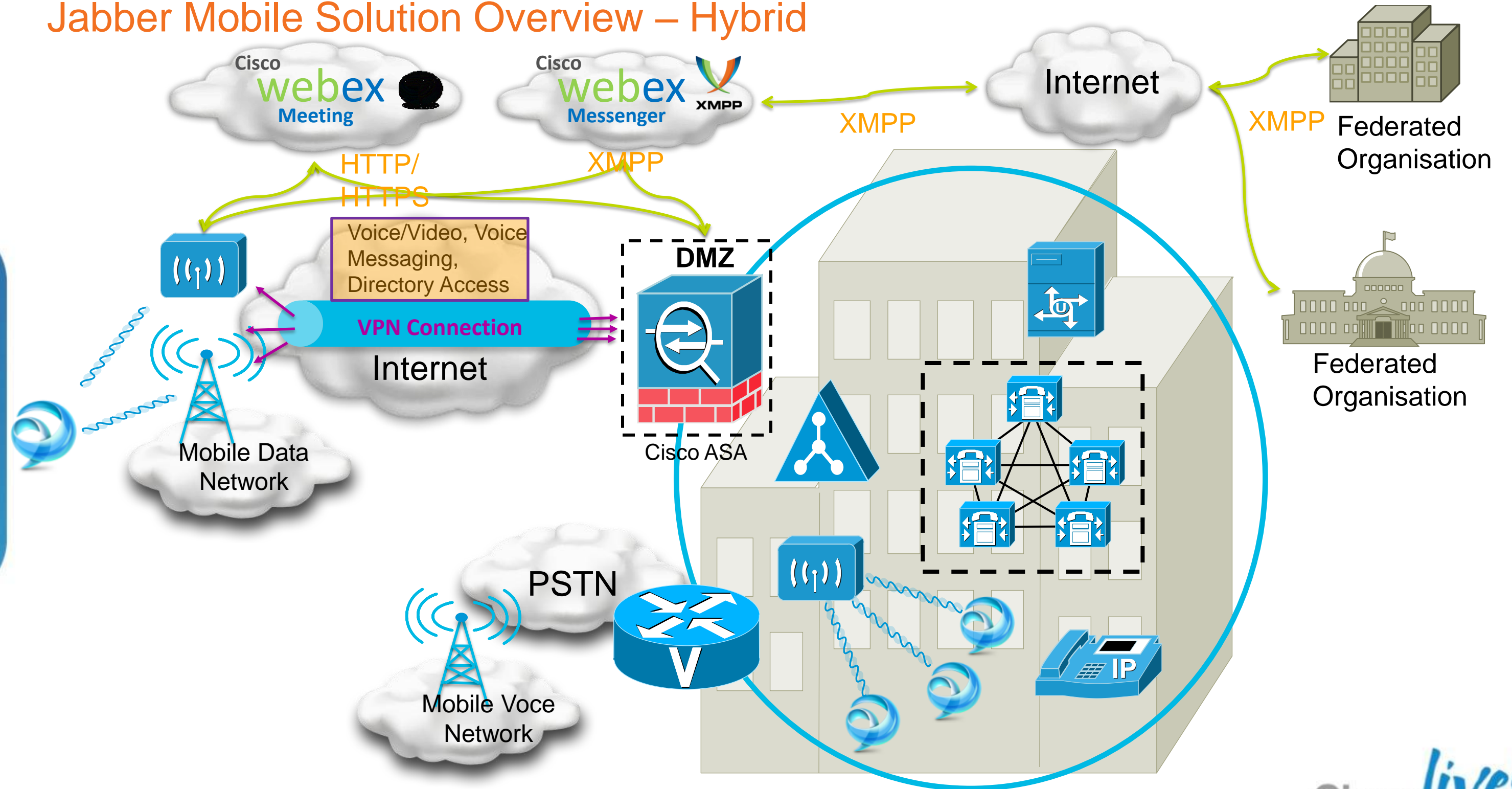
# Jabber Mobile Solution Architecture

## Jabber Mobile Solution Overview – On Premises



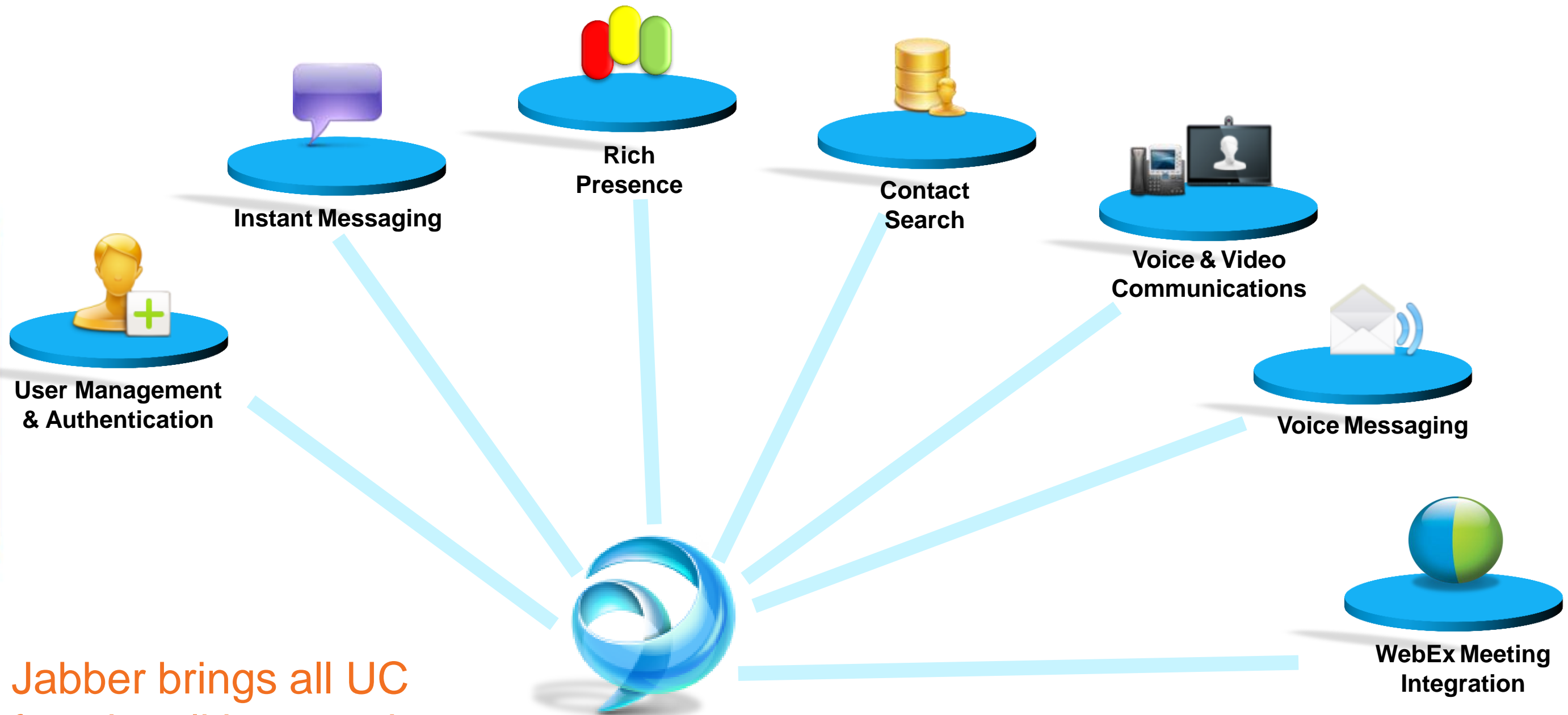
# Jabber Mobile Solution Architecture

## Jabber Mobile Solution Overview – Hybrid



# Jabber Solution Architecture

## Core Feature Functionalities



Jabber brings all UC functionalities together

Cisco *live!*



# Remote Access with ASA / Anyconnect

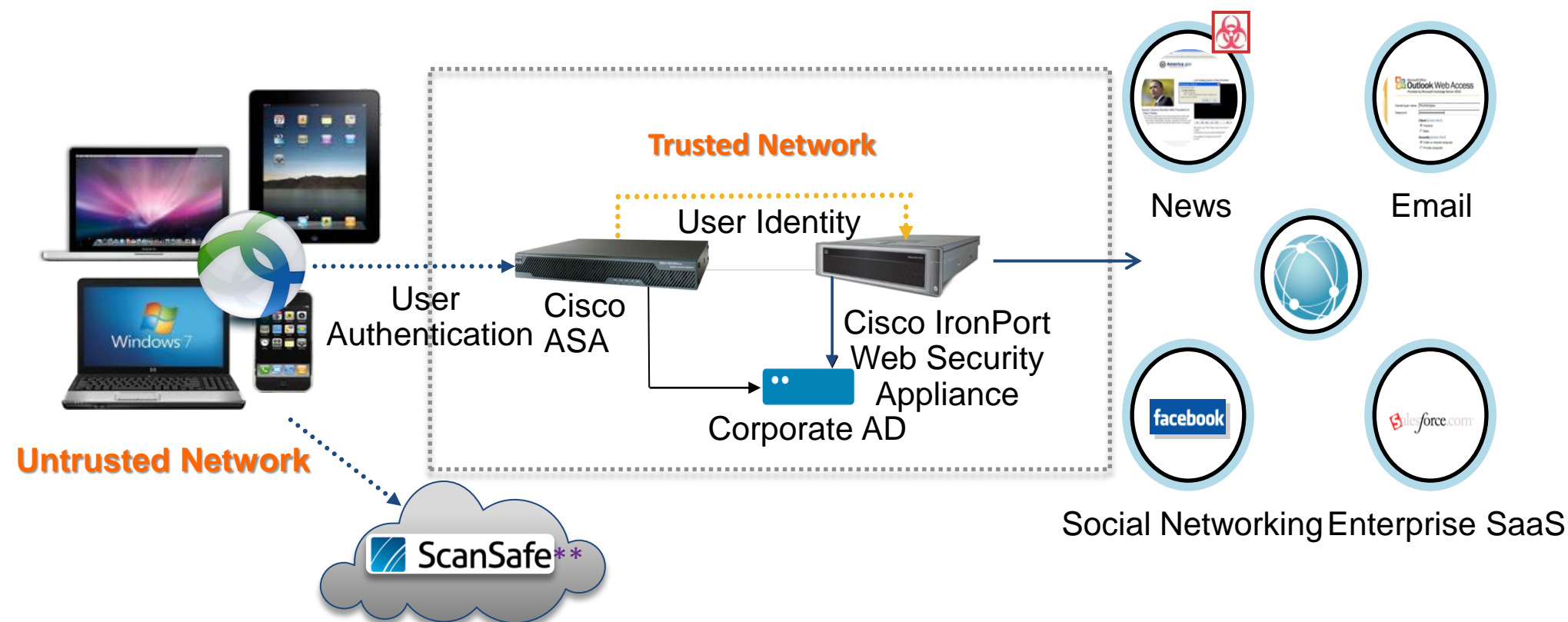


# Secure Remote Access

## Adaptive Security Appliance (ASA) and AnyConnect

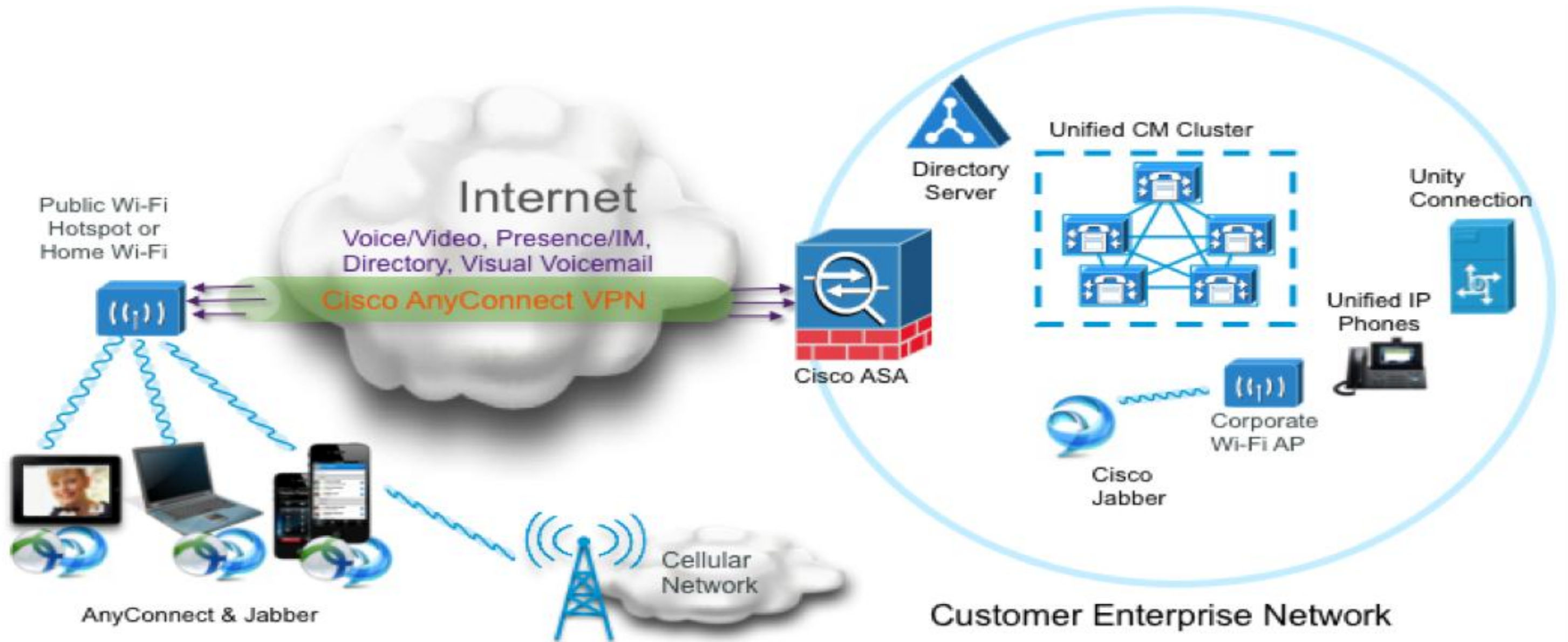


- Secure remote access with **Cisco AnyConnect Secure Mobility Client**
- Provides consistent security experience across broad platforms
- Enterprise-grade encryption and authentication
- Simple user experience with Cisco Jabber



