



Cisco VCS Expressway and VCS Control – Basic Configuration

Deployment Guide

First Published: November 2010

Last Updated: May 2018

Cisco VCS X8.9

Preface

Change History

Table 1 Deployment Guide Change History

Date	Change
May 2018	Clarify that ALG (Fixup) should be disabled on firewalls serving VCS Expressway (<i>Appendix 4, Advanced Network Deployments</i>).
December 2016	Republished for X8.9.
July 2016	Republished for X8.8.
November 2015	New template applied. Advanced Network Deployments appendix revised. Republished for X8.7.
July 2015	Updated for X8.6.
April 2015	Menu path changes for X8.5. Republished with X8.5.2.
December 2014	Republished for X8.5.
August 2014	Correction in firewall appendix.
June 2014	Republished for X8.2.
December 2013	Updated for X8.1.
October 2012	Revised page layout.
August 2012	Updated for X7.2.
March 2012	Updated for X7.1. Added Appendix 4 Static NAT and Dual Network Interface architectures.
September 2011	Updated for X7.0.
November 2010	Initial release.

Contents

Preface	3
Change History	3
Introduction	7
Example Network Deployment	9
Network Elements	10
Process Summary	12
Prerequisites	13
Run the Service Setup Wizard	14
Overview	14
Task 1: Accessing and Navigating the Wizard	14
Task 2: Running the Service Setup Wizard and Applying Licenses	16
Examples for Running the Service Setup Wizard	18
VCS System Configuration	19
Task 3: Setting the System Name	19
Task 4: Configuring DNS	19
Task 5: Replacing the Default Server Certificate	21
Task 6: Configuring NTP Servers	22
Task 7: Configuring SIP Domains	23
Routing Configuration	24
Pre-search Transforms	24
Search Rules	24
Task 8: Configuring Transforms	24
Task 9: Configuring Local Zone Search Rules	25
Task 10: Configuring the Traversal Zone	28
Neighboring Between VCS Clusters	32
Task 11: Configuring Traversal Zone Search Rules	33
Task 12: Configuring the DNS Zone	35
Task 13: Configuring DNS Zone Search Rules	35
Task 14: Configuring External (Unknown) IP Address Routing	37
Endpoint Registration	39
System Checks	40
Zone Status	40
Registration Status	40
Call Signaling	40
Maintenance Routine	41
Creating a System Backup	41
Optional Configuration Tasks	42
Task 15: Configuring Cisco TMS (Optional)	42
Task 16: Configuring Logging (Optional)	44
Task 17: Configuring Registration Restriction Policy (Optional)	44
Task 18: Configuring Device Authentication Policy (Optional)	45
Task 19: Restricting Access to ISDN Gateways (Optional)	46
Appendix 1: Configuration Details	53

VCS Control Configuration Details	53
VCS Expressway Configuration Details	54
VCS Control and VCS Expressway Configuration Details	56
Appendix 2: DNS Records	57
DNS Configuration on Host Server	57
DNS Configuration (internal DNS server)	57
Appendix 3: Firewall and NAT Settings	59
Internal Firewall Configuration	59
External Firewall Configuration Requirement	60
Appendix 4: Advanced Network Deployments	63
Prerequisites	63
Recommended: Dual NIC Static NAT Deployment	63
Background Information	65
Other Deployment Examples	70
Obtaining Documentation and Submitting a Service Request	75
Cisco Legal Information	76
Cisco Trademark	76

Introduction

The Cisco TelePresence Video Communication Server (VCS) software simplifies session management and control of telepresence conferences. It provides flexible and extensible conferencing applications, enabling organizations to benefit from increased employee productivity and enhanced communication with partners and customers.

The VCS delivers exceptional scalability and resiliency, secure communications, and simplified large-scale provisioning and network administration in conjunction with Cisco TelePresence Management Suite (Cisco TMS).

The VCS interworks transparently with Cisco Unified Communications Manager (Unified CM), bringing rich telepresence services to organizations with Unified CM. It also offers interoperability with third-party unified communications, IP telephony networks, and voice-over-IP (VoIP) systems.



This document describes how to configure a VCS Expressway and a VCS Control as the cornerstones of a basic video infrastructure deployment. It takes you through the following tasks:

1. Using the Service Setup Wizard to select the services you want to use and to apply the corresponding keys (licenses).
2. Configuring system parameters and routing information.
3. Checking that the system is working as expected.
4. Configuring optional items such as Cisco TMS, system logging, and access restrictions.

Advanced configuration

This document also provides detailed DNS, NAT, and firewall configuration information. In each case we assume that you have a working knowledge of how to configure these systems. The appendices to the document provide detailed reference information, as follows:

- VCS configuration details used in this document are listed in [Appendix 1: Configuration Details, page 53](#).
- DNS records required for the example deployment used in this document are in [Appendix 2: DNS Records, page 57](#).
- Details of required NAT and firewall configurations are in [Appendix 3: Firewall and NAT Settings, page 59](#). This document describes a small subset of the numerous NAT and firewall deployment options that are made possible by using the VCS Expressway dual network interface and NAT features.
- How to deploy your system with a static NAT and Dual Network Interface architecture is explained in [Appendix 4: Advanced Network Deployments, page 63](#).

For descriptions of all system configuration parameters, see the [VCS Administrator Guide](#) and the VCS web application's online field help  and page help .

Example configuration values used in this guide

For ease of reading this guide is based around an example deployment, which uses the following assumed configuration values throughout:

	VCS Control	VCS Expressway
LAN1 IPv4 address	10.0.0.2	192.0.2.2
IPv4 gateway	10.0.0.1	192.0.2.1
LAN1 subnet mask	255.255.255.0	255.255.255.0
Domain name	<i>internal-domain.net</i>	<i>example.com</i>

Information in other deployment guides

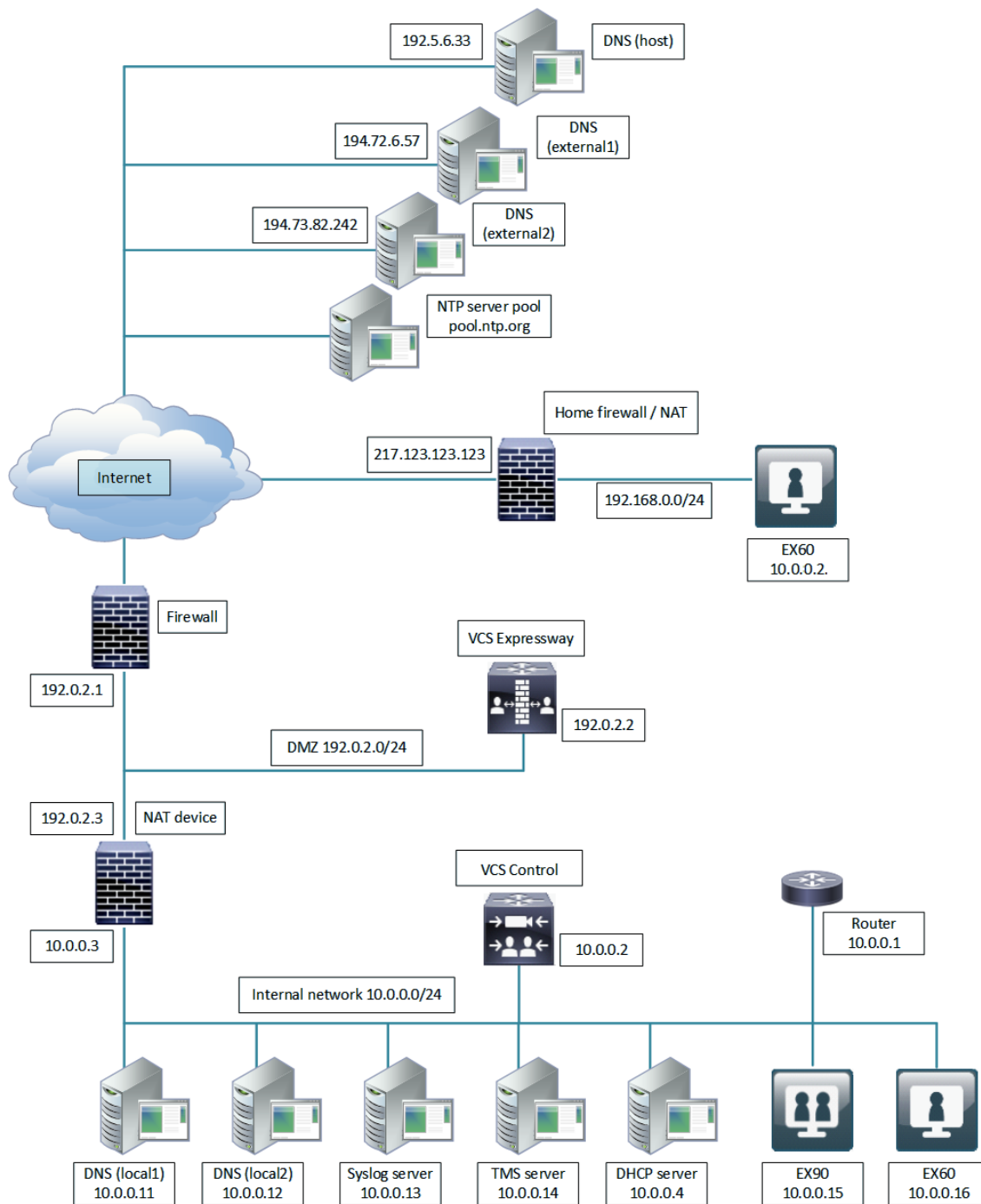
This document does not describe how to deploy a clustered system, or systems running device provisioning, device authentication, or FindMe applications. For more details about these features, see the following documents:

Introduction

- *VCS Cluster Creation and Maintenance Deployment Guide* on the [VCS configuration guides page](#)
- *Cisco TMS Provisioning Extension Deployment Guide* on the [VCS configuration guides page](#)
- *FindMe Express Deployment Guide* on the [VCS configuration guides page](#) (to deploy FindMe with the Cisco TMSPE see the *Cisco TMS Provisioning Extension Deployment Guide* instead)
- *VCS IP Port Usage for Firewall Traversal* on the [VCS configuration guides page](#)
- *Cisco VCS Authenticating Devices* on the [VCS configuration guides page](#)

Introduction

Example Network Deployment

Figure 1 Example Network for the Deployment Described in this Document

This example includes internal and DMZ segments – in which VCS Control and VCS Expressway platforms are respectively deployed.

Introduction

Network Elements

Internal Network Elements

The internal network elements are devices which are hosted on your local area network. Elements on the internal network have an internal network domain name. This name is not resolvable by a public DNS. For example, the VCS Control is configured with an internally resolvable name of `vcsc.internal-domain.net` (which resolves to an IP address of 10.0.0.2 by the internal DNS servers).

