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 – Hybrid

- Voice/Video, Voice Messaging, Directory Access
- HTTP/HTTPS
- XMPP
- Federated Organisation

Internet

DMZ

Cisco ASA

VPN Connection

Mobile Data Network

PSTN

Mobile Voice Network
Jabber Solution Architecture
Core Feature Functionalities

- Instant Messaging
- User Management & Authentication
- Rich Presence
- Contact Search
- Voice & Video Communications
- Voice Messaging
- WebEx Meeting Integration

Jabber brings all UC functionalities together
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

- VPN Profiles
- Auto-Reconnect
- On-Demand VPN for iOS
- Trusted Network Detection
- Certificate Authentication
- 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 Detection

**Trusted Network Configuration**

- **DNS Suffix**: comcast.net
- **DNS Server IP**: 68.87.78.130

**Untrusted Network Configuration**

- **DNS Suffix**: comcast.net
- **DNS Server IP**: 68.87.78.130

Corporate Headquarters

DHCP Request → DHCP Response

Home Office

DHCP Request → DHCP Response
Trusted Network Detection

- 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

<table>
<thead>
<tr>
<th>iPhone Network Connection</th>
<th>Configuration in Unified CM (Phone Configuration Page)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nothing Configured</td>
</tr>
<tr>
<td>Mobile Data(3/4G)</td>
<td>No auto launch</td>
</tr>
<tr>
<td>Corporate Wi-Fi</td>
<td>No auto launch</td>
</tr>
<tr>
<td>Non-corporate Wi-Fi</td>
<td>No auto launch</td>
</tr>
</tbody>
</table>

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

Resolve cm-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

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

Establish VPN
On-Demand VPN for iOS
CUCM - On-Demand VPN URL
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

SCEP request encrypted in PKCS7

ASA forwards the request to CA server
CA issues the certificate

Certificate delivered to the Client
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>iOS</th>
<th>Android ICS</th>
<th>Android (OEM or Rooted)</th>
<th>Windows and Mac OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Demand VPN</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>TND</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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

Voice/Video, Presence/IM, Directory, Visual Voicemail

AnyConnect & Jabber

Cellular Network

Full-Tunnel Tunnel

Customer Enterprise Network
Split-Tunnel
All Traffic is sent inside the VPN Tunnel
Configured under Group Policy
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
Prevent Non-Jabber Traffic

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

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

• 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 neighboured 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

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

For Your Reference
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

Systems registering directly to the VCS Expressway

Home Office
EX90 48246@company.com

Main Office
DMZ
VCS Expressway
VCS Control
Dual Profile

SIP  H.323  SIP and H.323  Media
Direct Peering Model

B2B communication

Enterprise A
DMZ

VCS Expressway

Peering

Enterprise B
DMZ

VCS Expressway

VCS Control

SIP
H.323
SIP and H.323
Media
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.

Dialing Joe.Shmoe@peerdomain.com will route across the trunk

Enterprise A

VCS-C

VCS-E

VCS-C

Enterprise B

VCS-E

VCS-C

Enterprise C

VCS-E

Internet

DNS

Dual Profile

E20

SIP

H.323

SIP and H.323

Media
Direct Peering Model
Main Office to Home Workers

Systems registering directly to the VCS Expressway

EX90 48246@company.com

SIP  H.323  SIP and H.323  Media
Open Internet Model

B2B Communications

Enterprise A
- VCS-C
- VCS-E

Internet
- DNS

Enterprise B
- VCS-C
- VCS-E

Enterprise C
- VCS-C
- VCS-E

Enterprise D
- VCS-C
- VCS-E

Enterprise XYZ
- VCS-C
- VCS-E

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

DMZ

Private network

VCS Control

NAT

10.23.72.2

64.5.2.1

LAN 1

LAN 2

VCS Expressway

Static Route

Default gateway

Internet

Private network

54.5.2.2 = public IP address

80.20.1.53

212.173.19.20

172.4.96.106
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

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

- 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

Inside corporate firewall (Intranet)
- UCM and other Collaboration Services
- VCS Control
- TC7.x Series

Outside corporate firewall (Public Internet)
- VCS Expressway
- EX90 @ partner
- EX60 @ home
- EX90s @ Cisco Live

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

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

### Outside corporate firewall (Public Internet)
- **SIP**
  - **Security**: TLS
  - **Service**: Session Establishment – Register, Invite, etc. via UCM
- **HTTP**
  - **Security**: TLS
  - **Service**: Logon, Provisioning/Configuration, Directory, Visual Voicemail
- **XMPP/XCP**
  - **Security**: TLS
  - **Service**: Instant Messaging, Presence, Federation

### Inside corporate firewall (Intranet)
- **Media**
  - **Security**: RFC 3711 & DTLS
  - **Service**: Audio, Video, Content Share, **Advanced Control** (RTP/SRTP, BFCP, iX/XCCP)

### UCM 8.6.2+
- **CUP**
- **Conference Resources**
- **Other UC Infrastructure & Resources**

---

© 2013 Cisco and/or its affiliates. All rights reserved. Cisco Public
What can Jabber do?
A full featured client outside the network

Outside corporate firewall (Public Internet)
- Access visual voicemail
- Make voice and video calls
- Search corporate directory
- Instant Message and Presence
- Outside Firewall

Inside corporate firewall (Intranet)
- Launch a web conference
- Share content

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

Jabber Clients

VCX Expressway

IP Communications

Personal TelePresence

Immersive TelePresence

UCM

VCX Control
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
- 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

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