\*\* Currently supported only on desktops

# Topology



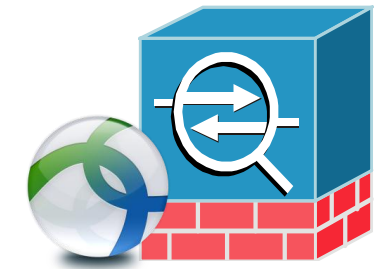
# AnyConnect Secure Mobility Client



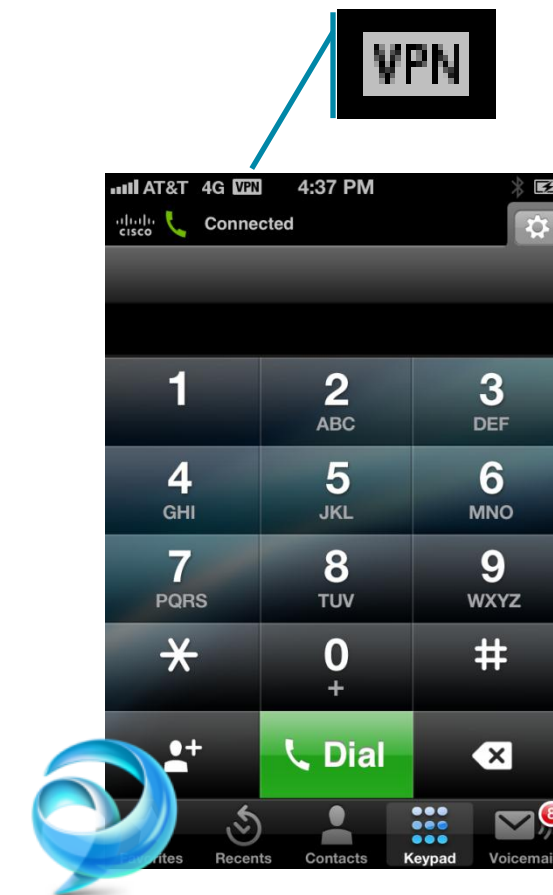
- Layer 3 VPN Client +
- Enables BYOD – Mac OS X, Windows, iOS, Android
- VPN Session protected by hardened ASA firewall
- Seamless authentication with Certificates
- IPSec / SSL / **DTLS** / IPv6
- Integrated with ScanSafe and Cisco ISE

# Secure Remote Access

## Cisco Jabber & Cisco AnyConnect



- Interworking behind the scene
  - Manual user intervention is not required after initial setup
- Automatic VPN establishment/reconnect
  - Certificate based authentication for Cisco AnyConnect
  - Utilises Connect On Demand feature in Apple iOS
  - VPN session persistence – auto reconnect
- Control VPN tunnel access
  - Using Split Tunnel policy & ACL on ASA
  - Only the traffic Cisco Jabber generates

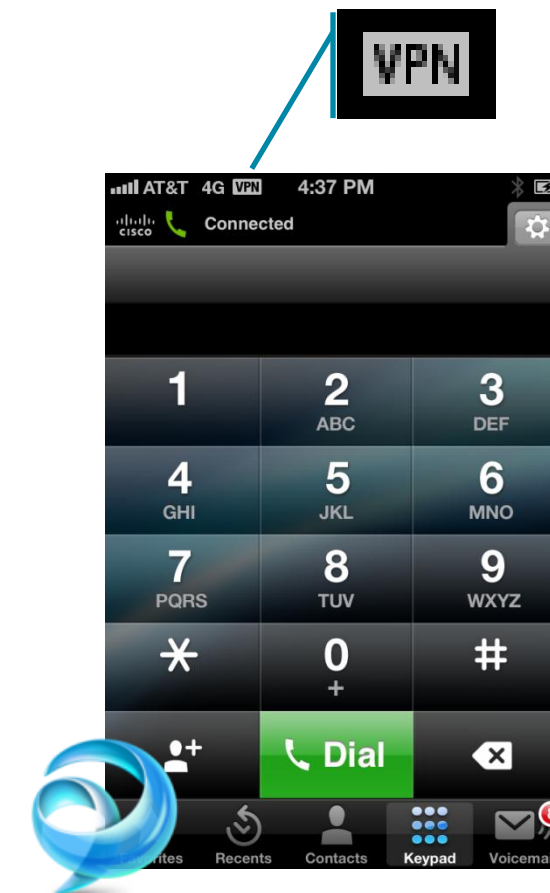


# Secure Remote Access

## Set Up Cisco AnyConnect



- Install and configure the Cisco Adaptive Security Appliance (ASA)
- Set up the ASA to support Cisco AnyConnect
  - Provision Application Profiles
  - Automate VPN Connection \* (Optional)
  - Set up Certificated-Based Authentication \* (Optional)
  - Set ASA Session Parameters
  - Set up Tunnel Policies
- Set up Automatic VPN Access on Unified CM \* (Optional)
  - On-Demand VPN URL
  - Preset Wi-fi Networks



\* Only required when using with the VPN on demand feature

# Anyconnect Usability Feature Options

<input checked="" type="checkbox"/>	VPN Profiles	>
<input checked="" type="checkbox"/>	Auto-Reconnect	>
<input checked="" type="checkbox"/>	On-Demand VPN for iOS	>
<input checked="" type="checkbox"/>	Trusted Network Detection	>
<input checked="" type="checkbox"/>	Certificate Authentication	>
<input checked="" type="checkbox"/>	SCEP for enrollment	>

# VPN Profiles

- Determines AnyConnect Behaviour
  - List of VPN Gateways
  - On-Demand, TND policies
  - Protocol – SSL / IPSec
- Defined on ASA using ASDM
- Downloaded by AnyConnect after connecting to VPN
- Tamper-Proof



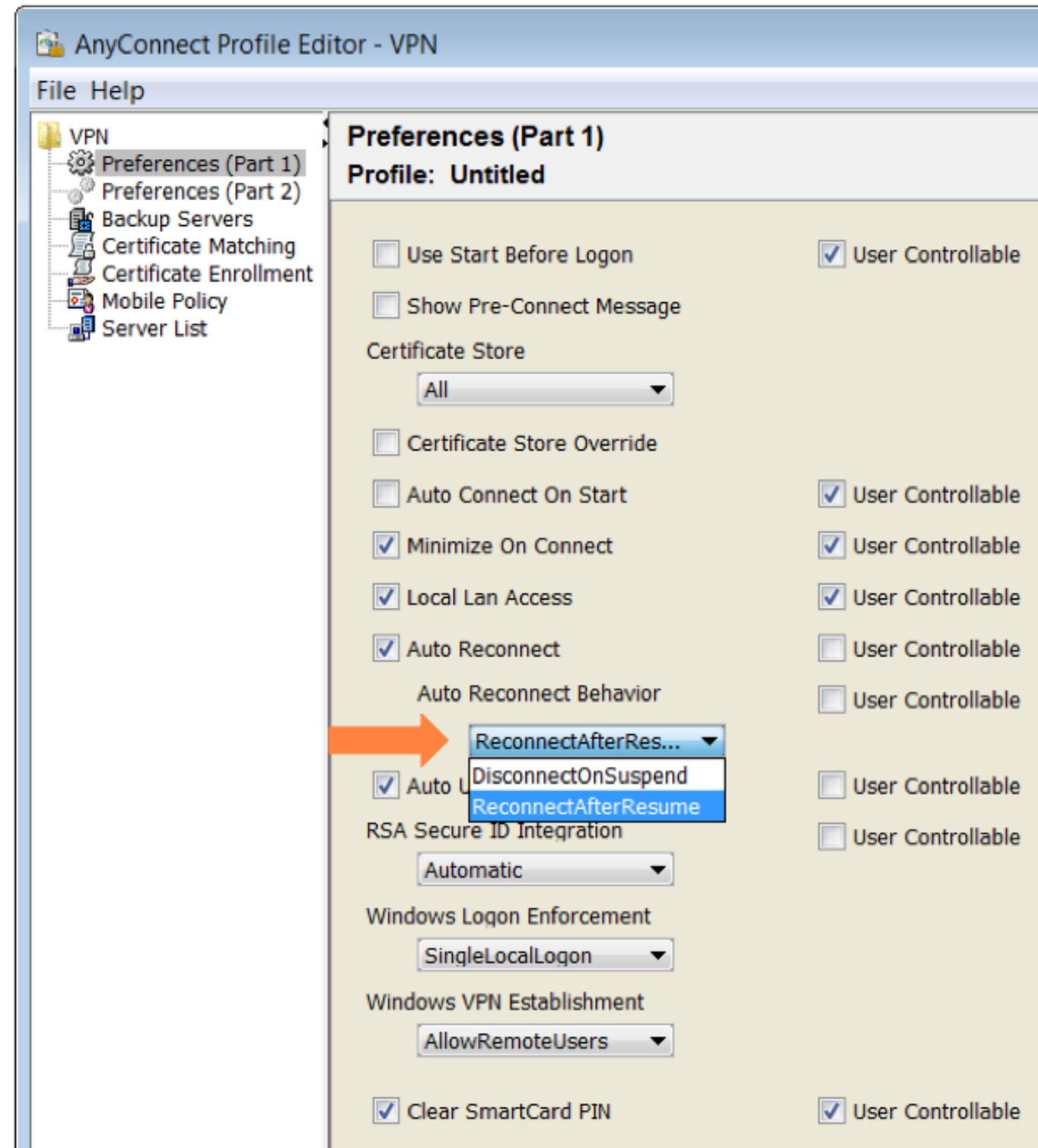


# Auto Reconnect

- Wired to WiFi, WiFi to 3G
- No Re-authentication
- Suspended on Head-end
- Idle Timeout

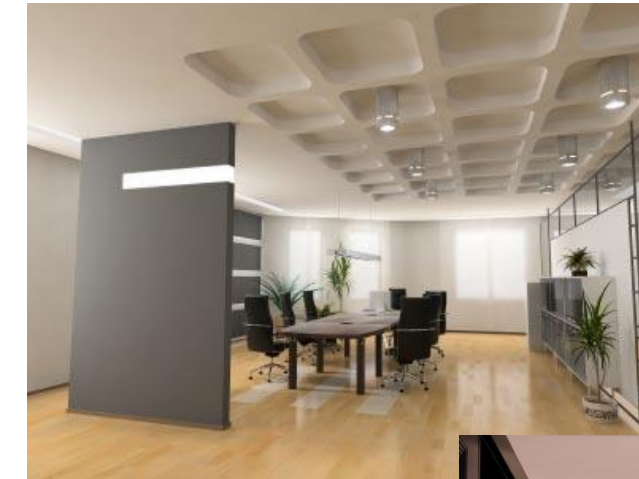


# Auto Reconnect



# Trusted Network Detection

- Auto disconnect inside office
- Auto connect when out of office
- Windows, Mac OS X and Android OEM
- Android – Not available in ICS (4.0) release
- No iOS support



Trusted  
Network



UnTrusted  
Network



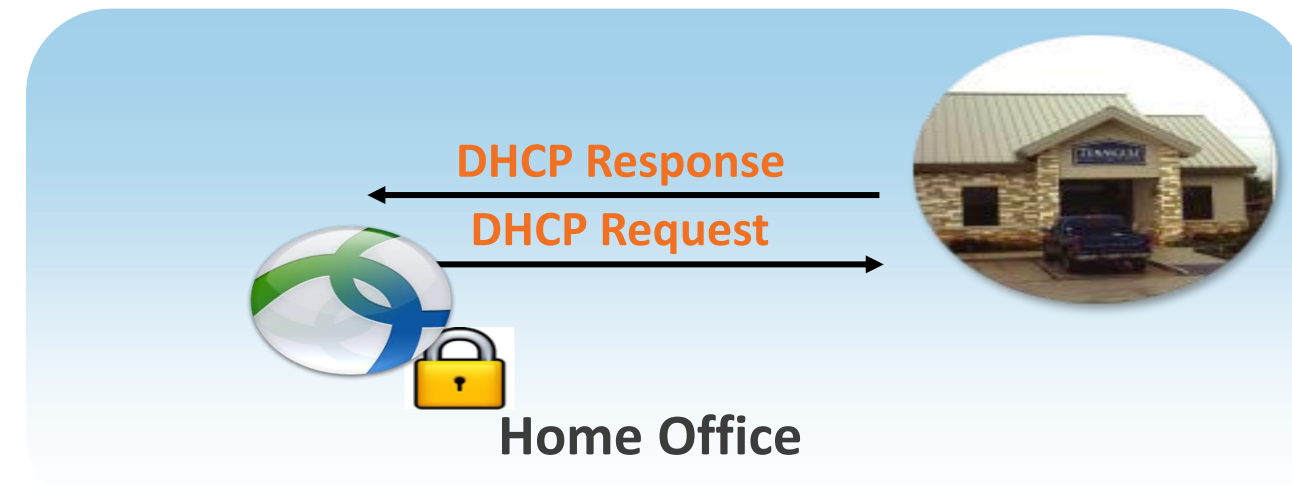
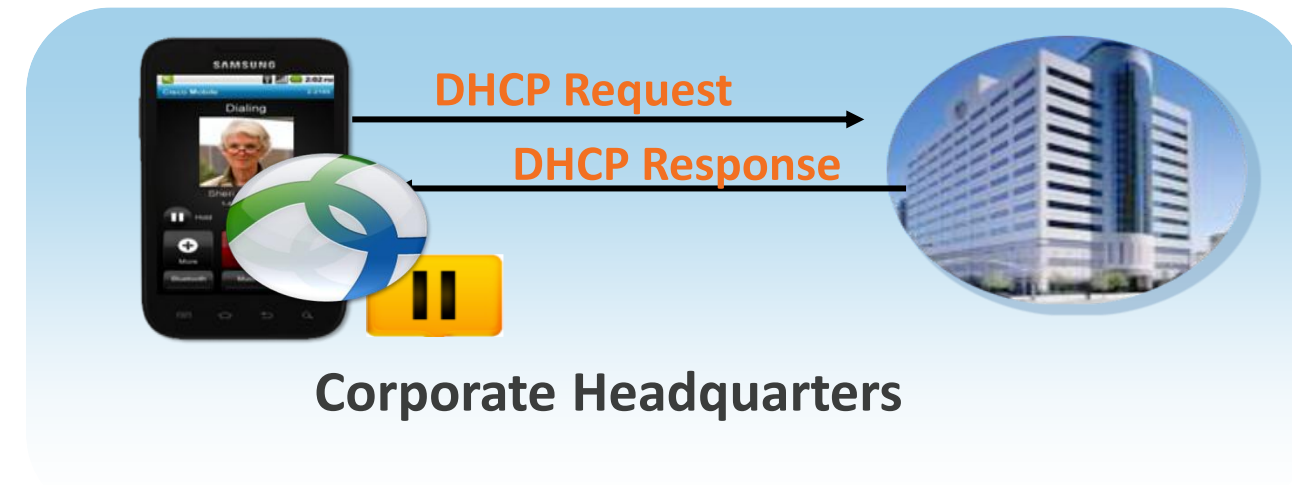
# Trusted Network Detection