Element	Role
VCS Control	SIP Registrar & Proxy and H.323 Gatekeeper for devices which are located on the internal network.
EX90 and EX60	Example endpoints hosted on the internal network which register to the VCS Control.
DNS (local 1 & local 2)	DNS servers used by the VCS Control to perform DNS lookups (resolve network names on the internal network).
DHCP Server	Provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.
Router	Acts as the gateway for all internal network devices to route towards the DMZ (to the NAT device internal address).
Cisco TMS Server	Management and scheduling server. See Task 15: Configuring Cisco TMS (Optional) , page 42.
Syslog Server	Logging server for Syslog messages. See Task 16: Configuring Logging (Optional) , page 44.

DMZ Network Element

VCS Expressway

The VCS Expressway is a SIP Registrar & Proxy and H.323 Gatekeeper for devices which are located outside the internal network (for example, home users and mobile worker registering across the internet and 3rd party businesses making calls to, or receiving calls from this network).

The VCS Expressway is configured with a traversal server zone to receive communications from the VCS Control in order to allow inbound and outbound calls to traverse the NAT device.

The VCS Expressway has a public network domain name. For example, the VCS Expressway is configured with an externally resolvable name of `vcse.example.com` (which resolves to an IP address of 192.0.2.2 by the external / public DNS servers).

External Network Elements

Element	Role
EX60	An example remote endpoint, which is registering to the VCS Expressway via the internet.
DNS (Host)	The DNS owned by the service provider which hosts the external domain <code>example.com</code> .
DNS (external 1 & external 2)	The DNS used by the VCS Expressway to perform DNS lookups.
NTP server pool	An NTP server pool which provides the clock source used to synchronize both internal and external devices.

NAT Devices and Firewalls

The example deployment includes:

Introduction

- NAT (PAT) device performing port address translation functions for network traffic routed from the internal network to addresses in the DMZ (and beyond – towards remote destinations on the internet).
- Firewall device on the public-facing side of the DMZ. This device allows all outbound connections and inbound connections on specific ports. See [Appendix 3: Firewall and NAT Settings, page 59](#).
- Home firewall NAT (PAT) device which performs port address and firewall functions for network traffic originating from the EX60 device.
- See [Appendix 4: Advanced Network Deployments, page 63](#) for information about how to deploy your system with a static NAT and Dual Network Interface architecture.

SIP and H.323 Domain

The example deployment is configured to route SIP (and H.323) signaling messages for calls made to URIs which use the domain example.com. The DNS SRV configurations are described in [Appendix 2: DNS Records, page 57](#).

- DNS SRV records are configured in the public (external) and local (internal) network DNS server to enable routing of signaling request messages to the relevant infrastructure elements (for example, before an external endpoint registers, it will query the external DNS servers to determine the IP address of the VCS Expressway).
- The internal SIP domain (example.com) is the same as the public DNS name. This enables both registered and non-registered devices in the public internet to call endpoints registered to the VCS Control.

Process Summary

Before You Begin

- [Prerequisites, page 13](#)

Run the Service Setup Wizard

- [Task 1: Accessing and Navigating the Wizard, page 14](#)
- [Task 2: Running the Service Setup Wizard and Applying Licenses, page 16](#)
- [Examples for Running the Service Setup Wizard, page 18](#)

VCS system configuration tasks

- [Task 3: Setting the System Name, page 19](#)
- [Task 4: Configuring DNS, page 19](#)
- [Task 5: Replacing the Default Server Certificate, page 21](#)
- [Task 6: Configuring NTP Servers, page 22](#)
- [Task 7: Configuring SIP Domains, page 23](#)

Routing configuration tasks

- [Task 8: Configuring Transforms, page 24](#)
- [Task 9: Configuring Local Zone Search Rules, page 25](#)
- [Task 10: Configuring the Traversal Zone, page 28](#)
- [Task 11: Configuring Traversal Zone Search Rules, page 33](#)
- [Task 12: Configuring the DNS Zone, page 35](#)
- [Task 13: Configuring DNS Zone Search Rules, page 35](#)
- [Task 14: Configuring External \(Unknown\) IP Address Routing, page 37](#)

Optional configuration tasks

- [Task 15: Configuring Cisco TMS \(Optional\), page 42](#)
- [Task 16: Configuring Logging \(Optional\), page 44](#)
- [Task 17: Configuring Registration Restriction Policy \(Optional\), page 44](#)
- [Task 18: Configuring Device Authentication Policy \(Optional\), page 45](#)
- [Task 19: Restricting Access to ISDN Gateways \(Optional\), page 46](#)

Prerequisites

Prerequisites

Before you begin any of the tasks in this guide, make sure that the following prerequisites are complete.

General prerequisites

- We recommend that you use the VCS web user interface to do the system configuration. This guide assumes that you are using a web browser running on a PC. The PC needs an Ethernet connection to a LAN which can route HTTP(S) traffic to the VCS.
- Review the relevant release notes on the [VCS release notes page](#).
- Have the *VCS Administrator Guide* on the [VCS maintenance and operation guides page](#) available for reference before you start.

IP address and password prerequisites

This guide also assumes that you have already configured a static IP address and changed the default passwords, as described in the appropriate installation guide:

- *Cisco VCS Virtual Machine Installation Guide* on the [VCS installation guides page](#).
- *Cisco Video Communication Server CE1100 Appliance Installation Guide* on the [VCS installation guides page](#).

Note: VCS requires a static IP address. It doesn't use DHCP/SLAAC to get an IP address.

DNS, NAT/firewall, and DHCP prerequisites

The following non-VCS system configuration needs to be in place before you start:

- Internal and external DNS records. See [Appendix 2: DNS Records, page 57](#).
- NAT & firewall configuration. See [Appendix 3: Firewall and NAT Settings, page 59](#).
- DHCP server configuration (not described in this document).

Run the Service Setup Wizard

Run the Service Setup Wizard

Overview

The Service Setup Wizard makes it easier to configure and license the VCS for its chosen purpose in your environment. It also simplifies the user interface. You select from a list of popular VCS services and the wizard then prompts you with the licensing requirements for those services. You can also use the wizard to review and edit the VCS basic network settings (typically already configured during initial installation).

When you restart the VCS, the user interface is tailored to match your service selections. You only see menus and pages for the services you chose.

Note: Some services are incompatible and cannot be selected together. The [VCS Administrator Guide](#) and the online help provide a matrix of compatible services. The matrix specifies which services you can use together on the same system or cluster.

What If I Don't Want to Use the Wizard?

A skip option exists if you don't want to use the wizard. If you change your mind later, you can go back and run it at any time (**Status > Overview** page; click **Run service setup**).

If you opt to skip the wizard, you need to deal with the VCS licensing setup requirements manually before you start the configuration tasks in this guide. Also, the user interface isn't customized to reflect your specific service selections.

Task 1: Accessing and Navigating the Wizard

There are multiple ways to access the wizard:

- As of X8.8, you'll automatically see the Service Setup Wizard when you first log in to the VCS user interface. You don't need to launch it.
- If you previously logged in or have upgraded, you'll see the **Status > Overview** page as usual. Click **Run service setup** to launch the wizard.
- If you've already run the wizard you can rerun it at any time. From the **Status > Overview** page, click **Return to service setup**.

To navigate the wizard:


- Click **Skip Service Setup Wizard** if you want to back out of the wizard completely, or **Back** to return to the previous page.
- Click **Continue** to save and move to the next wizard page.

Run the Service Setup Wizard

Figure 2 Service Setup Wizard Example - Selection Page


Welcome to Cisco Collaboration services [Help](#) [Logout](#)

Select Series

Expressway series ☒ 


VCS series ☐

Select Type

Expressway-C ☒ 

Expressway-E ☐

Select Services

After you select services, you get a simplified menu that is relevant to your selection. 

Cisco Spark Hybrid Services ☐

Mobile and remote access ☐

Jabber Guest services ☐

Microsoft Interoperability ☐

Registrar ☐

Collaboration Meeting Rooms (CMR) Cloud ☐

Business to business calls ☐

If you proceed without selecting services, you will get the full menu.

Proceed without selecting services ☐

[Cancel](#) [Continue](#)

5. On the **Option Keys** page, click the [Product License Registration Portal](#) link to go to the licensing portal. (For this step you need to work away from the wizard to obtain the necessary licenses, and you need the serial number of the system.) In the licensing portal, enter the necessary details for the required licenses.

Detailed information about using the licensing portal is in the online help or the [VCS Administrator Guide](#). An ordering guide for our products is available on the Cisco [Collaboration Ordering Guides page](#).

6. Wait for system-generated emails from the licensing portal with the release key and option keys for your selected services.
7. Back in the wizard, paste the text from the release key email into the first text area. The system reads the release key out of the pasted text and displays it next to the text area.
8. Paste the text from the option keys email into the second text area. The system reads the option keys out of the pasted text and displays them next to the text area.
9. Add new text areas if you have more email text to paste in, such as your room or desktop system registration license keys.
10. Click **Add Keys**.

The **License status** table groups the keys that are possible on this system, and indicates whether they are loaded or not loaded. The keys are grouped as follows:

 - **Required:** If any keys in this section are not yet loaded, you see status **Required** and will not be able to continue through the wizard.
 - **Optional:** Shows keys that may or may not be useful, but are not strictly required for the services you chose.
 - **Unrelated:** These keys won't harm the system if they are loaded, but will not provide any benefit for the services you chose.
 - **Incompatible:** These keys cannot work with the selected services. You must remove them or choose different services before you can continue.
11. Click **Continue**.
12. Review the network configuration and modify the settings if necessary. Save any changes before you continue the wizard.
13. Click **Finish**.
14. Restart the system when prompted.

Result: When you log in, the user interface is tailored to match your service selections. You only see menus and pages for the services you chose.

What to do next

The wizard is complete for the VCS Control element. Now you need to run it on the VCS Expressway. For typical deployments with the VCS Expressway the services you are most likely to select with the wizard include *Mobile and remote access* and *Business to business calls*. When the VCS Expressway is done, go to the next section in this guide, "VCS System Configuration."

Examples for Running the Service Setup Wizard

Example for VCS Registrar

1. Click *VCS series*.
2. Click *VCS Control*.
3. Check *Registrar*.
4. Check any other compatible services that you have bought for this system. For this example, let's assume *Business to business calls*. (The matrix of compatible services is in the online help and the [VCS Administrator Guide](#).)
5. Click **Continue**.
The wizard takes you to the licensing and options page.
6. [If required] Paste the release key into the first text area.
7. Paste the VCS series key into the second text area (eg. 116341E00-1-~~AAAAAAA~~).
8. Click **Continue**.
9. Review the networking configuration and click **Continue**.
10. Restart the system when prompted.