**DNS Suffix**  
**comcast.net**

Trusted DNS Configuration  
Untrusted DNS Configuration

**DNS Server IP**  
**68.87.78.130**

## Trusted Network



## Untrusted Network

# Trusted Network Detection

<input checked="" type="checkbox"/> Automatic VPN Policy	
Trusted Network Policy	Disconnect
Untrusted Network Policy	Connect
Trusted DNS Domains	getwell.com
Trusted DNS Servers	192.168.1.2

# Secure Remote Access

## Connect On-Demand Feature in iOS



- **Certificate-based** authentication only
- Based on domain name (no IP address support)
  - performs a 'pseudo' DNS query using 'VPN On-demand URL' field in the Unified CM Phone Configuration page
- **Actions (wild-card match support)**
  - Always Connect
  - Never Connect
  - Connect if Needed (only when the DNS query returns a failure)
- **Two ways to enable Connect On-Demand on iOS**
  - Automatically pushed to AnyConnect as part of Client Profile
  - End user to configure in his AnyConnect Connection Profile

iPhone Network Connection	Configuration in Unified CM (Phone Configuration Page)			
	Nothing Configured	Preset Wi-Fi Networks Only	On-Demand VPN URL Only	On-demand VPN URL & Preset Wi-Fi Networks
Mobile Data(3/4G)	No auto launch	No auto launch	Auto launch*	Auto launch*
Corporate Wi-Fi	No auto launch	No auto launch	Auto launch*	No auto launch
Non-corporate Wi-Fi	No auto launch	No auto launch	Auto launch*	Auto launch*

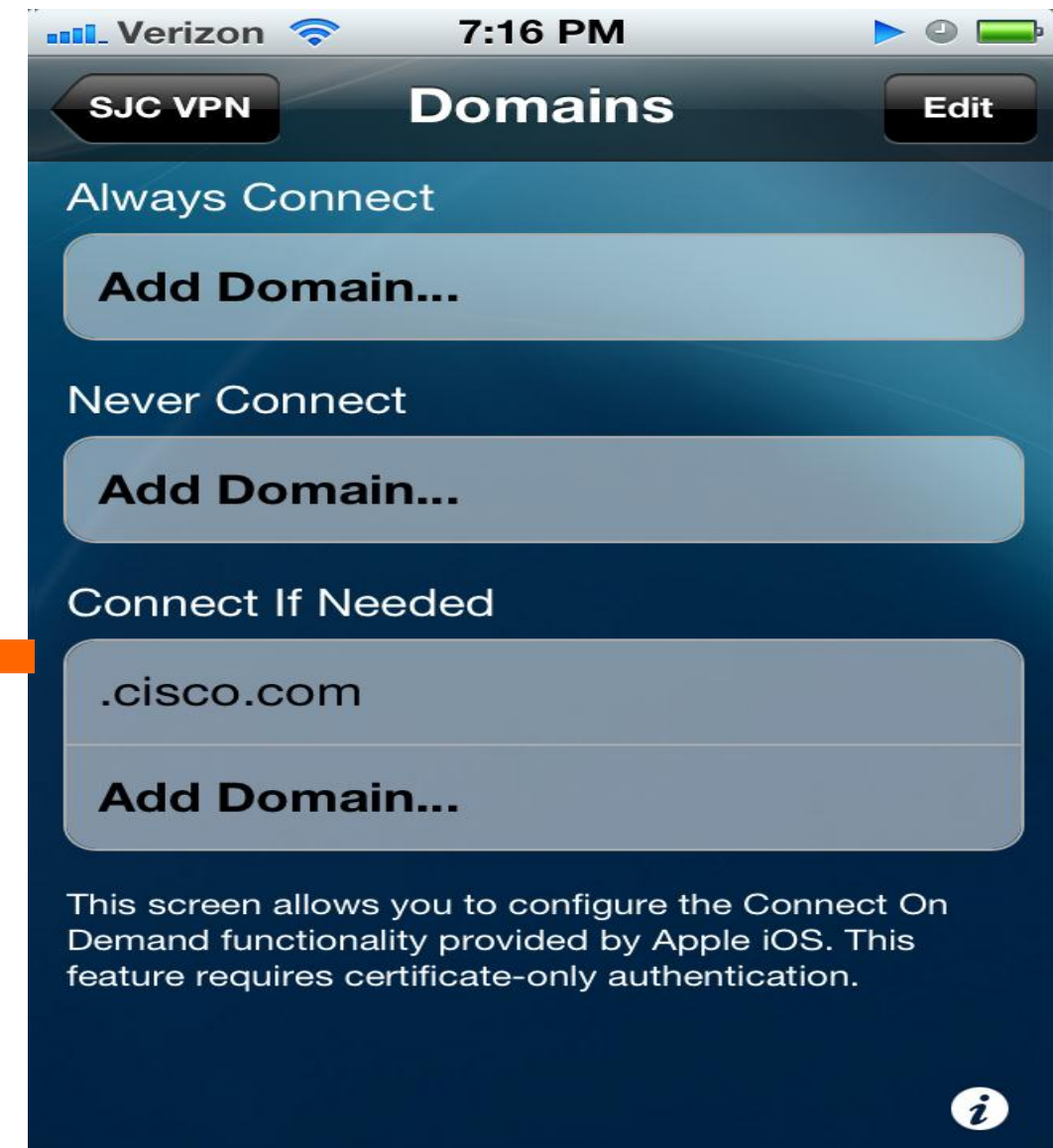
\* Exact behaviour depends on how Connect On Demand is configured in Cisco AnyConnect.

The screenshot shows a configuration form with the following fields:

- On-Demand VPN URL:** ios-ondemand.cisco.com
- XML Options:** (empty)
- Reserved:** domain=cisco.com
- Preset Wi-fi Networks:** hqwifi/sjwifi/engwifi/jabberwifi

# On-Demand VPN for iOS

- Auto Launch VPN
- Based on domain
- Certificate Auth. only
- Actions
  - Always-Connect
  - Connect-if-Needed
  - Never-Connect
- Wild-card support
  - .edu, .net, .com



# On-Demand VPN – Always Connect



iOS



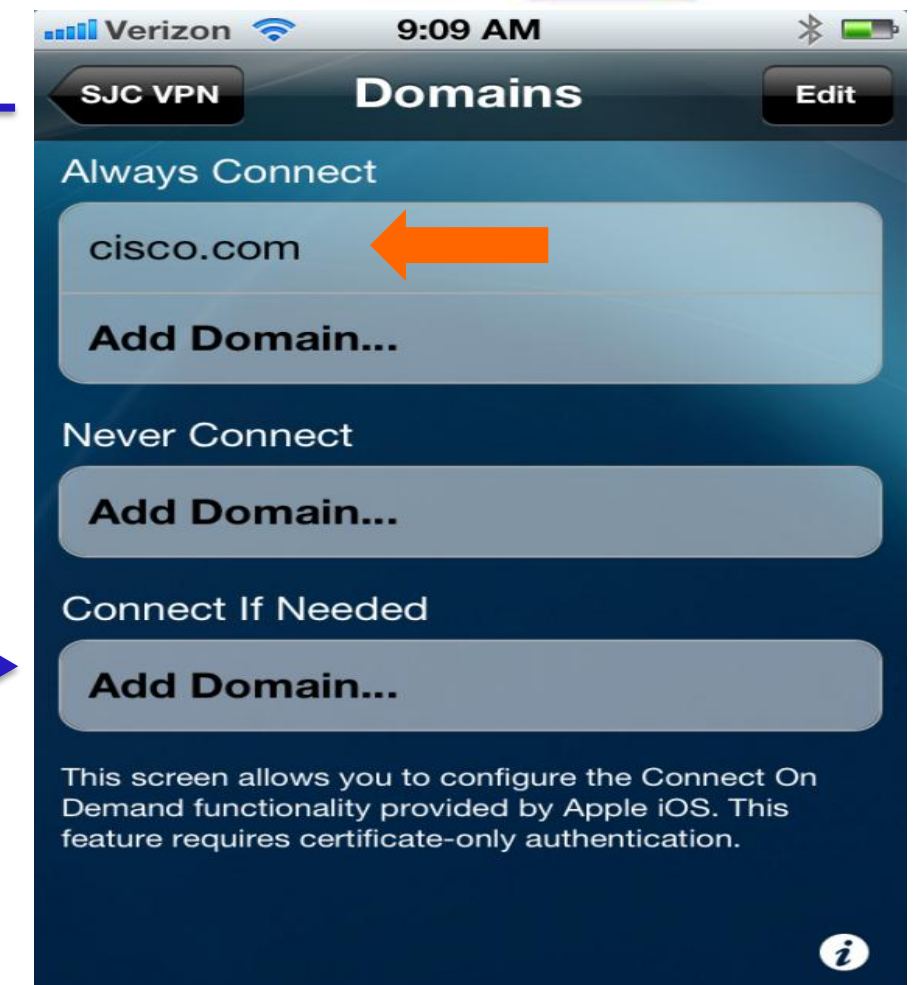
Resolve  
ccm-sjc-1.cisco.com →

Does it match the  
On-Demand list?

Yes, matches .cisco.com

← On-Demand list

Establish VPN →





# On-Demand VPN

Connect-If-Needed



iOS



Resolve  
ccm-sjc-1.cisco.com

Does it match the  
On-Demand list?

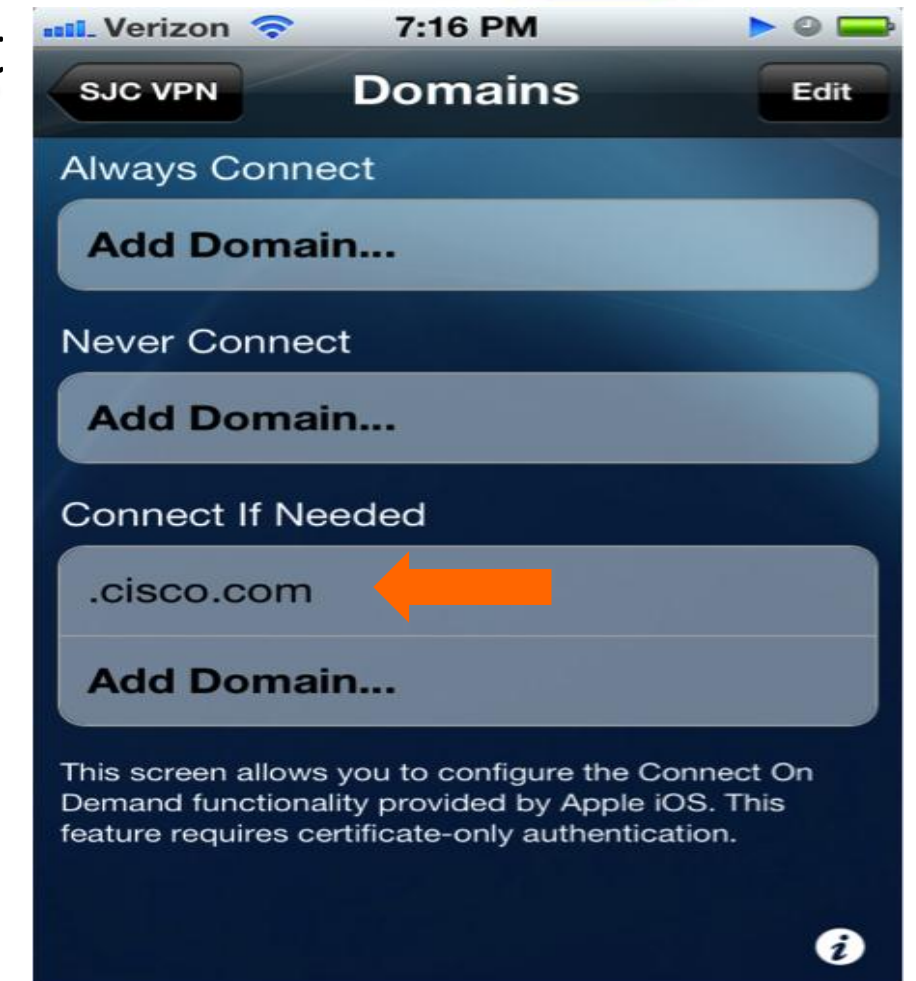
Yes, matches .cisco.com

Is the DNS resolved with local  
Network?

Not Resolved

← On-Demand list

Establish VPN →



# On-Demand VPN for iOS

The screenshot displays the 'Server List Entry' configuration window for a VPN profile. The 'Host Display Name (required)' is 'Seamless Access - Certificates' and the 'User Group' is 'User Group'. The 'FQDN or IP Address' is 'asa.getwell.com' and the 'Group URL' is also 'asa.getwell.com'. The 'Additional mobile-only settings' checkbox is checked.

The 'Mobile Settings' dialog box is open, showing the following configuration:

- Apple iOS / Android Settings:**
  - Certificate Authentication: Automatic
  - Client Certificate will never be used for authentication.
  - Make this Server List Entry active when profile is imported
- Apple iOS Only Settings:**
  - Reconnect when roaming between 3G / Wifi networks
  - Connect on Demand (requires certificate authentication)
- Match Domain or Host:** A table with the following entries:

Match Domain or Host	On Demand Action
getwell.com	Always Connect
*.edu	Always Connect
apple.com	Never Connect
cisco.com	Connect if Needed
- On Demand Action:** Connect if Needed

An orange arrow points from the 'Primary Protocol' section of the main window to the 'Match Domain or Host' table in the 'Mobile Settings' dialog.

# CUCM - On-Demand VPN URL

The screenshot displays the CUCM Phone Configuration interface for a Cisco Jabber device. The top navigation bar includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main title is 'Phone Configuration' with a 'Related Links: Back To Find/List' dropdown and a 'Go' button. Below the title is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New.

**Status:** Status: Ready

**Association Information:** A list of 8 lines is shown, with a 'Modify Button Items' button above it. The lines are:

- 1. Line [1] - 1002 (no partition)
- 2. Line [2] - Add a new DN
- 3. Line [3] - Add a new DN
- 4. Line [4] - Add a new DN
- 5. Line [5] - Add a new DN
- 6. Line [6] - Add a new DN
- 7. Add a new SD
- 8. Add a new SD

**Phone Type:** Product Type: Cisco Jabber, Device Protocol: SIP

**Device Information:** Registration: Registered with Cisco Unified Communications Manager 192.168.10.15, IP Address: 192.168.12.7, Active Load ID: image\_a, Device is Active (checked), Device is trusted (checked), Device Name\*: TABBRSAK, Description: Jabber, Device Pool\*: Default (with a 'View Details' link).

**Product Specific Configuration Layout:** This section contains several configuration options:

- Allow End User Configuration Editing: Enabled
- Country Code: US
- Cisco Usage and Error Tracking: Disabled
- Enable Sip Digest Authentication: Disabled
- Sip Digest Username: (empty field)
- Contacts: (empty field)
- On-Demand VPN URL: ccm-sjc-1.cisco.com
- XML Options: (empty field)

An orange arrow points to the 'On-Demand VPN URL' field.

# Certificate Authentication

- AnyConnect is issued a certificate
- AnyConnect presents certificate to ASA
- ASA validates certificates
  - Timestamp
  - Issuer
  - Revocation Status



No Passwords

# Configuration Steps – Cert Auth

- ASA / ASDM

- Import root certificate
- Generate Identity Certificate for ASA
- Use identity certificate for SSL
- Under Connection Profile - Change Authentication method to 'Certificate'
- Create Certificate to Connection Profile Map
- CLI - ssl certificate-authentication interface outside port 443

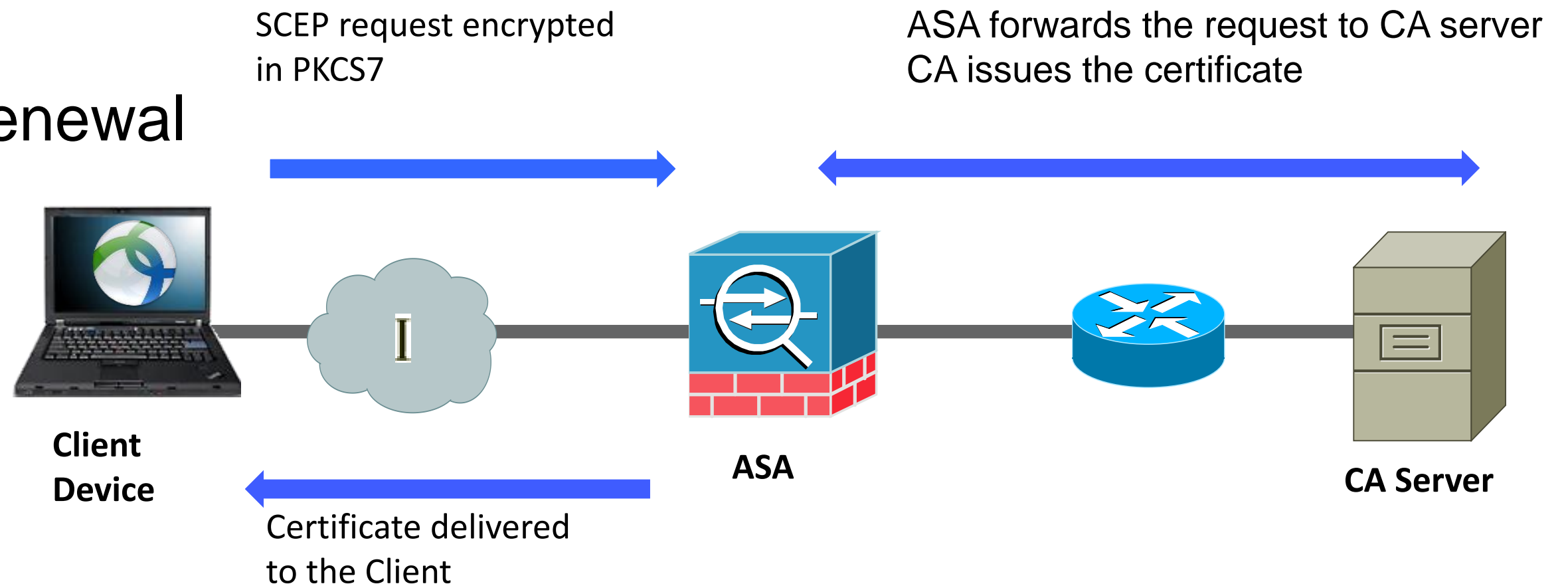
# SCEP – Simple Certificate Enrollment Protocol

- SCEP is supported by MS CA, IOS CA, OpenCA and others
- Embedded into Cisco Anyconnect on all Platforms
- Offers easy Certificate Deployment / Mngt options for Admins
- Some devices support SCEP natively
  
- SCEP is not a New Feature
- Alternative to SCEP for Cert Deployment
  - MDM, iPhone configuration utility, Email, Web Site Deployment etc

# SCEP

- Simple Certificate Enrollment

- Auto Renewal



# Configuration Steps - SCEP

- Windows 2008 Server
  - Enable SCEP (Microsoft Documentation)
- ASA / ASDM
  - Set up two connection profiles – enroll, cert-auth
  - Enroll – Uses AAA authentication (And set group alias as **'enroll'**)
  - Cert-Auth – Requires Certificates
- ASDM / AnyConnect Profile Editor
  - SCEP URL – <https://acme.vpn.com/enroll>
  - CA Server URL – <https://ca.acme.com/certsrv/mscep/mscep.dll>



# Jabber Anyconnect Feature Support

## Available on All Platforms

- VPN profiles
- Auto Reconnect
- Certificates
- SCEP

	iOS	Android ICS	Android (OEM or Rooted)	Windows and Mac OS X
On-Demand VPN	Yes	No	No	No
TND	No	No	Yes	Yes

# Deployment Considerations

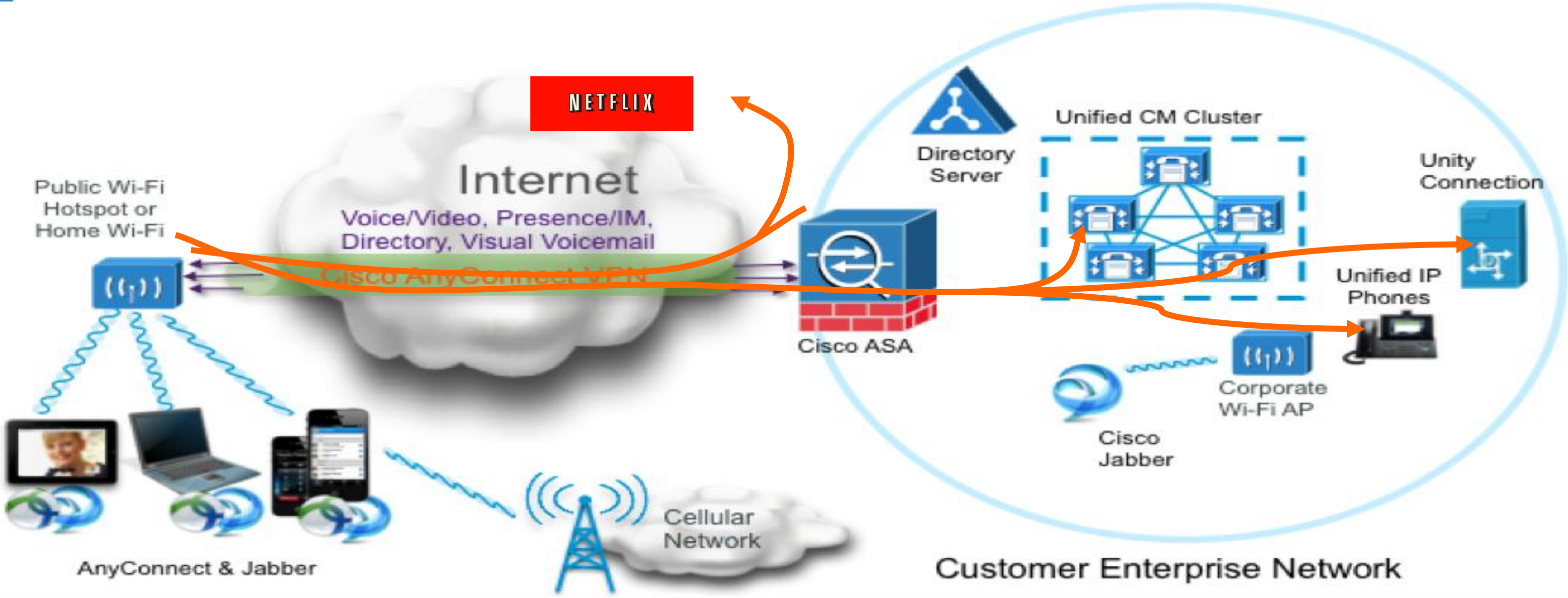
- **Full-Tunnel**

- Pros: Tunnels everything
- Cons: Bandwidth and Privacy Concerns

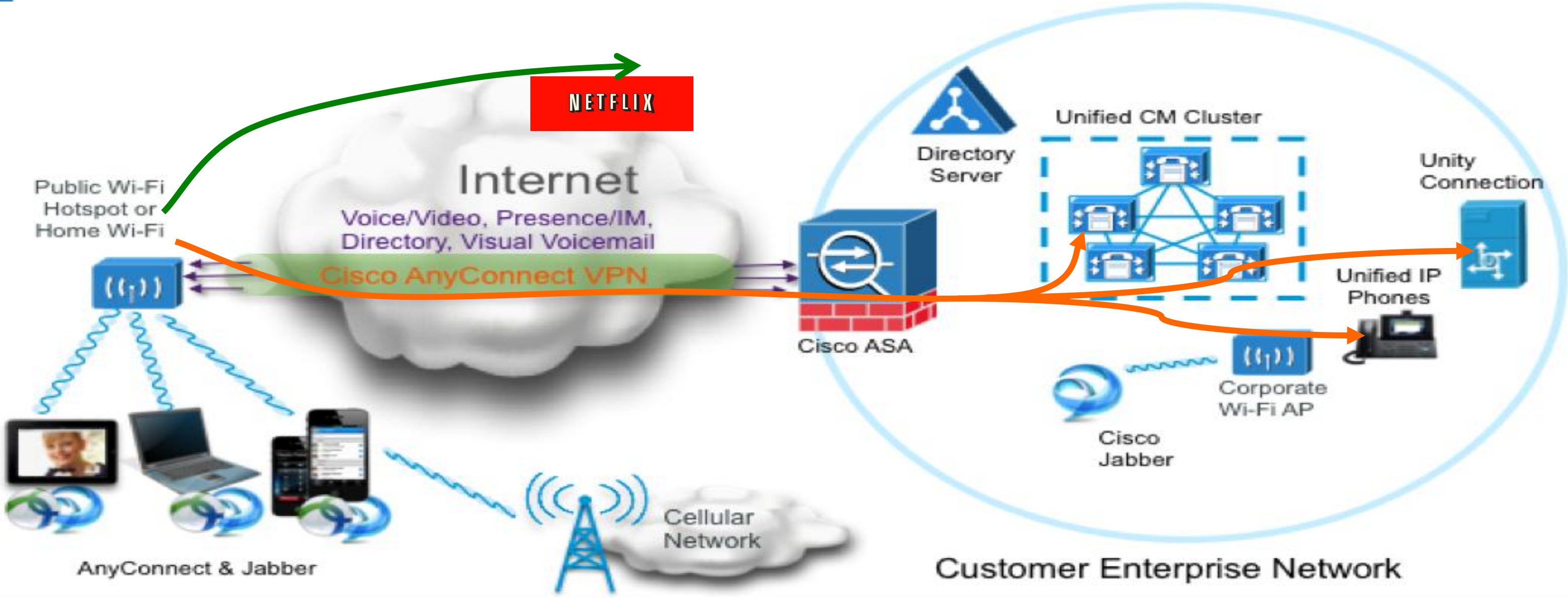
- **Split Tunnel**

- Pros: Limits to company subnet
- Cons: May be difficult to summarise split-tunnel list

# Full-Tunnel



# Split-Tunnel



# Full-Tunnel Policy

- All Traffic is sent inside the VPN Tunnel
- Configured under Group Policy

Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.

DNS Names:

Send All DNS Lookups Through Tunnel:  Yes  No

Policy: Tunnel All Networks

IPv6 Policy: Tunnel All Networks

Network List: -- None -- Manage...

**Note on using extended ACL:** If you use an extended ACL as Network list, please be aware that only the source address field will be used, and all other fields, such as destination address, service etc are ignored.

# Split-Include Policy

- I don't want all my user traffic over the AnyConnect VPN.
- Configure Split-Tunnel under the Group Policy
- Split-Include: IP Subnet of CUCM, TFTP, CUPS, CA, AD servers

The screenshot displays the configuration for an internal group policy. The main window is titled "Edit Internal Group Policy: DfltGrpPolicy". On the left, a navigation pane shows "General Servers" and "Advanced" settings, with "Split Tunneling" selected. The main area contains the following configuration:

- Split tunneling network lists** distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
- DNS Names:** (Empty text field)
- Send All DNS Lookups Through Tunnel:**  Yes  No
- Policy:** Tunnel Network List Below (indicated by a red arrow)
- IPv6 Policy:** Tunnel All Networks
- Network List:** Split-Tunnel-List (indicated by a red arrow) with a "Manage..." button.

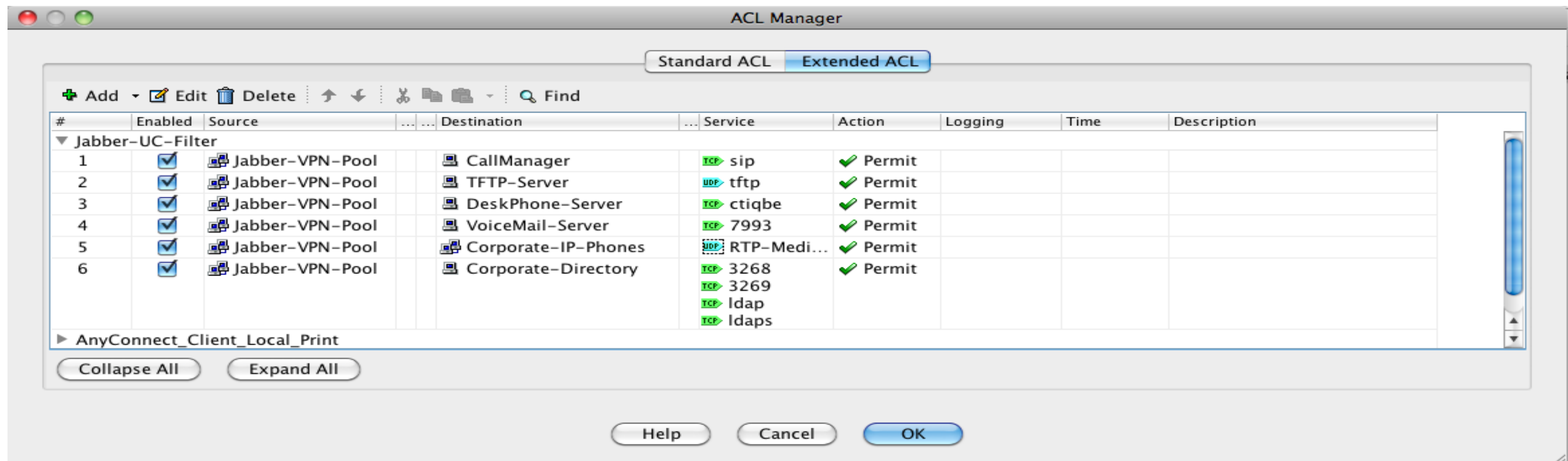
Below this, the "ACL Manager" window is open, showing a table of ACL entries for the "Split-Tunnel-List".