This completes the service setup and licensing for the VCS Control part of your desired outcome. However, since we chose *Business to business calls*, we would have to run the wizard again to set up and license the VCS Expressway, because the business to business calling deployment requires firewall traversal.

VCS System Configuration

Task 3: Setting the System Name

The **System name** defines the name of the VCS. It appears in various places in the web interface and is also used by Cisco TMS. We recommend using a name that lets you easily and uniquely identify the VCS.

To configure the **System name**:

1. Go to **System > Administration**.
2. Configure the **System name** as follows:

	VCS Control	VCS Expressway
System name	Enter <code>vcsc</code>	Enter <code>vcse</code>

3. Click **Save**.

Figure 4 VCS Control

The screenshot shows the 'System administration' page for VCS Control. The breadcrumb trail indicates 'You are here: System > Administration'. The 'System name' field is highlighted with a blue box. Below it, the 'System name' label is followed by a text input field containing 'VCSc' and an information icon.

Figure 5 VCS Expressway

The screenshot shows the 'System administration' page for VCS Expressway. The breadcrumb trail indicates 'You are here: System > Administration'. The 'System name' field is highlighted with a blue box. Below it, the 'System name' label is followed by a text input field containing 'VCSe' and an information icon.

Task 4: Configuring DNS

System Host Name

The **System host name** defines the DNS hostname that this system is known by. Note that this is not the fully-qualified domain name, just the host label portion.

Note that **<System host name>.<Domain name>** = FQDN of this VCS.

To configure the **System host name**:

1. Go to **System > DNS**.
2. Configure the **System host name** as follows:

	VCS Control	VCS Expressway
System host name	Enter <code>vcsc</code>	Enter <code>vcse</code>

3. Click **Save**.

VCS System Configuration

Domain Name

The **Domain name** is the name to append to an unqualified host name before querying the DNS server.

To configure the **Domain name**:

1. Go to **System > DNS**.
2. Configure the **Domain name** as follows:

	VCS Control	VCS Expressway
Domain name	Enter <code>internal-domain.net</code>	Enter <code>example.com</code>

3. Click **Save**.

The fully qualified domain name for the VCS Control is now `vcsc.internal-domain.net`

The fully qualified domain name for the VCS Expressway is now `vcse.example.com`

DNS Servers

The DNS server addresses specify the IP addresses of up to five domain name servers to be used for resolving domain names. In either of the following cases you must specify at least one default DNS server for address resolution:

- To use fully qualified domain names instead of IP addresses when specifying external addresses. For example, for LDAP and NTP servers, neighbor zones and peers.
- To use features such as URI dialing or ENUM dialing.

The VCS queries one server at a time. If that server is unavailable the VCS tries another server from the list.

In the example deployment two DNS servers are configured for each VCS, which provides a level of DNS server redundancy. The VCS Control is configured with DNS servers which are located on the internal network. The VCS Expressway is configured with DNS servers which are publicly routable.

To configure the **Default DNS server** addresses:

1. Go to **System > DNS**.
2. Configure the DNS server **Address** fields as follows:

	VCS Control	VCS Expressway
Address 1	Enter <code>10.0.0.11</code>	Enter <code>194.72.6.57</code>
Address 2	Enter <code>10.0.0.12</code>	Enter <code>194.73.82.242</code>

3. Click **Save**.

VCS System Configuration

VCS Control has a fully qualified domain name of `vcsc.internal-domain.net`

DNS

DNS settings

Local host name	<input type="text" value="vcsc"/>	
Domain name	<input type="text" value="internal-domain.net"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

Default DNS servers

Address 1	<input type="text" value="10.0.0.11"/>	
Address 2	<input type="text" value="10.0.0.12"/>	
Address 3	<input type="text"/>	
Address 4	<input type="text"/>	
Address 5	<input type="text"/>	

VCS Expressway has a fully qualified domain name of `vcse.example.com`

DNS

DNS settings

Local host name	<input type="text" value="vcse"/>	
Domain name	<input type="text" value="example.com"/>	
DNS requests port range	<input type="text" value="Use the ephemeral port range"/>	

Default DNS servers

Address 1	<input type="text" value="194.72.6.57"/>	
Address 2	<input type="text" value="194.73.82.242"/>	
Address 3	<input type="text"/>	
Address 4	<input type="text"/>	
Address 5	<input type="text"/>	

Task 5: Replacing the Default Server Certificate

For extra security, you may want to have the VCS communicate with other systems (such as LDAP servers, neighbor VCSs, or clients such as SIP endpoints and web browsers) using TLS encryption.

For this to work successfully in a connection between a client and server:

- The server must have a certificate installed that verifies its identity. This certificate must be signed by a Certificate Authority (CA).
- The client must trust the CA that signed the certificate used by the server.

VCS System Configuration

The VCS allows you to install a certificate that can represent the VCS as either a client or a server in connections using TLS. The VCS can also authenticate client connections (typically from a web browser) over HTTPS. You can also upload certificate revocation lists (CRLs) for the CAs used to verify LDAP server and HTTPS client certificates.

The VCS can generate server certificate signing requests (CSRs). This removes the need to use an external mechanism to generate certificate requests.

For secure communications (HTTPS and SIP/TLS) we recommend that you replace the VCS default certificate with a certificate generated by a trusted certificate authority.

Note that in connections:

- to an endpoint, the VCS acts as the TLS server
- to an LDAP server, the VCS is a client
- between two VCS systems, either VCS may be the client with the other VCS being the TLS server
- via HTTPS, the web browser is the client and the VCS is the server

TLS can be difficult to configure. For example, when using it with an LDAP server we recommend that you confirm the system is working correctly over TCP before attempting to secure the connection with TLS. We also recommend using a third party LDAP browser to verify that your LDAP server is correctly configured for TLS.

Note: Be careful not to allow your CA certificates or CRLs to expire. This may cause certificates signed by those CAs to be rejected.

To load the trusted CA list, go to **Maintenance > Security certificates > Trusted CA certificate**.

To generate a CSR and/or upload the VCS's server certificate, go to **Maintenance > Security certificates > Server certificate**.

For full information, see *VCS Certificate Creation and Use Deployment Guide* on the [VCS configuration guides page](#).

Task 6: Configuring NTP Servers

The **NTP server** address fields set the IP addresses or Fully Qualified Domain Names (FQDNs) of the NTP servers to be used to synchronize system time. The **Time zone** sets the local time zone of the VCS.

Note: You can synchronize the VCS Control and VCS Expressway with different NTP servers, if the result is that the VCS traversal pair are synchronized.

To configure the NTP server address and time zone:

1. Go to **System > Time**.
2. Configure the fields as follows, on both VCS Control and VCS Expressway:

	VCS Control	VCS Expressway
NTP server 1	Enter pool.ntp.org	Enter pool.ntp.org
Time zone	GMT in this example	GMT in this example

3. Click **Save**.

VCS System Configuration

Time You are here: [System](#) > [Time](#)

NTP servers

NTP server 1	Address	<input type="text" value="pool.ntp.org"/>	Authentication	<input type="button" value="Disabled"/>
NTP server 2	Address	<input type="text"/>	Authentication	<input type="button" value="Disabled"/>
NTP server 3	Address	<input type="text"/>	Authentication	<input type="button" value="Disabled"/>
NTP server 4	Address	<input type="text"/>	Authentication	<input type="button" value="Disabled"/>
NTP server 5	Address	<input type="text"/>	Authentication	<input type="button" value="Disabled"/>

Time zone

Time zone

Task 7: Configuring SIP Domains

The VCS acts as a SIP Registrar for configured SIP domains, accepting registration requests for any SIP endpoints attempting to register with an alias that includes these domains.

- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See [Task 17: Configuring Registration Restriction Policy \(Optional\)](#), page 44.
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

- Go to **Configuration > Domains**.
- Click **New**.
- Enter the domain name into the **Name** field (on both VCS Control and VCS Expressway):

	VCS Control	VCS Expressway
Name	Enter example.com	Enter example.com

- Click **Create domain**.
- The **Domains** page displays all configured SIP domain names.

Domains You are here: [Configuration](#) > [Domains](#) > [New](#)

Configuration

Domain name

On VCS Expressway, if you are not using device authentication, leave **Traversal zone for delegated credential checking** set to *Do not delegate*. If you are using device authentication, see [Task 18: Configuring Device Authentication Policy \(Optional\)](#), page 45.

What To Do Next

The VCS system configuration is now complete. Go to the next section, "[Routing Configuration](#)."

Routing Configuration

Pre-search Transforms

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The VCS applies the transformation before any searches take place, either locally or to external zones.

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices. This means that the same call searches work for calls from both H.323 and SIP endpoints.

For example, if the called address is an H.323 E.164 alias "01234", the VCS automatically appends the configured domain name (in this case example.com) to the called address (that is, 01234@example.com making it into a URI), before attempting to set up the call.

- Use pre-search transforms with care, because they apply to *all* signaling messages. If they match, they will affect the routing of Unified Communications messages, provisioning and presence requests as well as call requests.
- Transformations can also be carried out in search rules. Consider whether it's best to use a pre-search transform or a search rule to modify the called address to be looked up.

Search Rules

Search rules define how the VCS routes calls (to destination zones) in specific call scenarios. When a search rule is matched, the destination alias can be modified according to the conditions defined in the search rule.

The search rules described in this document are used to ensure that endpoints can dial H.323 devices that have registered E.164 numbers or H.323 IDs without a domain portion. The search rules first search for received destination aliases without the domain portion of the URI, and then search with the full URI.

The search rules described here are used to enable the following routing combinations:

Calling party	Called party
Registered devices (VCS Control or VCS Expressway)	Registered devices (VCS Control or VCS Expressway)
Registered devices (VCS Control or VCS Expressway)	External domains and un-registered devices (via VCS Expressway using DNS zone)
Registered devices (VCS Control or VCS Expressway)	Public external IP addresses (via VCS Expressway)
External domains and un-registered devices	Registered devices (VCS Control or VCS Expressway)

The routing configuration in this document searches for destination aliases that have valid SIP URIs. That is, using a valid SIP domain, such as id@domain.

You can configure routing which enables calls to unregistered devices on an internal network (routing to the addresses of IP of the devices) by configuring a search rule with a mode of *Any IP address* with target Local Zone. However this is not recommended (and not described in this document). The best practice is to register all devices and route using destination aliases.

Task 8: Configuring Transforms

The pre-search transform configuration described in this document is used to standardize destination aliases originating from both H.323 and SIP devices.

Routing Configuration

The following transform modifies the destination alias of all call attempts made to destination aliases which do not contain an '@'. The old destination alias has @example.com appended to it, thus standardizing all called destination aliases into a SIP URI format.