No	Address	Action	Description
▼ Split-Tunnel-List			
1	inside-network/24	✓ Permit	Corporate Network
2	10.17.0.0/16	✓ Permit	Corporate IP Phone Voice VLAN Network
3	171.70.146.0/24	✓ Permit	Call Manager Cluster, TFTP Service, Active Directory Server

At the bottom of the ACL Manager window are buttons for "Help", "Cancel", and "OK".

# Prevent Non-Jabber Traffic

- I want to allow only the Jabber Traffic over VPN
- Configure Network ACLs under Group Policy
- Can be Port Based



The screenshot shows the ACL Manager interface with the 'Extended ACL' tab selected. The table below displays the configuration for the 'Jabber-UC-Filter' group policy.

#	Enabled	Source	Destination	Service	Action	Logging	Time	Description
▼ Jabber-UC-Filter								
1	<input checked="" type="checkbox"/>	Jabber-VPN-Pool	CallManager	TCP sip	Permit			
2	<input checked="" type="checkbox"/>	Jabber-VPN-Pool	TFTP-Server	UDP tftp	Permit			
3	<input checked="" type="checkbox"/>	Jabber-VPN-Pool	DeskPhone-Server	TCP ctiqbe	Permit			
4	<input checked="" type="checkbox"/>	Jabber-VPN-Pool	VoiceMail-Server	TCP 7993	Permit			
5	<input checked="" type="checkbox"/>	Jabber-VPN-Pool	Corporate-IP-Phones	UDP RTP-Medi...	Permit			
6	<input checked="" type="checkbox"/>	Jabber-VPN-Pool	Corporate-Directory	TCP 3268 TCP 3269 TCP ldap TCP ldaps	Permit			
▶ AnyConnect_Client_Local_Print								

Buttons: Collapse All, Expand All, Help, Cancel, OK

# Split-Exclude Policy

- Possible to prevent known subnets from using VPN Tunnel
- Configure under Group Policy

The screenshot displays the Cisco Group Policy Editor interface. The main window is titled "Edit Internal Group Policy: DfltGrpPolicy". On the left sidebar, the navigation tree shows "General", "Servers", and "Advanced" expanded to "Split Tunneling". The main content area contains the following settings:

- DNS Names:** An empty text field.
- Send All DNS Lookups Through Tunnel:** Radio buttons for "Yes" and "No", with "No" selected.
- Policy:** A dropdown menu set to "Exclude Network List Below", with a red arrow pointing to it.
- IPv6 Policy:** A dropdown menu set to "Tunnel All Networks".
- Network List:** A dropdown menu set to "Split-Exclude-List", with a red arrow pointing to it. A "Manage..." button is located to the right.

Below the main window, an "ACL Manager" window is open, showing a table of ACL entries. The "Standard ACL" tab is active. The table lists four entries under the "Split-Exclude-List" group:

No	Address	Action	Description
1	74.125.224.0/24	✓ Permit	YouTube Traffic
2	69.53.236.17	✓ Permit	NetFlix Videos
3	69.171.0.0/24	✓ Permit	Facebook Traffic - 1
4	69.220.0.0/24	✓ Permit	Facebook Traffic-2



# Other Recommendations

- Ensure DTLS is negotiated
- Disable Server-Side Dead Peer Detection
- Enable Client-Side Dead Peer Detection
- Idle Timeout – 30 minutes



# Jabber Video Remote Access

## VCS Expressway

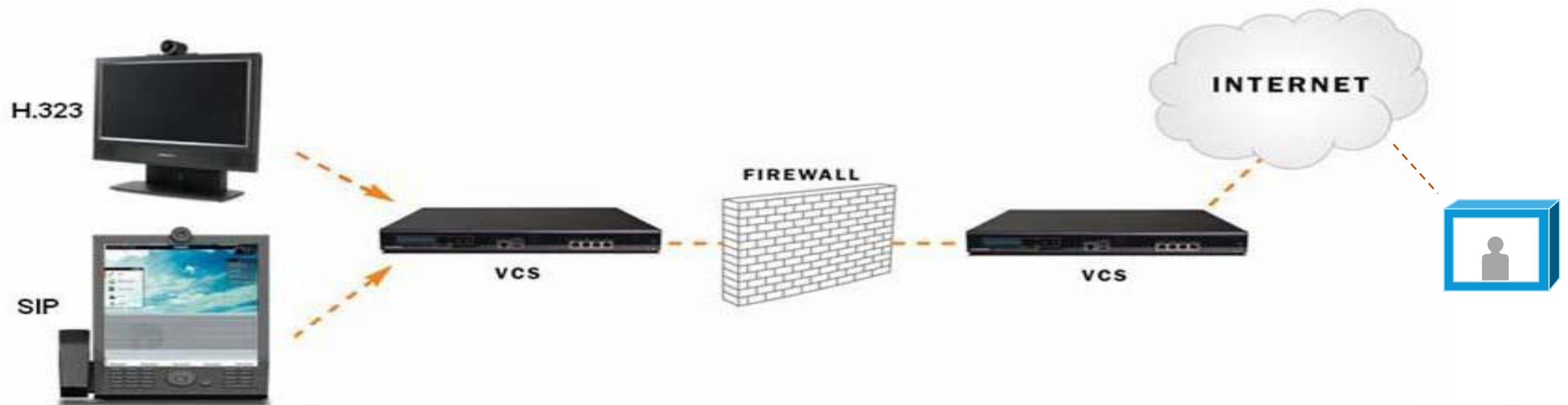


# Cisco VCS Expressway Traversal Solution

VCS Expressway opens up outside world to video communication, users can connect to home or remote workers, suppliers, consultants or anyone else outside the network

VCS Expressway provides standards-based firewall traversal for SIP and H.323 devices allowing secure firewall traversal of any firewall or NAT device. As well as all the functionality of a VCS Control

The VCS Expressway is normally deployed outside of your firewall or within the DMZ.



# Firewall Traversal

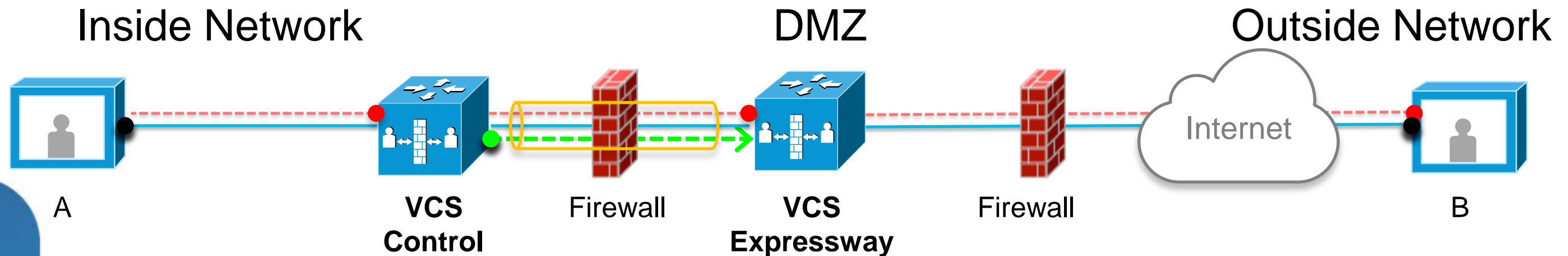
- Firewalls generally block unsolicited incoming requests, meaning any calls originating from outside your network will be blocked - can be overcome via expressway.

The Expressway solution consists of:

- VCS Expressway located outside the firewall on the public network / DMZ, which acts as the firewall traversal server
- VCS Control, or traversal-enabled endpoint located in a private network, which acts as the firewall traversal client

The two systems work together to create an environment where all connections between the two are outbound, i.e. established from the client to the server, and thus able to successfully traverse the firewall.

# VCS Expressway Firewall Traversal



1. VCS Expressway is the traversal server in DMZ. VCS Control is the traversal client installed inside the network.
2. VCS Control connects via the firewall to a specific port on the VCS Expressway **with secure login credentials**.
3. Once the connection has been established, the VCS Control sends keep-alive packets to the VCS Expressway
4. When VCS Expressway receives an incoming call, it issues an incoming call request to VCS Control.
5. The VCS Control then initiates connection to the endpoint
6. The call is established and media traverses the firewall securely

# Traversal-server

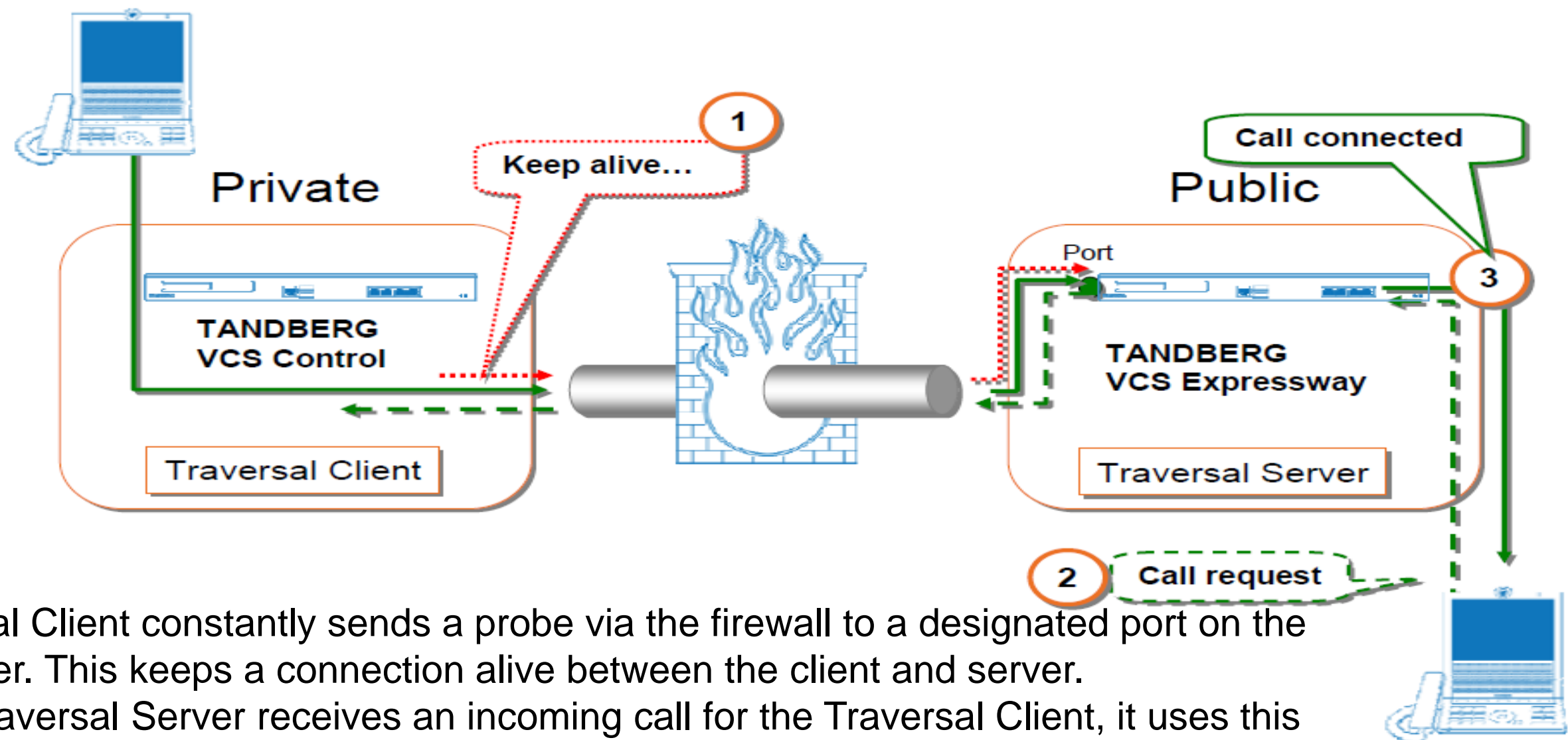
- A VCS Expressway is able to act as a traversal server, providing firewall traversal on behalf of traversal clients (for example, VCS Controls or gatekeepers).
- To act as a traversal server, the VCS Expressway must have a special type of two-way relationship with each traversal client.
- To create this connection, you create a traversal server zone on your local VCS Expressway and configure it with the details of the corresponding zone on the traversal client. (The client must also be configured with details of the VCS Expressway.)

# Traversal-client

Your VCS can act as a firewall traversal client on behalf of SIP and H.323 endpoints registered to it, and any gatekeepers that are neighbored with it.

To act as a firewall traversal client, the VCS must be configured with information about the systems that will act as its firewall traversal server

# How Firewall Traversal Client-Server Works



1. The Traversal Client constantly sends a probe via the firewall to a designated port on the Traversal Server. This keeps a connection alive between the client and server.
2. When the Traversal Server receives an incoming call for the Traversal Client, it uses this existing connection to send an incoming call request to the client.
3. The client then initiates a connection to the server and upon receipt the server responds with the incoming call.

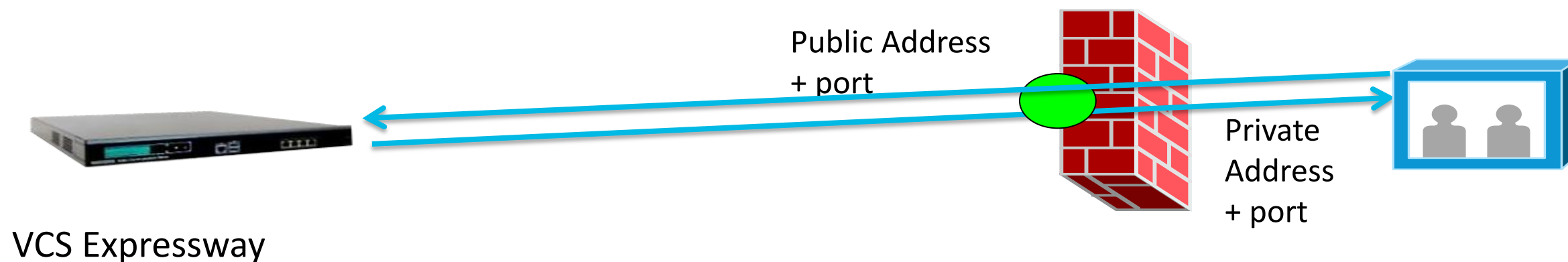
This process ensures that from the firewall's point of view, all connections are initiated from the Traversal Client inside the firewall out to the Traversal Server.



# Expressway Traversal Technology

## VCS Media Latching

- VCS determined destination is NAT'd
  - “Via” IP address differs from source IP address
- No media (RTP&RTCP) sent to remote end until media packet is received (this opens up the NAT binding).
- Media sent to network address from which the media packet is received



# VCS Traversal Call Scenarios



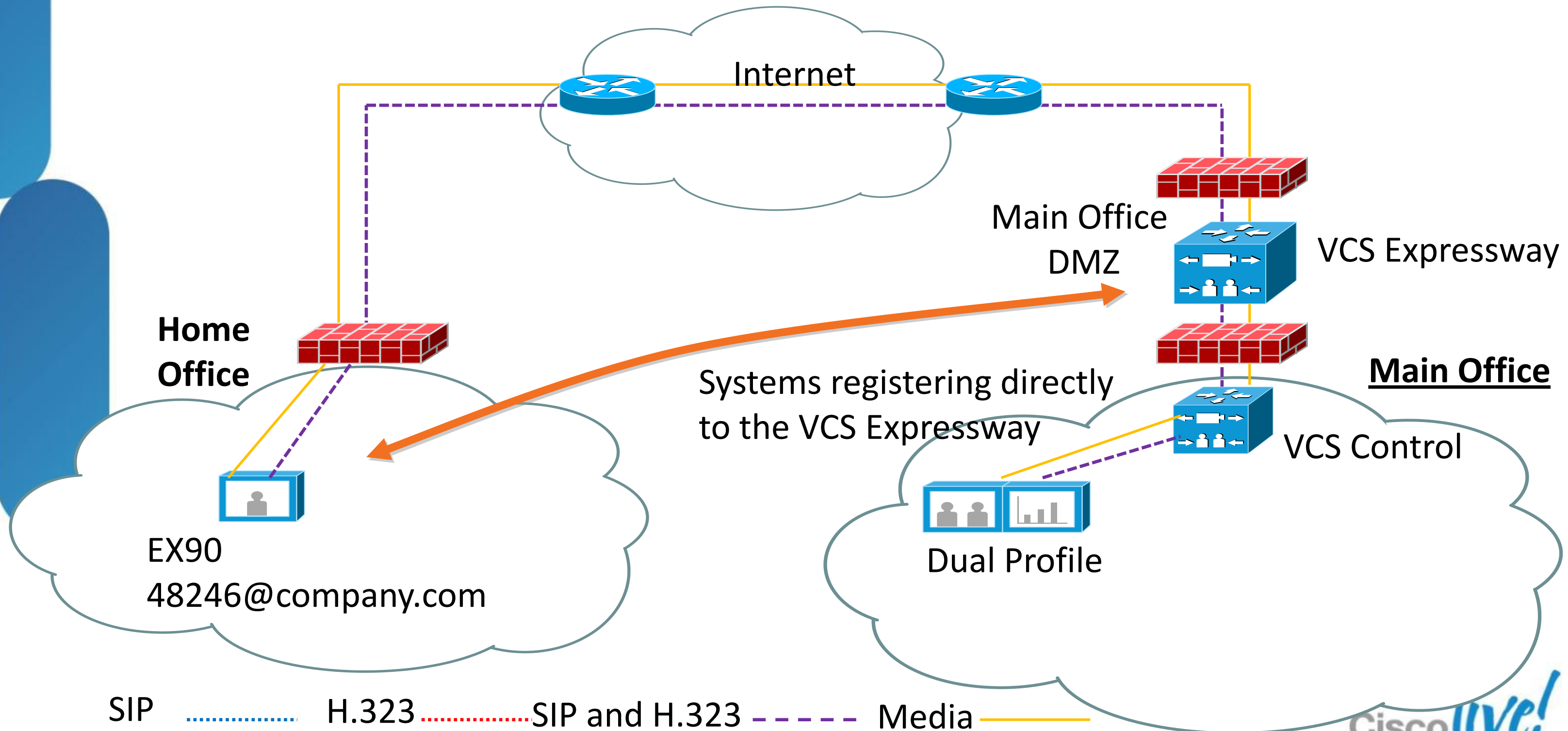
Assume all endpoints are registered	Internal Network VCS-C ————— VCS-E	External Network VCS-E ————— VCS-C	Notes
H.323 Ex. TANDBERG Classic	<b>Yes:</b> Endpt. Registers as standard H.323. VCS-C provides client-side traversal on behalf of endpt.	<b>Yes:</b> Expressway accepts H.323 registrations and calls from endpoints on public IP. In this case VCS-E provides traversal for non H.460 endpt.	Larger port range needed to communicate H.323 to VCS-E from external
H.323 + H.460 Ex. Ex90	<b>Yes:</b> Endpt. registers as standard H.323. H.460 header ignored. VCS-C provides client side traversal	<b>Yes:</b> Endpt. registers on VCS-E as H.460 traversal client.	Calls will always be traversal calls
SIP Ex. Ex90	<b>Yes :</b> Endpt. Registers a standard SIP. VCS-C provides client-side traversal on behalf of endpt.	<b>Yes:</b> Expressway accepts SIP registrations and calls .	Traversal call on VCS-E will occur if apparent address differs from host
SIP + ICE/TURN Ex. Movi	<b>Yes:</b> If other endpt. is non-ICE client. <b>Note:</b> if other endpt. Is SIP+ICE call may not be traversal.	<b>Yes :</b> If other endpt. Is non-ICE client. <b>Note:</b> if other endpt. Is SIP+ICE call may not be traversal.	If TURN server is used on Expressway, this is <b>NOT</b> a traversal call

# External Video Connectivity Options

- Intercompany and external call scenarios
  - **Direct Peering Model** - Teleworkers connect back to enterprise domain. Only allow calls to and from trusted parties. (i.e. known and trusted entities on the outside).
  - **Direct Peering Model** - B2B communications are directly peered to each other.
  - **Open Internet model** - Full flexibility in reaching other organisation based on URI

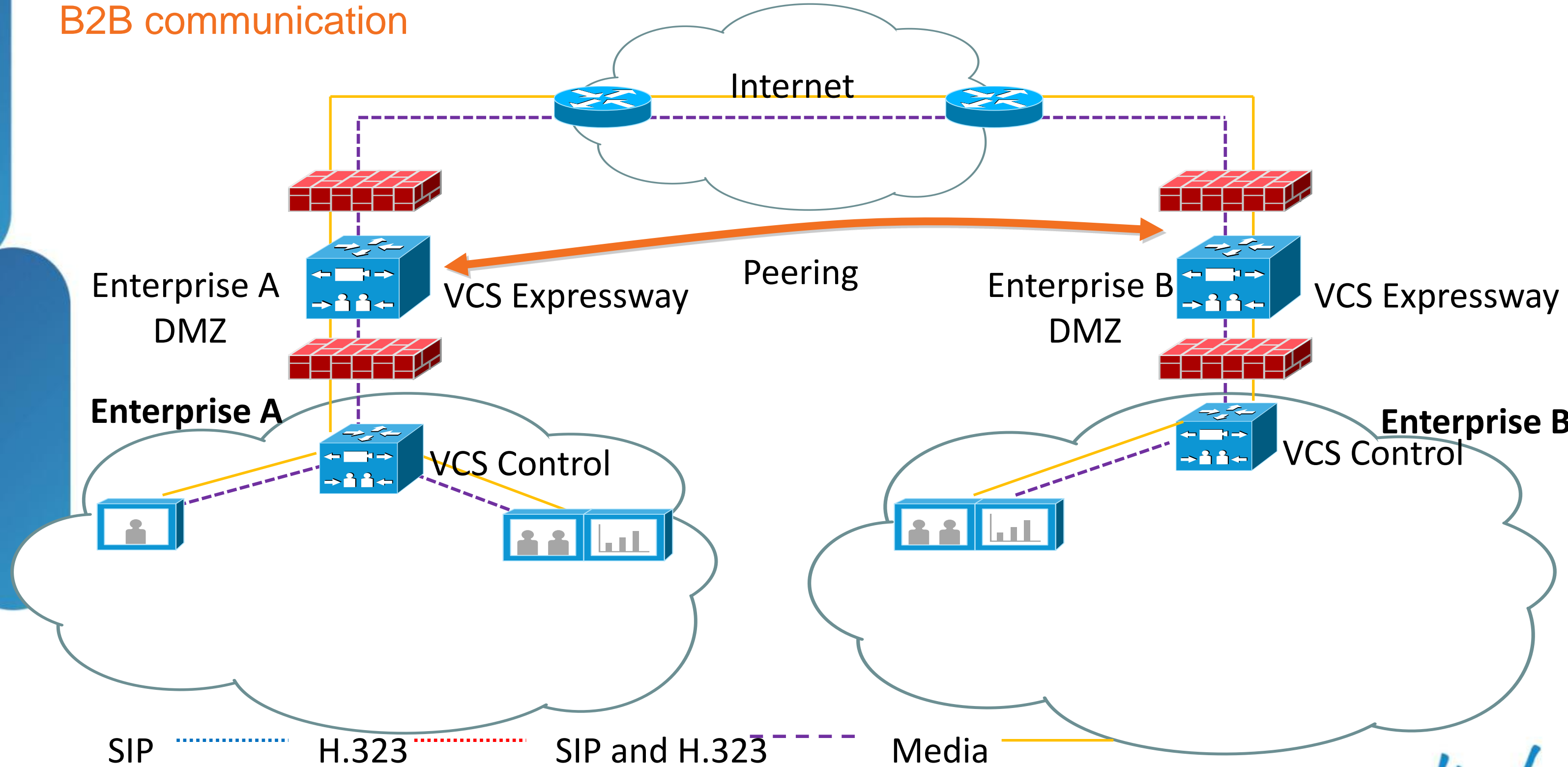
# Direct Peering Model

Main Office to Home Workers



# Direct Peering Model

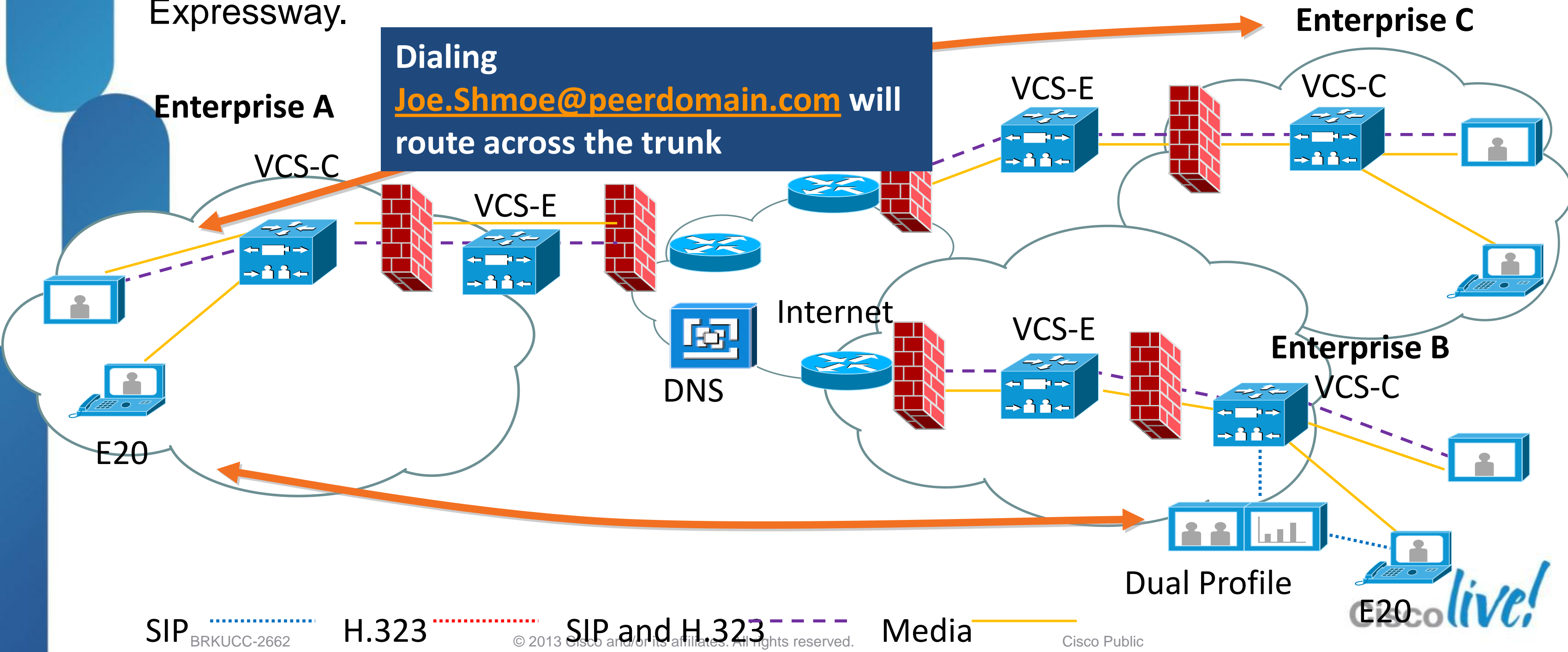
B2B communication



# Direct Peering Model

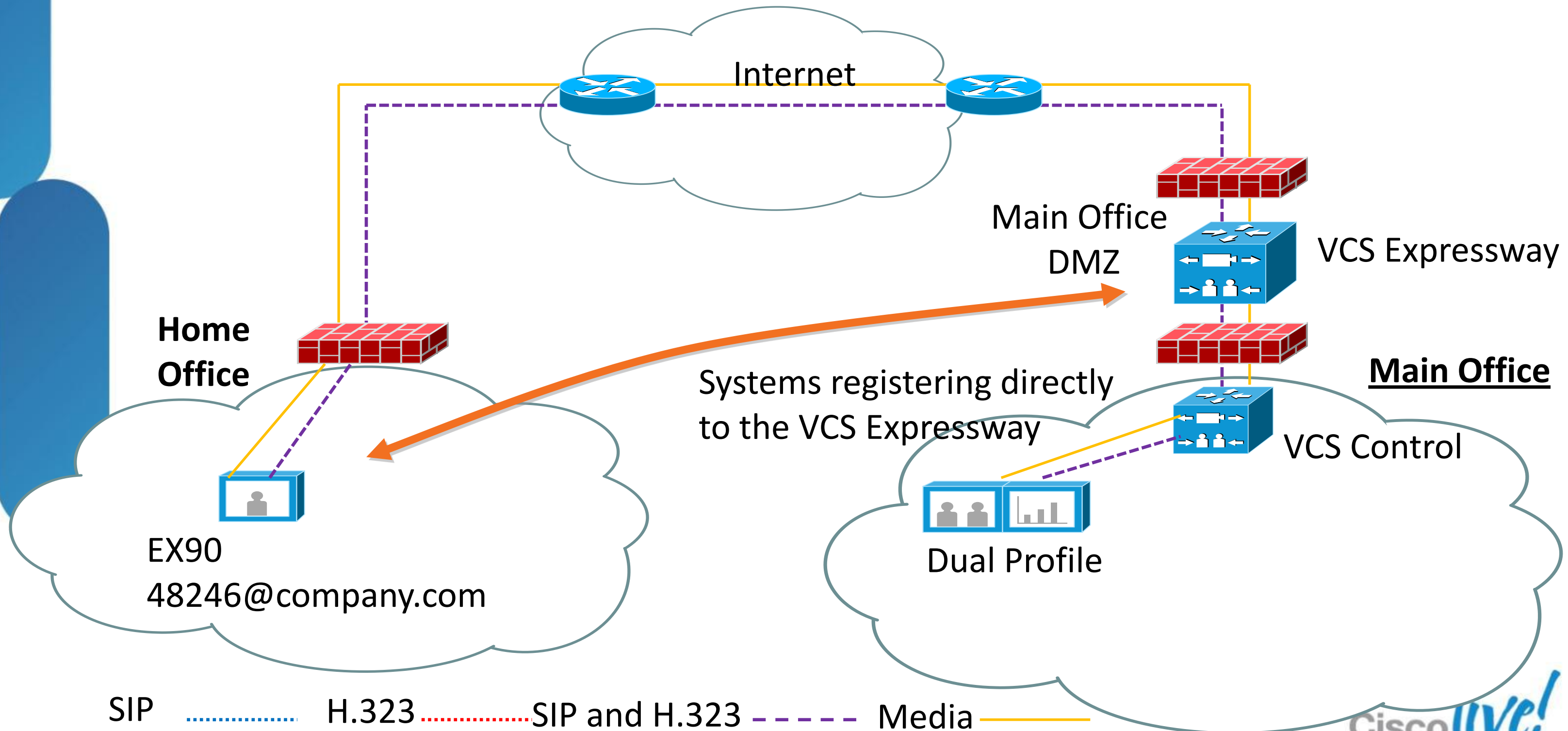
## B2B Communication

The relationship (trunk) between the companies is configured using the domain of the peer, i.e. calls to \*@peerdomain.com will be routed over the trunk to the peer VCS Expressway.