To configure the transform:

1. Go to **Configuration > Dial plan > Transforms**.
2. Click **New**.
3. Configure the transform fields as follows:

	VCS Control	VCS Expressway
Priority	Enter 1	Same as VCS Control
Description	Enter Transform destination aliases to URI format	
Pattern type	Regex	
Pattern string	Enter ([^@] *)	
Pattern behavior	Replace	
Replace string	Enter \1@example.com	
State	Enabled	

4. Click **Create transform**.

Create transform You are here: [Configuration](#) > [Dial plan](#) > [Transforms](#) > Create transform

Configuration

Priority	<input type="text" value="1"/>	
Description	<input type="text" value="Transform destination aliases to URI format"/>	
Pattern type	Regex	
Pattern string	<input type="text" value="* ([^@]*)"/>	
Pattern behavior	Replace	
Replace string	<input type="text" value="\1@example.com"/>	
State	Enabled	

Task 9: Configuring Local Zone Search Rules

To configure the search rules to route calls to the Local Zone (to locally registered endpoint aliases):

1. Go to **Configuration > Dial plan > Search rules**.
2. First disable the supplied default search rule (**LocalZoneMatch**), as follows:
 - a. Select the check box next to **LocalZoneMatch**.
 - b. Click **Disable**.
 - c. Click **OK**.

Routing Configuration

3. Click **New**.
4. Configure the search rule fields as follows:

	VCS Control	VCS Expressway
Rule name	Enter <code>Local zone - no domain</code>	Same as VCS Control
Description	Enter <code>Search local zone for H.323 devices (strip domain)</code>	
Priority	Enter <code>48</code>	
Protocol	<i>Any</i>	
Source	<i>Any</i>	
Request must be authenticated	<i>No</i>	
Mode	<i>Alias pattern match</i>	
Pattern type	<i>Regex</i>	
Pattern string	Enter <code>(.+)@example\.com.*</code>	
Pattern behavior	<i>Replace</i>	
Replace string	Enter <code>\1</code>	
On successful match	<i>Continue</i>	
Target	<i>LocalZone</i>	
State	<i>Enabled</i>	

Routing Configuration

5. Click **Create search rule**.

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	★ Local zone – no domain ⓘ
Description	Search local zone for H.323 devices (strip domain) ⓘ
Priority	★ 48 ⓘ
Protocol	Any ⓘ
Source	Any ⓘ
Request must be authenticated	No ⓘ
Mode	Alias pattern match ⓘ
Pattern type	Regex ⓘ
Pattern string	★ (.+)@example.com.* ⓘ
Pattern behavior	Replace ⓘ
Replace string	\1 ⓘ
On successful match	Continue ⓘ
Target	★ LocalZone ⓘ
State	Enabled ⓘ

6. Click **New**.

Routing Configuration

7. Configure the search rule fields as follows:

	VCS Control	VCS Expressway
Rule name	Enter <code>Local zone - full URI</code>	Same as VCS Control
Description	Enter <code>Search local zone for SIP and H.323 devices with a domain</code>	
Priority	Enter <code>50</code>	
Protocol	<i>Any</i>	
Source	<i>Any</i>	
Request must be authenticated	<i>No</i>	
Mode	<i>Alias pattern match</i>	
Pattern type	<i>Regex</i>	
Pattern string	Enter <code>(.+)@example.com.*</code>	
Pattern behavior	<i>Leave</i>	
On successful match	<i>Continue</i>	
Target	<i>LocalZone</i>	
State	<i>Enabled</i>	

8. Click **Create search rule**.

Task 10: Configuring the Traversal Zone

The traversal zone configuration defines a connection between the VCS Control and VCS Expressway platforms. A traversal zone connection allows firewall traversal for signaling and media between the two platforms. VCS Control is configured with a traversal client zone. VCS Expressway is configured with a traversal server zone.

Which type of traversal zone?

- If your deployment is for business to business calling, use a traversal zone.
- If your deployment is for mobile and remote access, use a Unified Communications traversal zone (see next section).

Traversal zones for Unified Communications

If you need Unified Communications features like mobile and remote access or Jabber Guest, a secure traversal zone connection must exist between VCS Control and VCS Expressway:

- The VCS Control and VCS Expressway must be configured with a zone of type *Unified Communications traversal*. This automatically configures an appropriate traversal zone (a traversal client zone when selected on VCS Control or a traversal server zone when selected on VCS Expressway) that uses SIP TLS with **TLS verify mode** set to *On*, and **Media encryption mode** set to *Force encrypted*.
- Both VCSs must trust each other's server certificate. As each VCS acts both as a client and as a server you must ensure that each VCS's certificate is valid both as a client and as a server.
- If an H.323 or a non-encrypted connection is also required, a separate pair of traversal zones must be configured.

Routing Configuration

To configure the traversal zone:

1. Go to **Configuration > Zones > Zones**.
2. Click **New**.
3. Configure the fields as follows. Leave all other fields with default values:

	VCS Control	VCS Expressway
Name	Enter TraversalZone	Enter TraversalZone
Type	<i>Traversal client</i>	<i>Traversal server</i>
Username	Enter exampleauth	Enter exampleauth
Password	Enter ex4mpl3.c0m	Not applicable
H.323 Mode	<i>On</i>	<i>On</i>
H.323 Protocol	<i>Assent</i>	<i>Assent</i>
H.323 Port	Enter 6001	Enter 6001
H.323 H.460.19 demultiplexing mode	Not applicable	<i>Off</i>
SIP Mode	<i>On</i>	<i>On</i>
SIP Port	Enter 7001	Enter 7001
SIP Transport	<i>TLS</i>	<i>TLS</i>
SIP TLS verify mode	<i>Off</i>	<i>Off</i>
SIP Accept proxied registrations	<i>Allow</i>	<i>Allow</i>
Location Peer 1 address	Enter 192.0.2.2	Not applicable


4. Click **Create zone**.


Routing Configuration


Figure 6 VCS Control

Create zone You are here: [Configuration](#) > [Zones](#) > [Zones](#) > Create zone


Configuration


Name ★ 

Type ★ 


Hop count ★ 


Connection credentials


Username ★ 

Password ★ 


H.323


Mode 


Protocol 


Port ★ 


SIP


Mode 


Port ★ 


Transport 

TLS verify mode 


Accept proxied registrations 

Media encryption mode 


ICE support 

Poison mode 


Authentication

Authentication policy 

Client settings

Retry interval ★ 

Location

Peer 1 address 

Routing Configuration

Figure 7 VCS Expressway

Create zone You are here: [Configuration](#) > [Zones](#) > [Zones](#) > Create zone

Configuration

Name ★ ⓘ

Type ★ ⓘ

Hop count ★ ⓘ

Connection credentials

Username ★ ⓘ

Password ★ Ensure matching credentials are configured in the [local database](#) or the H.350 directory.

H.323

Mode ⓘ

Protocol ⓘ

Port ★ ⓘ

H.460.19 demultiplexing mode ⓘ

SIP

Mode ⓘ

Port ★ ⓘ

Transport ⓘ

TLS verify mode ⓘ

Accept proxied registrations ⓘ

Media encryption mode ⓘ

ICE support ⓘ

Poison mode ⓘ

Authentication

Authentication policy ⓘ

Configuring authentication credentials in VCS Expressway

To configure the authentication credentials in the **Local authentication database** (configured in the VCS Expressway only), do the following:

1. Go to **Configuration > Authentication > Devices > Local database**.
2. Click **New**.

Routing Configuration

3. Configure the fields as follows:

	VCS Control	VCS Expressway
Name	Not applicable	Enter <code>exampleauth</code>
Password	Not applicable	Enter <code>ex4mp13.c0m</code>

4. Click **Create credential**.

Local authentication database You are here: [Configuration](#) > [Authentication](#) > [Devices](#) > [Local database](#)

Configuration

Name ⓘ

Password ⓘ

Neighboring Between VCS Clusters

You can neighbor your local VCS (or VCS cluster) to a remote VCS cluster; this remote cluster could be a neighbor, traversal client, or traversal server to your local VCS. In this case, when a call is received on your local VCS and is passed via the relevant zone to the remote cluster, it will be routed to whichever peer in that neighboring cluster has the lowest resource usage. That peer will then forward the call as appropriate to one of its:

- locally registered endpoints (if the endpoint is registered to that peer)
- peers (if the endpoint is registered to another peer in that cluster)
- external zones (if the endpoint has been located elsewhere)

Lowest resource usage is determined by comparing the number of available traversal calls (maximum - current use) on the peers, and choosing the peer with the highest number. Peers that are in maintenance mode are not considered.

When configuring a connection to a remote cluster, you create a single zone and configure it with details of all the peers in the cluster. Adding this information to the zone ensures that the call is passed to that cluster regardless of the status of the individual peers.

You also need to enter the IP address of all peers in the remote cluster when the connection is via a **neighbor** or **traversal client** zone. You do not do this for **traversal server** zones, as these connections are not configured by specifying the remote system's IP address.

Note: Systems that are configured as peers must **not** also be configured as neighbors to each other, and vice versa.

Neighboring your clusters

To neighbor your local VCS (or VCS cluster) to a remote VCS cluster, you create a single zone to represent the cluster and configure it with the details of all the peers in that cluster:

1. On your local VCS (or, if the local VCS is a cluster, on the primary peer), create a zone of the appropriate type. This zone will represent the connection to the cluster.
2. In the **Location** section, enter the IP address or FQDN of each peer in the remote cluster in the **Peer 1 to Peer 6** address fields.

Note that:

- Ideally you should use FQDNs in these fields. Each FQDN must be different and must resolve to a single IP address for each peer. With IP addresses, you may not be able to use TLS verification, because many CAs will not supply certificates to authenticate an IP address.

Routing Configuration

- The order in which the peers in the remote VCS cluster are listed here does not matter.
- Whenever you add an extra VCS to a cluster (to increase capacity or improve redundancy, for example) you will need to modify any VCSs which neighbor to that cluster to let them know about the new cluster peer.

Task 11: Configuring Traversal Zone Search Rules

To create the search rules to route calls via the traversal zone.

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows:

	VCS Control	VCS Expressway
Rule name	"Traversal zone search rule" for example	"Traversal zone search rule" for example
Description	"Search traversal zone - VCSe" for example	"Search traversal zone - VCSc" for example
Priority	100	100
Protocol	<i>Any</i>	<i>Any</i>
Source	<i>Any</i>	<i>Any</i>
Request must be authenticated	<i>No</i>	<i>No</i>
Mode	<i>Any alias</i>	<i>Any alias*</i>
On successful match	<i>Continue</i>	<i>Continue</i>
Target	<i>Traversal zone</i>	<i>Traversal zone</i>
State	<i>Enabled</i>	<i>Enabled</i>

* This example routes any alias across the traversal zone towards the VCS Control. You can be more selective by adding search rules or configuring call policy.