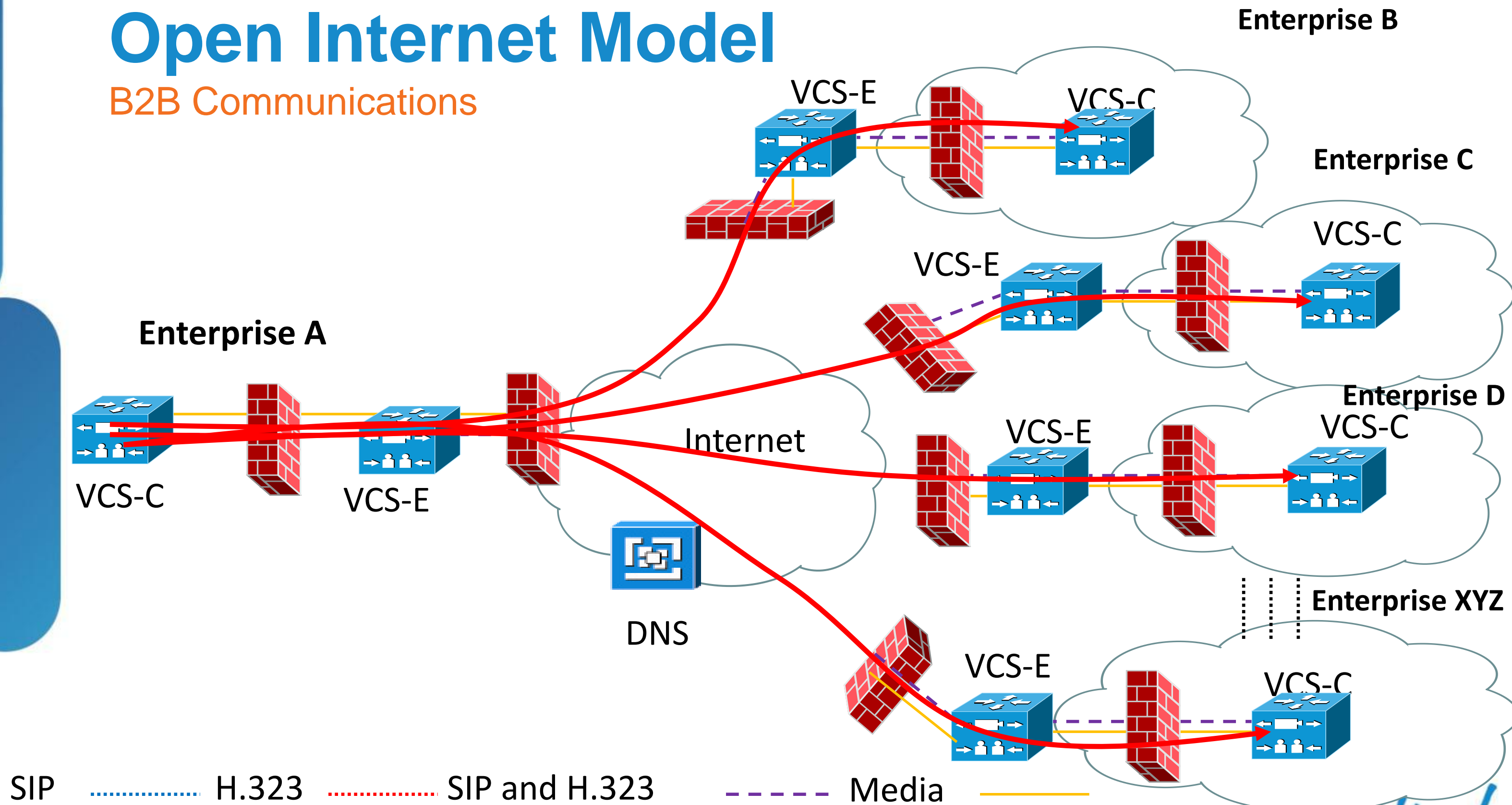
# Direct Peering Model

Main Office to Home Workers



# Open Internet Model

## B2B Communications



SIP ..... H.323 ..... SIP and H.323 - - - - Media - - - -

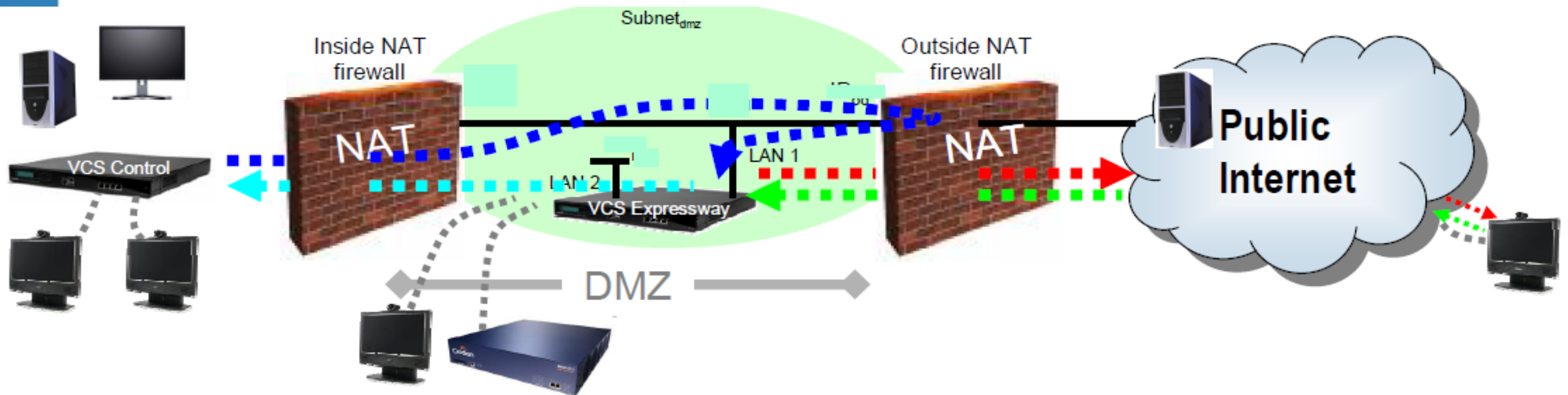




# Authentication and NTP

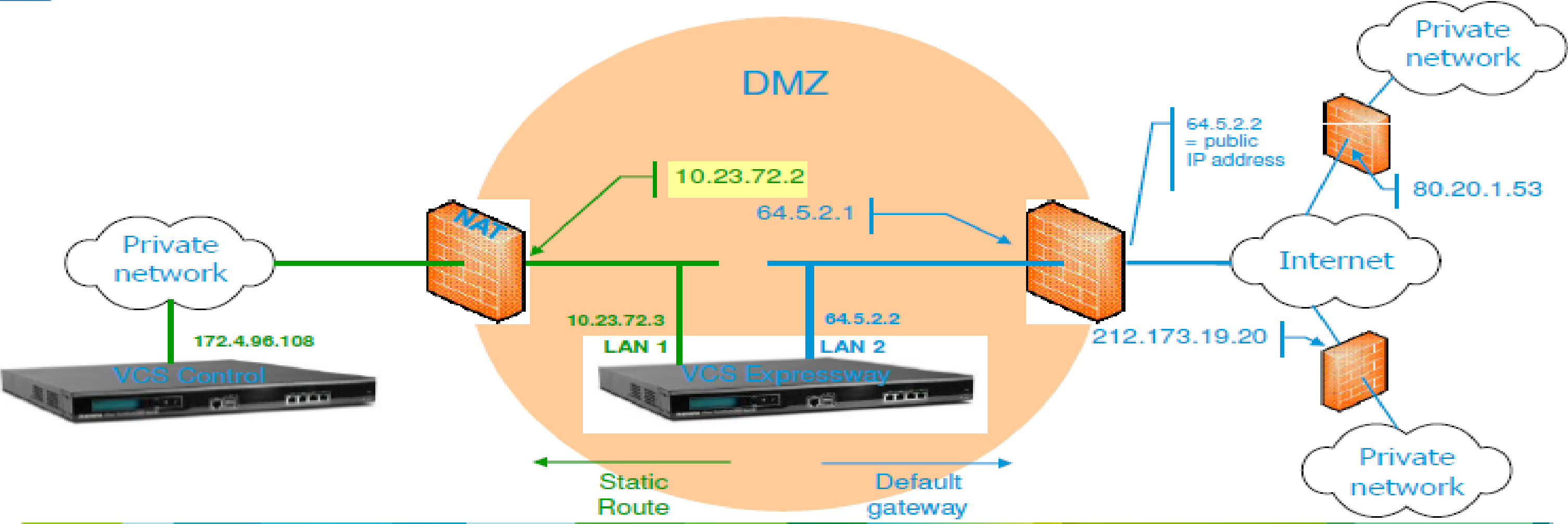
- All VCS and Gatekeeper traversal clients that support H.323 must authenticate with the VCS Expressway.
- The authentication process makes use of timestamps and requires that each system uses an accurate system time.
- The system time on a VCS is provided by a NTP server. Therefore, for firewall traversal to work, all systems involved must be configured with details of an NTP server.

# VCS Expressway using Single Interface



- ➔ A VCS Control to VCS Expressway call is a private to public flow through the firewall, so firewall ports are normally open
- ➔ ■ A VCS Expressway to VCS Control call only requires responses to Control to Expressway messages, so no firewall configuration is required.
- ➔ A VCS Expressway to Public Internet call is a private to public flow through the firewall, so firewall ports are normally open
- ➔ ■ A Public Internet to VCS Expressway call needs all relevant ports opened in the firewall

# VCS Expressway – Dual Network



# Dual Network Option Key

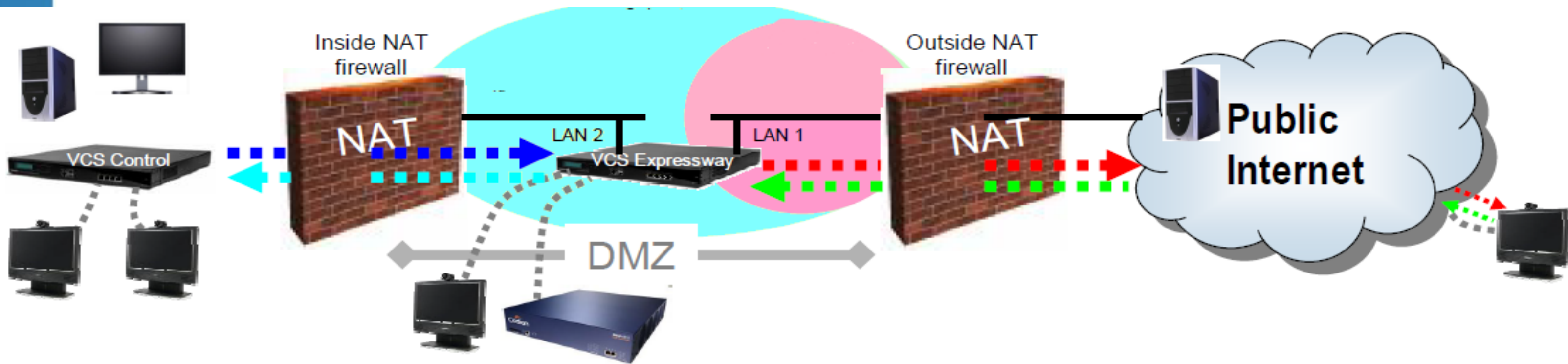
The Dual Network Interfaces option key enables the LAN 2 interface on your VCS Expressway.





The LAN 2 interface is used in situations where your VCS Expressway is located in a DMZ that consists of two separate networks - an inner DMZ and an outer DMZ - and your network is configured to prevent direct communication between the two.

With the LAN 2 interface enabled, you can configure the VCS with two separate IP addresses, one for each network in the DMZ. It also allows you to configure the static NAT option on the NIC card.

Your VCS then acts as a proxy server between the two networks, allowing calls to pass between the internal and outer firewalls that make up your DMZ.