4. Click **Create search rule**.

Routing Configuration

Figure 8 Traversal Zone Search Rule on VCS Control

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	★ Traversal zone search rule	
Description	Search traversal zone - VCSe	
Priority	★ 100	
Protocol	Any	
Source	Any	
Request must be authenticated	No	
Mode	Any alias	
On successful match	Continue	
Target	★ TraversalZone	
State	Enabled	

Figure 9 Traversal Zone Search Rule on VCS Expressway

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	★ Traversal zone search rule	
Description	Search traversal zone - VCSc	
Priority	★ 100	
Protocol	Any	
Source	Any	
Request must be authenticated	No	
Mode	Any alias	
On successful match	Continue	
Target	★ TraversalZone	
State	Enabled	

Task 12: Configuring the DNS Zone

The DNS zone is used to search for externally hosted systems (such as for business to business calling). Destination aliases are searched for by a name using a DNS lookup.

To configure the DNS zone:

1. Sign in to the VCS Expressway.
2. Go to **Configuration > Zones > Zones**.
3. Click **New**.
4. Configure the fields as follows (leave all other fields with default values):

Field name	Value
Name	Enter <code>DNSZone</code> for example
Type	<i>DNS</i>
H.323 Mode	<i>On</i>
SIP Mode	<i>On</i>
Fallback transport protocol	<i>TCP</i>
Include address record	<i>Off</i>

5. Click **Create zone**.

Task 13: Configuring DNS Zone Search Rules

The DNS search rule defines when the DNS zone should be searched.

A specific regular expression is configured which will prevent searches being made using the DNS zone (i.e. on the public internet) for destination addresses (URLs) using any SIP domains which are configured on the local network (local domains).

To create the search rules to route via DNS:

1. Sign in to the VCS Expressway.
2. Go to **Configuration > Dial plan > Search rules**.
3. Click **New**.

Routing Configuration

4. Configure the fields as follows:

Field name	Value
Rule name	Enter DNS zone search rule for example
Description	Enter Search DNS zone (external calling) for example
Priority	150
Protocol	Any
Source	All zones
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	Enter (?!.*@example\.com.*\$).*
Pattern behavior	Leave
On successful match	Continue
Target	DNSZone
State	Enabled

5. Click **Create search rule**.

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	★ DNS zone search rule ⓘ
Description	Search DNS zone (external calling) ⓘ
Priority	★ 150 ⓘ
Protocol	Any ⓘ
Source	AllZones ⓘ
Request must be authenticated	No ⓘ
Mode	Alias pattern match ⓘ
Pattern type	Regex ⓘ
Pattern string	★ (?!.*@%localdomains%.*\$).* ⓘ
Pattern behavior	Leave ⓘ
On successful match	Continue ⓘ
Target	★ DNSZone ⓘ
State	Enabled ⓘ

Note that the regular expression used to prevent local domains being searched via the DNS zone can be broken down into the following components:

Routing Configuration

(.*) = match all pattern strings

(?!.*@example\.com.*\$).* = do not match any pattern strings ending in @example.com

In the deployment example, calls destined for @cisco.com would be searched via the DNS zone, whereas calls destined for @example.com would not.

Task 14: Configuring External (Unknown) IP Address Routing

The following configuration defines how a VCS routes calls (and other requests) to external IP addresses. An external IP address is an IP address which is not 'known' to the VCS and therefore assumed to be a publicly routable address.

Known IP addresses are addresses defined in a subzone (using a subzone membership subnet rule) or the IP address of an H.323 registered device.

- All requests destined for external IP addresses, originating at the VCS Control are routed to the VCS Expressway using a search rule.
- The VCS Expressway then attempts to open a connection directly to the IP address.

To configure how the VCS handles calls to unknown IP addresses:

1. Go to **Configuration > Dial plan > Configuration**.
2. Configure the fields as follows:

	VCS Control	VCS Expressway
Calls to unknown IP addresses	<i>Indirect</i>	<i>Direct</i>

VCS Control

Dial plan configuration You are here: [Configuration](#) > [Dial plan](#) > Configuration

Configuration

Calls to unknown IP addresses Indirect i

Fallback alias i

Save

VCS Expressway

Dial plan configuration You are here: [Configuration](#) > [Dial plan](#) > Configuration

Configuration

Calls to unknown IP addresses Direct i

Fallback alias i

Save

3. Click **Save**.

To create the search rules to route calls to IP addresses to the VCS Expressway:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

Routing Configuration

3. Configure the fields as follows:

	VCS Control	VCS Expressway
Rule name	Enter External IP address search rule	Not applicable
Description	Enter Route external IP address	Not applicable
Priority	Enter 100	Not applicable
Protocol	Any	Not applicable
Source	Any	Not applicable
Request must be authenticated	No	Not applicable
Mode	Any IP address	Not applicable
On successful match	Continue	Not applicable
Target	TraversalZone	Not applicable
State	Enabled	Not applicable

4. Click **Create search rule**.

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	★ External IP address search rule ⓘ
Description	Route external IP address ⓘ
Priority	★ 100 ⓘ
Protocol	Any ⓘ
Source	Any ⓘ
Request must be authenticated	No ⓘ
Mode	Any IP address ⓘ
On successful match	Continue ⓘ
Target	★ TraversalZone ⓘ
State	Enabled ⓘ

Endpoint Registration

The example network configuration diagram shows three endpoints.

Endpoint	IP address	Network
EX90	10.0.0.15	Internal network
EX60	10.0.0.16	Internal network
EX60	192.168.0.2	Home user network

After system configuration, endpoint registration should be possible using these endpoint configuration details:

EX90 (uses SIP protocol)	
SIP URI	user.one.ex90@example.com
SIP Proxy1	vcsc.internal-domain.net
EX60 (uses H.323 and SIP protocol)	
H.323 ID	user.two.mxp@example.com
H.323 E.164	7654321
Gatekeeper IP Address	vcsc.internal-domain.net
SIP URI	user.two.mxp@example.com
SIP Proxy1	vcsc.internal-domain.net
EX60 at home (uses H.323 and SIP protocol)	
H.323 ID	user.three.mxp@example.com
H.323 E.164	1234567
Gatekeeper IP Address	vcse.example.com
SIP URI	user.three.mxp@example.com
SIP Proxy1	vcse.example.com

What To Do Next

The VCS routing configuration is now complete. Go to the next section, "*System Checks*."

System Checks

Zone Status

Go to **Status > Zones** on both VCS Control and VCS Expressway to check that the traversal zone is **Active**. You can also check the zone status in **Configuration > Zones > Zones**.

If the traversal zone is not active, do the following:

- Review the traversal zone configuration.
- Check that the relevant ports are enabled for outbound routing on the NAT and firewall devices located between the VCS Control and VCS Expressway. See [Appendix 3: Firewall and NAT Settings, page 59](#).
- Check that the username and password credentials are configured correctly (and match) on VCS Control and VCS Expressway traversal zones and in the authentication database on the VCS Expressway.

Registration Status

Check that all endpoints which are expected to be registered are actually registered to the relevant VCS. And that they are registering the expected aliases. All successfully registered endpoints are listed on **Status > Registrations > By device**.

If the expected endpoints are not registered, review the following items:

- The endpoint's registration configuration. Is it configured to register with the VCS Expressway if located on the external network / internet, and to register with the VCS Control if located on the internal network?
- The SIP domains ([Task 7: Configuring SIP Domains, page 23](#)).
- Any registration restriction configuration applied to the VCS (optional, [Task 17: Configuring Registration Restriction Policy \(Optional\), page 44](#)).

In some cases, home endpoints may fail to register when using SRV records. This can happen if the endpoint uses the home router for its DNS server, and the router's DNS server software doesn't support SRV records lookup. (Also applies to the DNS server being used by a PC when Jabber Video is running on it.) If registration failure occurs, do either of the following:

- Change the DNS server on the endpoint to use a publicly available DNS server which can resolve SRV record lookups. For example, Google – 8.8.8.8
- Change the SIP/H.323 server address on the endpoint to use the FQDN of a node in the VCS cluster and not the cluster SRV record. So that the device performs an AAAA or A record lookup.

Call Signaling

If calls do not complete, despite the endpoints being successfully registered to a VCS:

- Review the VCS Control search rule configuration.
- Review the VCS Expressway search rule configuration.
- Check the search history page for search attempts and failures (**Status > Search history**).
- Check the Event Log for call connection failure reasons (**Status > Logs > Event Log**).

What To Do Next

When you've completed the system checks and are satisfied that the system is working as expected, [create a system backup](#) and then go on to "[Optional Configuration Tasks](#)".

Maintenance Routine

Creating a System Backup

To create a backup of VCS system data:

1. Go to **Maintenance > Backup and restore**.
2. Optionally, enter an **Encryption password** with which to encrypt the backup file.
If a password is specified, the same password will be required to restore the file.
3. Click **Create system backup file**.
4. After the backup file has been prepared, a pop-up window appears and prompts you to save the file (the exact wording depends on your browser). The default name is in the format:
<software version>_<hardware serial number>_<date>_<time>_backup.tar.gz.
(The file extension is normally **.tar.gz.enc** if an encryption password is specified. However, if you use Internet Explorer to create an encrypted backup file, the filename extension will be **.tar.gz.gz** by default. These different filename extensions have no operational impact; you can create and restore encrypted backup files using any supported browser.)
The preparation of the system backup file may take several minutes. Do not navigate away from this page while the file is being prepared.
5. Save the file to a designated location.

Log files are not included in the system backup file.

Optional Configuration Tasks

Task 15: Configuring Cisco TMS (Optional)

The following configuration enables the VCS system to be integrated to a Cisco TelePresence Management Suite (Cisco TMS).

Points to note:

- Further configuration tasks are also required on Cisco TMS to fully integrate the VCS with the TMS server. For details, see *Cisco TMS Administrator Guide* on the [TMS Maintain and Operate Guides page](#).
- Enabling SNMP speeds up the VCS - TMS integration process, but is not essential.
- VCS Expressway integration with TMS requires additional firewall / NAT configuration. VCS Expressway needs to access port 80/443 on Cisco TMS from outside the firewall. See [Appendix 3: Firewall and NAT Settings, page 59](#).

To enable and configure SNMP:

1. Go to **System > SNMP**.
2. Configure the SNMP fields as follows:

	VCS Control	VCS Expressway
SNMP mode	<i>v3 plus TMS support</i>	Same as VCS Control
Community name	Check that it is <code>public</code>	
System contact	Enter <code>IT administrator</code>	
Location	Enter <code>example.com head office</code>	
Username	Enter <code>vcs</code>	
Authentication mode	<i>On</i>	
Type	<i>SHA</i>	
Password	Enter <code>ex4mpl3.c0m</code>	
Privacy mode	<i>On</i>	
Type	<i>AES</i>	
Password	Enter <code>ex4mpl3.c0m</code>	

3. Click **Save**.

Optional Configuration Tasks

SNMP You are here: [System](#) > [SNMP](#)

Configuration

SNMP mode: v3 plus TMS support ⓘ

Community name: public ⓘ

System contact: IT administrator ⓘ

Location: example.com head office ⓘ

Username: VCS ⓘ

Authentication

Authentication mode: On ⓘ

Type: SHA ⓘ

Password: ⓘ

Privacy

Privacy mode: On ⓘ

Type: AES ⓘ

Password: ⓘ

To configure the necessary external manager (Cisco TMS) parameters:

1. Go to **System > External manager**.
2. Configure the fields as follows:

	VCS Control	VCS Expressway
Address	Enter 10.0.0.14	Same as VCS Control
Path	Enter tms/public/external/management/SystemManagementService.asmx	
Protocol	Select <i>HTTP</i> or <i>HTTPS</i>	
Certificate verification mode	Select <i>On</i> or <i>Off</i> The certificate is only verified if the value is <i>On</i> and the protocol is set to <i>HTTPS</i> . If you switch this on then Cisco TMS and VCS must have appropriate certificates.	

3. Click **Save**.

Optional Configuration Tasks

External manager You are here: [System](#) > External manager

Configuration

Address	<input type="text" value="10.0.0.14"/>	
Path	<input type="text" value="tms/public/external/management/SystemManagementService.asmx"/>	
Protocol	<input type="text" value="HTTP"/>	
Certificate verification mode	<input type="text" value="On"/>	

Task 16: Configuring Logging (Optional)

The following configuration enables event logs to be sent to an external logging server using the SYSLOG protocol.

- The **Local event log verbosity** setting controls the granularity of event logging. 1 is the least verbose, 4 the most.
- We recommend a minimum level of 2. This provides both system and basic signaling message logging.

The VCS Expressway needs further firewall / NAT configuration for external logging. See [Appendix 3: Firewall and NAT Settings](#), page 59 for details.

To configure a logging server:

1. Go to **Maintenance > Logging**.
2. Configure the fields as follows:

	VCS Control	VCS Expressway
Local event log verbosity	2	2
Remote syslog server 1: Address	Enter 10.0.0.13	Enter 10.0.0.13
Remote syslog server 1: Message Format	<i>IETF syslog format</i>	<i>IETF syslog format</i>

3. Click **Save**.

Task 17: Configuring Registration Restriction Policy (Optional)

You can limit the aliases that endpoints can register, using either an Allow list or a Deny list. This is an example of how to configure Allow list registration restrictions:

1. Go to **Configuration > Registration > Allow List**.
2. Click **New**.
3. Create an allow pattern by configuring the following fields. This example limits registrations to endpoints which register with an identity that contains “@example.com”.

	VCS Control	VCS Expressway
Description	Enter Only allow registrations containing “@example.com”	Same as VCS Control
Pattern type	<i>Regex</i>	
Pattern string	Enter <code>.*@example\.com</code>	

Optional Configuration Tasks

4. Click **Add Allow List pattern**.

Create allow pattern You are here: [Configuration](#) > [Registration](#) > [Allow List](#) > Create allow pattern

Configuration

Description: only allow registrations containing "@example.com" ⓘ

Pattern type: **Regex** ⓘ

Pattern string: ***.example.com** ⓘ

Add Allow List pattern **Cancel**

To activate the registration restriction:

1. Go to **Configuration > Registration > Configuration**.
2. Configure the **Restriction policy** as follows:

	VCS Control	VCS Expressway
Restriction policy	<i>Allow List</i>	<i>Allow List</i>

3. Click **Save**.

Registration configuration You are here: [Configuration](#) > [Registration](#) > Configuration

Configuration

Restriction policy: **Allow List** ⓘ

Save

Task 18: Configuring Device Authentication Policy (Optional)

Authentication policy is applied by the VCS at the zone and subzone levels. It controls how the VCS challenges incoming messages (for provisioning, registration, presence, phone books, and calls) from that zone or subzone and whether those messages are rejected, treated as authenticated, or treated as unauthenticated within the VCS.

Each zone and subzone can set its **Authentication policy** to *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone configuration (or the relevant alternative subzone).
- Initial provisioning subscription request authentication is controlled by the Default Zone configuration.
- Call, presence, and phone book request authentication is controlled by the Default Subzone (or relevant alternative subzone) if the endpoint is registered, or by the Default Zone if the endpoint is not registered.

By default, zones and subzones are configured as *Do not check credentials*.

Using Delegated Credential Checking

If you have enabled device authentication in your network (by using an **Authentication policy** of *Check credentials*) and you have remote workers (outside the enterprise) with SIP devices, you should consider enabling delegated credential checking. In summary, this would require you to:

Optional Configuration Tasks

- Set up a secure traversal zone between the VCS Expressway and the VCS Control.
- Enable the VCS Expressway and the VCS Control's SIP settings, traversal zones and required SIP domains for delegated credential checking.
- Configure the VCS Control with the relevant authentication mechanisms.

This means that remote workers can now register to the VCS Expressway (assuming it has its **SIP registration proxy mode** set to *Off*) and be authenticated securely via the VCS Control against an authentication mechanism inside the enterprise.

See [Device Authentication on VCS Deployment Guide](#) for full information on configuring device authentication and delegated credential checking.

Task 19: Restricting Access to ISDN Gateways (Optional)

We recommend that you restrict unauthorized access to any ISDN gateway resources (also known as toll-fraud prevention). Some methods to achieve this are described here.

In these examples, an ISDN gateway is registered to the VCS Control with a prefix of 9. And / or it has a neighbor zone specified that routes calls starting with a 9.

VCS Expressway

Two search rules are created on the VCS Expressway:

- Both rules have a pattern string that matches calls directed at the ISDN gateway. (In this example calls prefixed with a 9.)
- The first rule has a **Source** of *All zones*. This allows calls from registered endpoints and neighbor zones to pass through to the traversal zone.
- The second rule is similar to the first rule but has a **Source** of *All*. So it includes nonregistered endpoints (which are excluded from the previous rule). They can be stopped by defining the **Replace string** as "do-not-route-this-call."
- Both rules stop any further search rules from being looked at (**On successful match** = *Stop*).

To create the search rules:

1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.

Optional Configuration Tasks

3. Configure the fields as follows:

	VCS Expressway
Rule name	Enter <code>Allow ISDN call</code> for example
Description	Enter <code>Allow ISDN calls for registered devices and neighbors</code>
Priority	Enter 40 (these rules must be the highest priority in the search rule configuration)
Protocol	<i>Any</i>
Source	<i>All zones</i>
Request must be authenticated	<i>No</i>
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	Enter <code>(9\d+) (@example.com)</code>
Pattern behavior	<i>Replace</i>
Replace string	Enter <code>\1</code>
On successful match	<i>Stop</i>
Target	<i>TraversalZone</i>
State	<i>Enabled</i>

Optional Configuration Tasks

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	<input type="text" value="Allow ISDN call"/>	
Description	<input type="text"/>	
Priority	<input type="text" value="40"/>	
Protocol	<input type="text" value="Any"/>	
Source	<input type="text" value="AllZones"/>	
Request must be authenticated	<input type="text" value="No"/>	
Mode	<input type="text" value="Alias pattern match"/>	
Pattern type	<input type="text" value="Regex"/>	
Pattern string	<input type="text" value="(9\d+)(@example.com)"/>	
Pattern behavior	<input type="text" value="Replace"/>	
Replace string	<input type="text" value="\1"/>	
On successful match	<input type="text" value="Stop"/>	
Target	<input type="text" value="TraversalZone"/>	
State	<input type="text" value="Enabled"/>	

4. Click **Create search rule**.
5. Click **New**.

Optional Configuration Tasks

6. Configure the fields as follows:

	VCS Expressway
Rule name	Enter <code>Block ISDN call</code> for example
Description	Enter <code>Blocks everything (including nonregistered endpoints)</code>
Priority	Enter <code>41</code>
Protocol	<i>Any</i>
Source	<i>Any</i>
Request must be authenticated	<i>No</i>
Mode	<i>Alias pattern match</i>
Pattern type	<i>Regex</i>
Pattern string	Enter <code>(9\d+) (.*) (@example.com)</code>
Pattern behavior	<i>Replace</i>
Replace string	Enter <code>do-not-route-this-call</code> for example
On successful match	<i>Stop</i>
Target	<i>TraversalZone</i>
State	<i>Enabled</i>

Optional Configuration Tasks

Create search rule You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#) > Create search rule

Configuration

Rule name	* Block ISDN call i
Description	Blocks everything, including non-registered endpoints i
Priority	* 41 i
Protocol	Any i
Source	Any i
Request must be authenticated	No i
Mode	Alias pattern match i
Pattern type	Regex i
Pattern string	* (9\d+)(.*)(@example.com) i
Pattern behavior	Replace i
Replace string	do-not-route-this-call i
On successful match	Stop i
Target	* TraversalZone i
State	Enabled i

[Create search rule](#) [Cancel](#)

7. Click **Create search rule**.

Search rules You are here: [Configuration](#) > [Dial plan](#) > [Search rules](#)

Priority	State	Rule name	Protocol	Source	Authentication required	Mode	Pattern type	Pattern string	Pattern behavior	On match	Target	Actions
<input type="checkbox"/> 40	✓ Enabled	Allow ISDN call	Any	AllZones	No	Alias pattern match	Regex	(9\d+)(.*)(@example.com)	Replace	Stop	TraversalZone	View/Edit
<input type="checkbox"/> 41	✓ Enabled	Block ISDN call	Any	Any	No	Alias pattern match	Regex	(9\d+)(.*)(@example.com)	Replace	Stop	TraversalZone	View/Edit
<input type="checkbox"/> 50	✓ Enabled	LocalZoneMatch	Any	Any	No	Any alias				Continue	LocalZone	View/Edit

VCS Control

This example describes how to configure the VCS Control to stop calls that come in through the gateway, from being able to route calls back out of the gateway.

To do this, you load some specially constructed CPL onto the VCS Control and configure its **Call policy mode** to use *Local CPL*.

Creating a CPL File

The CPL file can be created in a text editor.

Here are two example sets of CPL. In these examples:

- “GatewayZone” is the neighbor zone to the ISDN gateway.
- “GatewaySubZone” is the subzone to the ISDN gateway (required if the gateway registers the 9 prefix to the VCS).
- Calls coming into the ISDN gateway and hitting a FindMe do not ring devices that use the gateway. So for example, calls forwarded to a mobile phone are disallowed.