# Using 2 VCS Expressway Interface



-  A VCS Control to VCS Expressway call is a private to public flow through the firewall, so firewall ports are normally open
-  A VCS Expressway to VCS Control call only requires responses to Control to Expressway messages, so no firewall configuration is required.
-  A VCS Expressway to Public Internet call is a private to public flow through the firewall, so firewall ports are normally open
-  A Public Internet to VCS Expressway call needs all relevant ports opened in the firewall

# Remote Access Strategy

## Collaboration Edge (Future)



# What is Collaboration Edge?

## Unified Voice, Video, Messaging, & Conferencing

### Remote and Mobile Access

Consistent experience outside the network

**Jabber and EX/MX Series**



### Business to Business

Secure communications with anyone

**Enterprise Border, Internal Border**



**Collaboration  
Edge**



### Cloud

Enterprise grade flexibility and scale

**Rich Integration WebEx, Service Provider Offerings**



### Gateway & Interop Services

Media and Signalling Normalisation

**Non-standard EP termination, Consumer to Business**

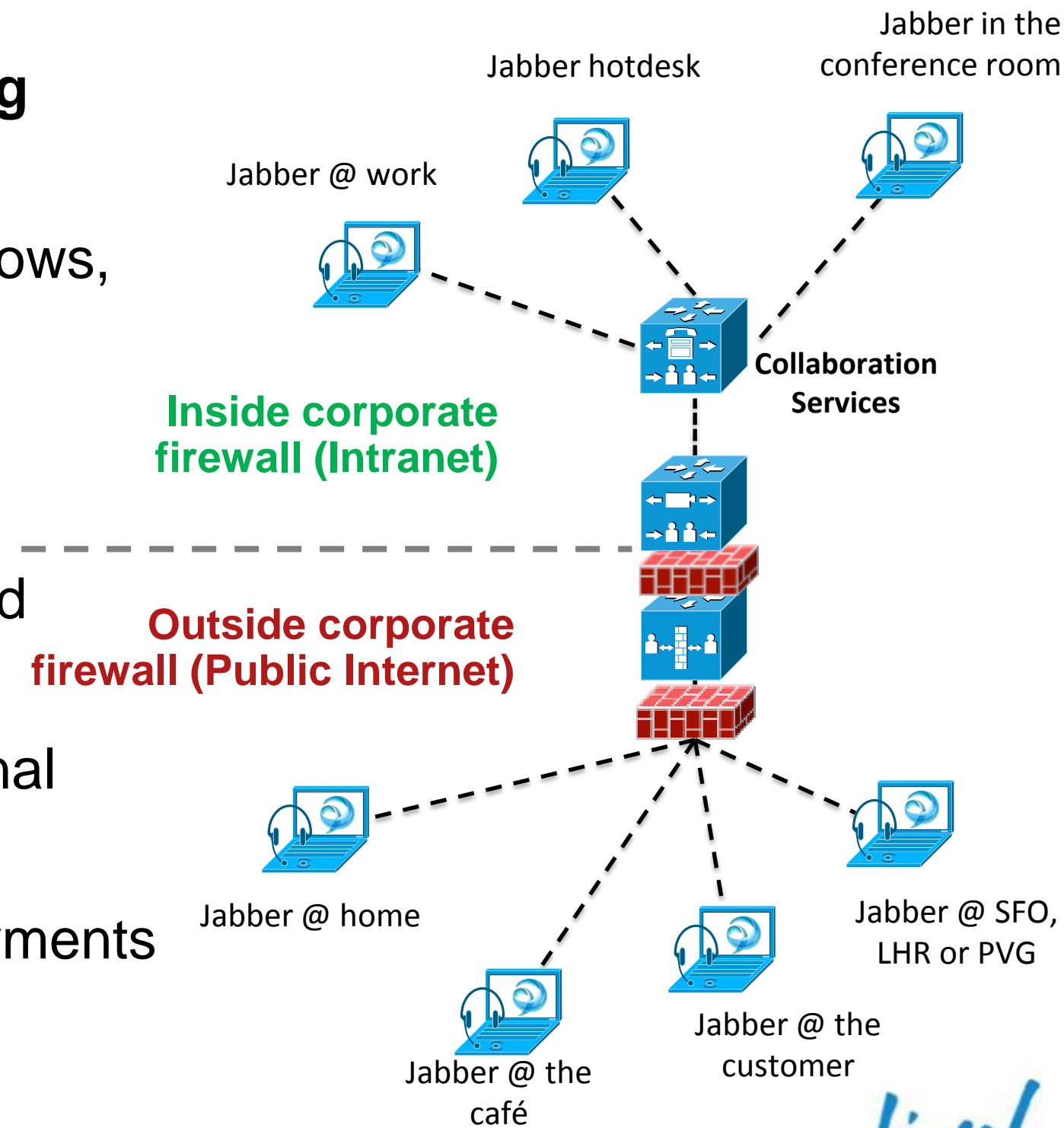


**Consistent Experience**

# Collaboration Edge

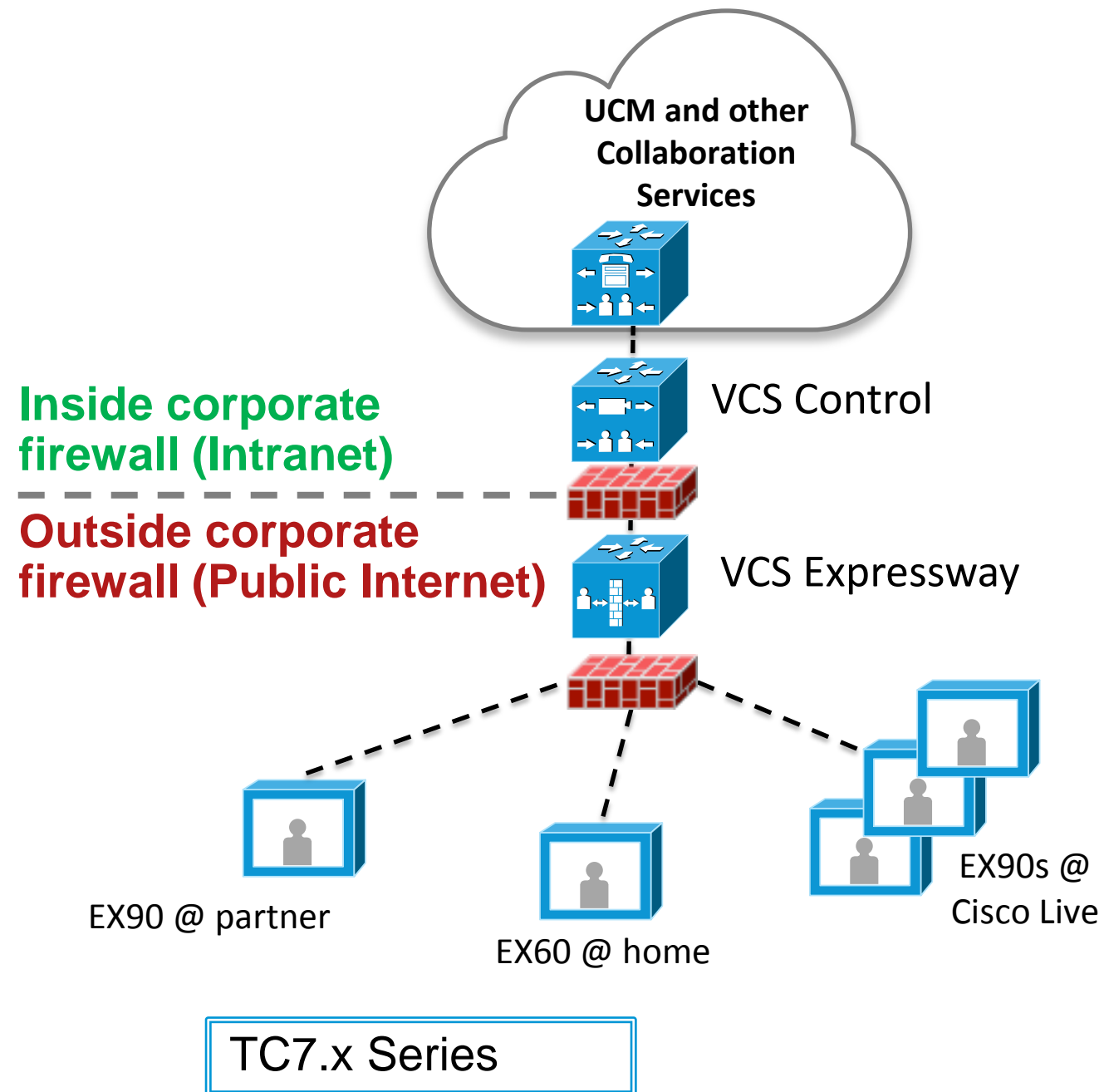
## Seamless and Secure Connectivity

- Use Jabber seamlessly (**without reconfiguring anything**) as you move around.
- Device / OS independent – works across Windows, Mac, iOS, Android
- Consistent experience inside and outside the enterprise for all Cisco UC capabilities
- Support for hybrid service models (on-prem and cloud)
- Secures only Jabber Application traffic. Personal data is not connected to the corporate network
- Easy to deploy, works with most firewall deployments





# Remote Fixed Endpoint Concept

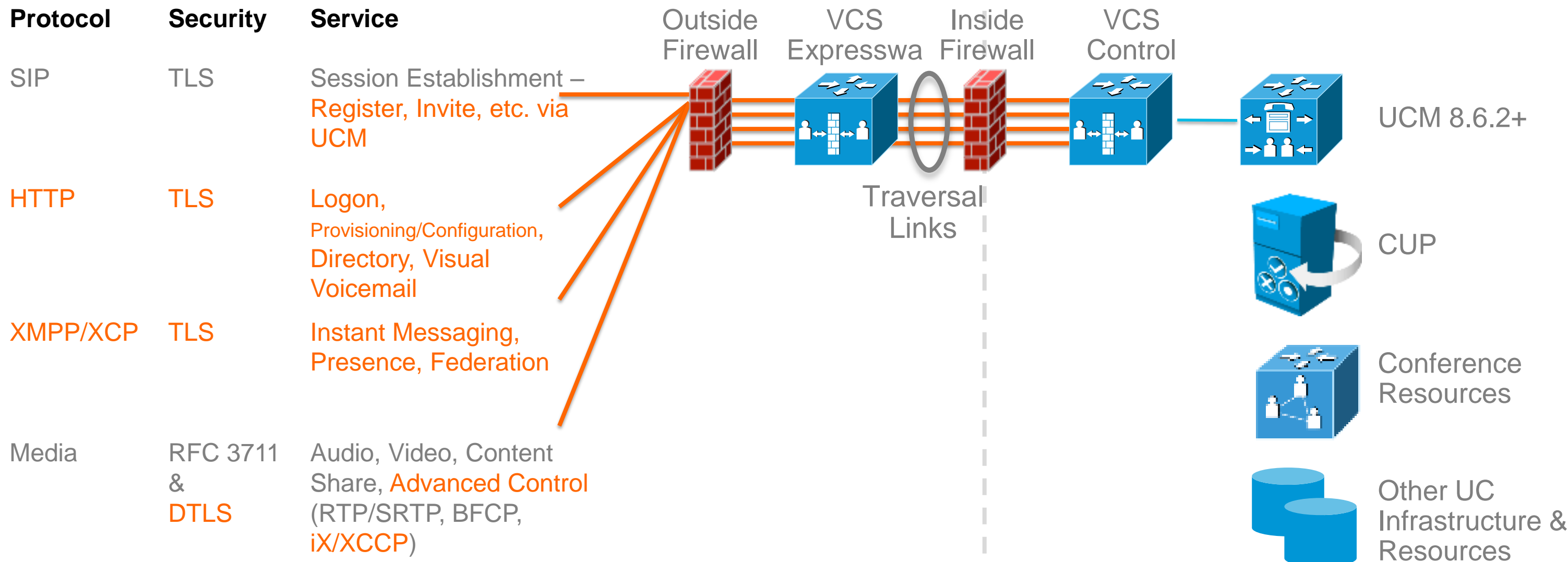


Endpoint registration, call control and provisioning serviced by UCM  
All endpoints registered to UCM

Today remote endpoint registration, call control and provisioning are serviced by VCS Control/TMS

- Remote endpoint is fully functional 'outside' network
- User can call point-to-point
- Remote worker can conference with internal and external parties via audio or video.
- Remote worker can escalate a call to multiparty
- User can share presentation
- User has access to internal directory services
- Automatic provisioning and maintenance of endpoint without user intervention

# Protocol Workloads



# What can Jabber do?

A full featured client outside the network

Outside corporate firewall (Public Internet)

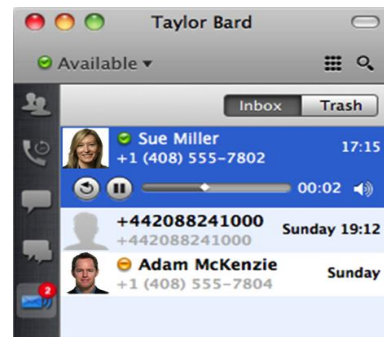
Inside corporate firewall (Intranet)

JCF-based clients: Win, Mac, iOS, Android, SDK

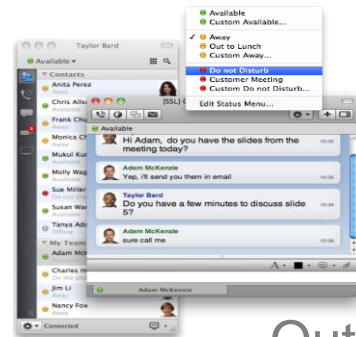
Make voice and video calls



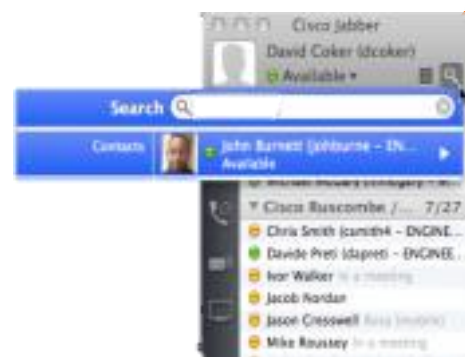
Access visual voicemail



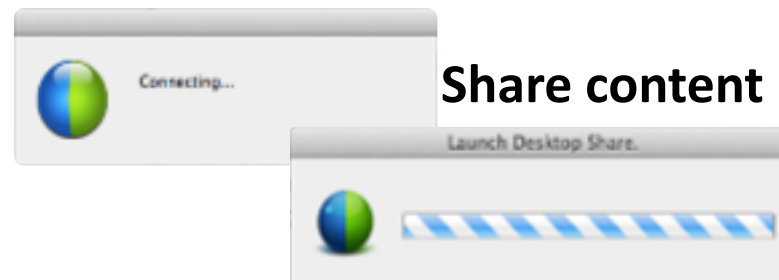
Instant Message and Presence



Search corporate directory



Launch a web conference



Share content



Jabber Clients

UCM

IP Communications

VCS Control

VCS Expressway

Outside Firewall

Inside Firewall

Personal TelePresence

Immersive TelePresence



# Q & A



# Complete Your Online Session Evaluation

## Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site [www.ciscoliveaustralia.com/mobile](http://www.ciscoliveaustralia.com/mobile)
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

[www.ciscoliveaustralia.com/portal/login.wv](http://www.ciscoliveaustralia.com/portal/login.wv)

Cisco *live!*