This example CPL excludes any checking of whether the calling party is authenticated:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:tta="http://www.tandberg.net/cpl-extensions"
```

Optional Configuration Tasks

```

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!--Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not send calls back out of this gateway -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" destination="9.*">
      <!-- Calls coming from the gateway may not send calls back out of this gateway -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>

```

This example CPL also ensures that the calling party is authenticated:

```

<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!-- Check that calling party is authenticated -->
    <taa:rule authenticated-origin="" destination="9.*">
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN call denied as unauthenticated caller"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Neighbor zone -->
    <taa:rule originating-zone="GatewayZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <!-- Check that gateway is not hairpinning call - Subzone for registered gateway -->
    <taa:rule originating-zone="GatewaySubZone" destination="9.*">
      <!-- Calls coming from the gateway may not hairpin and send calls back out -->
      <!-- Reject call with a status code of 403 (Forbidden) -->
      <reject status="403" reason="ISDN hairpin call denied"/>
    </taa:rule>
    <taa:rule origin=".*" destination=".*">
      <!-- All other calls allowed -->
      <proxy/>
    </taa:rule>
  </taa:rule-switch>
</taa:routed>
</cpl>

```

Loading the CPL onto VCS Control


To configure the VCS Control to use the CPL:

Optional Configuration Tasks

1. Go to **Configuration > Call Policy > Configuration**.
2. Click **Browse....** Select the CPL file you created in the previous step from your file system.
3. Click **Upload file**.
 - If the file upload succeeds, you see a "File upload successful" message.
 - If you receive an "XML invalid" message, correct the problems with the CPL file and upload it again.
4. Select a **Call policy mode** of *Local CPL*.
5. Click **Save**.





Call Policy configuration You are here: [Configuration](#) > [Call Policy](#) > Configuration

Configuration

Call Policy mode Local CPL 

Save

Policy files

Call policy file	CPL File	Show Call Policy file	
CPL XSD file	XSD File	Show CPL XSD file	
CPL extensions xsd file	XSD File	Show CPL extensions XSD file	
Select the new Call Policy file	<input type="text"/>	Browse...	

Upload file

Appendix 1: Configuration Details

This appendix summarizes the configuration required for the VCS Control and VCS Expressway. It is broken down into 3 sections:

- VCS Control (configuration to apply to the VCS Control only)
- VCS Expressway (configuration to apply to the VCS Expressway only)
- VCS Control and VCS Expressway (configuration to apply to both the VCS Control and VCS Expressway)

VCS Control Configuration Details

Configuration item	Value	VCS page
System configuration		
System name	VCS	System > Administration
LAN1 IPv4 address	10.0.0.2	System > Network interfaces > IP
IPv4 gateway	10.0.0.1	System > Network interfaces > IP
LAN1 subnet mask	255.255.255.0	System > Network interfaces > IP
DNS server address 1	10.0.0.11	System > DNS
DNS server address 2	10.0.0.12	System > DNS
DNS Domain name	internal-domain.net	System > DNS
DNS System host name	vcsc	System > DNS
NTP server 1	pool.ntp.org	System > Time
Time zone	GMT	System > Time
Protocol configuration		
SIP domain name	example.com	Configuration > Domains
Traversal zone		
Zone Name	TraversalZone	Configuration > Zones > Zones
Zone Type	Traversal client	Configuration > Zones > Zones
Protocol SIP port	7001	Configuration > Zones > Zones
Protocol H.323 port	6001	Configuration > Zones > Zones
Location Peer 1 address	192.0.2.2	Configuration > Zones > Zones
Authentication username	exampleauth	Configuration > Zones > Zones
Authentication password	ex4mpl3.c0m	Configuration > Authentication > Devices > Local database
Traversal search rule		
Rule name	Traversal zone search rule	Configuration > Dial plan > Search rules
Description	Search traversal zone (VCS Control)	Configuration > Dial plan > Search rules

Appendix 1: Configuration Details

Configuration item	Value	VCS page
Priority	100	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Any alias	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	TraversalZone	Configuration > Dial plan > Search rules
Direct IP search rule		
Rule name	External IP address search rule	Configuration > Dial plan > Search rules
Description	Route external IP address	Configuration > Dial plan > Search rules
Priority	100	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Any IP address	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	TraversalZone	Configuration > Dial plan > Search rules
IP call routing		
Calls to unknown IP addresses	Indirect	Configuration > Dial plan > Configuration

VCS Expressway Configuration Details

Configuration item	Value	VCS page
System configuration		
System name	VCSe	System > Administration
LAN1 IPv4 address	192.0.2.2	System > Network interfaces > IP
IPv4 gateway	192.0.2.1	System > Network interfaces > IP
LAN1 subnet mask	255.255.255.0	System > Network interfaces > IP
DNS server address 1	194.72.6.57	System > DNS
DNS server address 2	194.73.82.242	System > DNS
DNS Domain name	example.com	System > DNS
DNS System host name	vcse	System > DNS
NTP server 1	pool.ntp.org	System > Time
Time zone	GMT	System > Time
Protocol configuration		
SIP domain name	example.com	Configuration > Domains
Traversal zone		

Appendix 1: Configuration Details

Configuration item	Value	VCS page
Zone Name	TraversalZone	Configuration > Zones > Zones
Zone Type	Traversal server	Configuration > Zones > Zones
Client authentication username	exampleauth	Configuration > Zones > Zones
Protocol SIP port	7001	Configuration > Zones > Zones
Protocol H.323 port	6001	Configuration > Zones > Zones
Name	exampleauth	Configuration > Authentication > Devices > Local database
Password	ex4mpl3.c0m	Configuration > Authentication > Devices > Local database
Traversal zone search rule		
Rule name	Traversal zone search rule	Configuration > Dial plan > Search rules
Description	Search traversal zone (VCS Expressway)	Configuration > Dial plan > Search rules
Priority	100	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Any alias	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	TraversalZone	Configuration > Dial plan > Search rules
DNS zone		
Zone Name	DNSZone	Configuration > Zones
Zone Type	DNS	Configuration > Zones > Zones
DNS zone search rule		
Rule name	DNS zone search rule	Configuration > Dial plan > Search rules
Zone name	Search DNS zone (external DNS)	Configuration > Dial plan > Search rules
Priority	150	Configuration > Dial plan > Search rules
Source	All zones	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(?!.*@example\.com.*\$).*	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	DNSZone	Configuration > Dial plan > Search rules
IP call routing		
Calls to unknown IP addresses	Direct	Configuration > Dial plan > Configuration

Appendix 1: Configuration Details

VCS Control and VCS Expressway Configuration Details

Configuration item	Value	VCS page
Transform		
Pattern string	([^\@]*)	Configuration > Dial plan > Transforms
Pattern type	Regex	Configuration > Dial plan > Transforms
Pattern behavior	Replace	Configuration > Dial plan > Transforms
Replace string	\1@example.com	Configuration > Dial plan > Transforms
Local search rule 1		
Rule name	Local zone - no domain	Configuration > Dial plan > Search rules
Priority	48	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+)@example\.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Replace	Configuration > Dial plan > Search rules
Replace string	\1	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules
Local search rule 2		
Rule name	Local zone - full URI	Configuration > Dial plan > Search rules
Priority	50	Configuration > Dial plan > Search rules
Source	Any	Configuration > Dial plan > Search rules
Mode	Alias pattern match	Configuration > Dial plan > Search rules
Pattern type	Regex	Configuration > Dial plan > Search rules
Pattern string	(.+)@example\.com.*	Configuration > Dial plan > Search rules
Pattern behavior	Leave	Configuration > Dial plan > Search rules
On successful match	Continue	Configuration > Dial plan > Search rules
Target	LocalZone	Configuration > Dial plan > Search rules

Appendix 2: DNS Records

DNS Configuration on Host Server

The following records are required in the external DNS which hosts the externally routable domain (*example.com*). This allows:

- External endpoints registration messages to be routed to the VCS Expressway.
- Calls from non-registered endpoints (or other infrastructure devices) to be routed to the VCS Expressway.

Host DNS A Record

Host	Host IP address
vcse.example.com	192.0.2.2

DNS SRV Records

Name	Service	Protocol	Priority	Weight	Port	Target host
example.com.	h323cs	tcp	10	10	1720	vcse.example.com.
example.com.	h323ls	udp	10	10	1719	vcse.example.com.
example.com.	h323rs	udp	10	10	1719	vcse.example.com.
example.com.	sip	tcp	10	10	5060	vcse.example.com.
example.com.	sip	udp *	10	10	5060	vcse.example.com.
example.com.	sips	tcp	10	10	5061	vcse.example.com.
example.com.	turn	udp	10	10	3478 **	vcse.example.com.

* SIP UDP is disabled on VCS by default.

** On Large VCS deployments you should configure multiple records for the range 3478 – 3483.

For example, the DNS records would be:

```
_h323cs._tcp.example.com. 86400 IN SRV 10 10 1720 vcse.example.com.
_h323ls._udp.example.com. 86400 IN SRV 10 10 1719 vcse.example.com.
_h323rs._udp.example.com. 86400 IN SRV 10 10 1719 vcse.example.com.
_sip._tcp.example.com.    86400 IN SRV 10 10 5060 vcse.example.com.
_sip._udp.example.com.    86400 IN SRV 10 10 5060 vcse.example.com.
_sips._tcp.example.com.   86400 IN SRV 10 10 5061 vcse.example.com.
_turn._udp.example.com.   86400 IN SRV 10 10 3478 vcse.example.com.
vcse.example.com.         86400 IN A 192.0.2.2
```

If you have a cluster of VCS Expressways, you must set up DNS A and SRV records for each peer/host in the cluster. See [VCS Cluster Creation and Maintenance Deployment Guide](#) for more information.

DNS Configuration (internal DNS server)

The following records are required in the local DNS which hosts the internally routable domain: internal-domain.net to allow internal messages to be routed to the VCS Control.

Appendix 2: DNS Records

Local DNS A Record

Host	Host IP address
vcsc.internal-domain.net	10.0.0.2

Local DNS SRV Records

Name	Service	Protocol	Priority	Weight	Port	Target host
internal-domain.net.	h323cs	tcp	10	10	1720	vcsc.internal-domain.net.
internal-domain.net.	h323ls	udp	10	10	1719	vcsc.internal-domain.net.
internal-domain.net.	h323rs	udp	10	10	1719	vcsc.internal-domain.net.
internal-domain.net.	sip	tcp	10	10	5060	vcsc.internal-domain.net.
internal-domain.net.	sip	udp *	10	10	5060	vcsc.internal-domain.net.
internal-domain.net.	sips	tcp	10	10	5061	vcsc.internal-domain.net.

* SIP UDP is disabled on VCS by default.

For example, the DNS records would be:

```
_h323cs._tcp.internal-domain.net. 86400 IN SRV 10 10 1720 vcsc.internal-domain.net.
_h323ls._udp.internal-domain.net. 86400 IN SRV 10 10 1719 vcsc.internal-domain.net.
_h323rs._udp.internal-domain.net. 86400 IN SRV 10 10 1719 vcsc.internal-domain.net.
_sip._tcp.internal-domain.net.      86400 IN SRV 10 10 5060 vcsc.internal-domain.net.
_sip._udp.internal-domain.net.      86400 IN SRV 10 10 5060 vcsc.internal-domain.net.
_sips._tcp.internal-domain.net.     86400 IN SRV 10 10 5061 vcsc.internal-domain.net.
vcsc.internal-domain.net.           86400 IN A 10.0.0.2
```

If you have a cluster of VCS Controls, you must set up DNS A and SRV records for each peer/host in the cluster. See *VCS Cluster Creation and Maintenance Deployment Guide* for more information.

Appendix 3: Firewall and NAT Settings

Internal Firewall Configuration

In many deployments outbound connections (from internal network to DMZ) will be permitted by the NAT/firewall device. If the administrator wants to restrict this further, the following tables provide the permissive rules required. For further information, see [VCS IP Port Usage for Firewall Traversal](#).

Ensure that any SIP or H.323 'fixup' ALG or awareness functionality is disabled on the NAT firewall – if enabled this will adversely interfere with the VCS functionality.

Outbound (Internal Network > DMZ)

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
Management	Management computer	VCSe	As required	>=1024	TCP	192.0.2.2	80 / 443 / 22 / 23
SNMP monitoring	Management computer	VCSe	As required	>=1024	UDP	192.0.2.2	161
H.323 traversal calls using Assent							
RAS Assent	VCSc	VCSe	Any	1719	UDP	192.0.2.2	6001
Q.931/H.225 and H.245	VCSc	VCSe	Any	15000 to 19999	TCP	192.0.2.2	2776
RTP Assent	VCSc	VCSe	Any	36002 to 59999 *	UDP	192.0.2.2	36000 *
RTCP Assent	VCSc	VCSe	Any	36002 to 59999 *	UDP	192.0.2.2	36001 *
SIP traversal calls							
SIP TCP/TLS	VCSc	VCSe	10.0.0.2	25000 to 29999	TCP	192.0.2.2	Traversal zone ports, e.g. 7001
RTP Assent	VCSc	VCSe	10.0.0.2	36002 to 59999 *	UDP	192.0.2.2	36000 *
RTCP Assent	VCSc	VCSe	10.0.0.2	36002 to 59999 *	UDP	192.0.2.2	36001 *
When ICE is enabled on VCS Control zones and the VCS Expressway is used as the TURN server							
TURN server control	VCSc	VCSe	Any	>=1024	UDP	192.0.2.2	3478 **
TURN server media	VCSc	VCSe	Any	>=1024	UDP	192.0.2.2	24000 to 29999 **

* On new installations of X8.1 or later, the default media traversal port range is 36000 to 59999, and is set on the VCS Control (**Configuration > Local Zones > Traversal Subzone**). In Large VCS Expressway systems the first 12 ports in the range – 36000 to 36011 by default – are always reserved for multiplexed traffic. The VCS Expressway listens on these ports. You cannot configure a distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the VCS Expressway (**Configuration > Traversal > Ports**). On upgrades to X8.2 or later, the VCS Control retains the media traversal port range from the previous version (could be 50000 – 54999 or

Appendix 3: Firewall and NAT Settings

36000 - 59999, depending on source version). The VCS Expressway retains the previously configured demultiplexing pair (either 2776 & 2777 or 50000 & 50001 by default, depending on upgrade path) and the switch **Use configured demultiplexing ports** is set to Yes. If you do not want to use a particular pair of ports, switch **Use configured demultiplexing ports** to No, then the VCS Expressway will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default). In this case, we recommend that you close the previously configured ports after you configure the firewall for the new ports.

Inbound (DMZ > Internal network)

As VCS Control to VCS Expressway communications are always initiated from the VCS Control to the VCS Expressway (VCS Expressway sending messages by responding to VCS Control's messages) no ports need to be opened from DMZ to Internal for call handling.

However, if the VCS Expressway needs to communicate with local services, such as a Syslog server, some of the following NAT configurations may be required:

Purpose	Source	Destination	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
Logging	VCSe	Syslog server	192.0.2.2	30000 to 35999	UDP	10.0.0.13	514
Management	VCSe	Cisco TMS server	192.0.2.2	>=1024	TCP	10.0.0.14	80 / 443
LDAP (for log in, if required)	VCSe	LDAP server	192.0.2.2	30000 to 35999	TCP		389 / 636
NTP (time sync)	VCSe	Local NTP server	192.0.2.2	123	UDP		123
DNS	VCSe	Local DNS server	192.0.2.2	>=1024	UDP		53

Traffic destined for logging or management server addresses (using specific destination ports) must be routed to the internal network.

External Firewall Configuration Requirement

In this example it is assumed that outbound connections (from DMZ to external network) are all permitted by the firewall device.

Ensure that any SIP or H.323 "fixup" ALG or awareness functionality is disabled on the NAT firewall - if enabled this will adversely interfere with the VCS functionality.

Inbound (Internet > DMZ)

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
H.323 endpoints registering with Assent							
RAS Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	1719
Q.931/H.225 and H.245	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	2776
RTP Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	36000
RTCP Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	36001

Appendix 3: Firewall and NAT Settings

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
H.323 endpoints registering with public IP addresses							
RAS	Endpoint	VCSe	Any	1719	UDP	192.0.2.2	1719
Q.931/H.225	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	1720
H.245	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	15000 to 19999
RTP & RTCP	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	36002 to 59999
SIP endpoints registering using UDP / TCP or TLS							
SIP TCP	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	5060
SIP UDP	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	5060
SIP TLS	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	5061
RTP & RTCP	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	36002 to 59999
TURN server control	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	3478 **
TURN server media	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	24000 to 29999 **

** On Large systems you can configure a range of TURN request listening ports. The default range is 3478 – 3483. The default TURN relay media port range of 24000 – 29999 applies to new installations of X8.1 or later. The previous default range of 60000 – 61799 still applies to earlier releases that have upgraded to X8.1.

Outbound (DMZ > Internet)

If you want to restrict communications from the DMZ to the wider Internet, the following table provides information on the outgoing IP addresses and ports required to permit the VCS Expressway to provide service to external endpoints.

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
H.323 endpoints registering with public IP address							
RAS	VCSe	Endpoint	192.0.2.2	>=1024	UDP	Any	1719
Q.931/H.225	VCSe	Endpoint	192.0.2.2	15000 to 19999	TCP	Any	1720
H.245	VCSe	Endpoint	192.0.2.2	15000 to 19999	TCP	Any	>=1024
RTP & RTCP	VCSe	Endpoint	192.0.2.2	36000 to 59999	UDP	Any	>=1024
SIP endpoints registering using UDP / TCP or TLS							
SIP TCP & TLS	VCSe	Endpoint	192.0.2.2	25000 to 29999	TCP	Any	>=1024
SIP UDP	VCSe	Endpoint	192.0.2.2	5060	UDP	Any	>=1024
RTP & RTCP	VCSe	Endpoint	192.0.2.2	36000 to 59999	UDP	Any	>=1024
TURN server media	VCSe	Endpoint	192.0.2.2	24000 to 29999 **	UDP	Any	>=1024
Other services (as required)							

Appendix 3: Firewall and NAT Settings

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
DNS	VCSe	DNS server	192.0.2.2	>=1024	UDP	DNS servers	53
NTP (time sync)	VCSe	NTP server	192.0.2.2	123	UDP	NTP servers	123

It is assumed that remote H.323 devices are registering using the Assent protocol. If the devices are registering using H.460 18/19, see *VCS IP Port Usage for Firewall Traversal Deployment Guide* or *VCS Administrator Guide* for port usage information.

Appendix 4: Advanced Network Deployments

Prerequisites

- Apply an **Advanced Networking** option key on any VCS Expressway that needs static NAT or two LAN interfaces.
The **Advanced Networking** option is available for both the VCS Expressway and VCS Control, but only the VCS Expressway supports static NAT.
- Disable SIP and H.323 ALGs (SIP / H.323 awareness) on routers/firewalls carrying network traffic to or from the VCS Expressway. We do not support this functionality on the firewall/s when deploying a VCS Expressway behind a NAT, because our experience shows that they do not handle video traffic properly. You must use the VCS to perform the static network address translation on its own interface. For more information, see [What About Routers/Firewalls with SIP/H.323 ALG?](#), page 69.

Planning Your Deployment

Do Not Overlap Subnets

The recommended deployment of the VCS Expressway configures both LAN interfaces. The LAN1 and LAN2 interfaces **must** be located in non-overlapping subnets to ensure that traffic is sent out the correct interface.

Clustering

- When the peers have the **Advanced Networking** option installed, you must use the LAN1 interface address of each peer to create the cluster.
- The LAN interface that you use for clustering must not have **Static NAT mode** enabled.

For these reasons, we recommend that you use LAN2 as the externally facing interface, and also enable static NAT on LAN2 when it's required.

External LAN Interface Setting

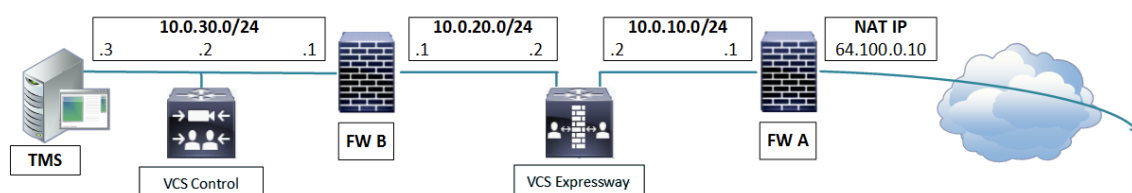
The **External LAN interface** configuration setting, on the **IP** configuration page, controls where the VCS Expressway's TURN server allocates TURN relays. In the recommended dual NIC deployment, you should select the externally-facing LAN interface (LAN2) on the VCS Expressway.

Recommended: Dual NIC Static NAT Deployment

The following example illustrates the recommended deployment. It shows the typical DMZ configuration where the internal and external firewalls cannot route directly to each other, and dual NIC devices such as VCS Expressway are required to validate and forward the traffic between the isolated subnets.

The VCS Expressway has both NICs enabled, and it has static NAT enabled on its outward-facing LAN interface. The VCS Control inside the network is a traversal client of the VCS Expressway in the DMZ.

Figure 10 Dual Network Interfaces Deployment



Appendix 4: Advanced Network Deployments

This deployment consists of:

- DMZ subnet 1 – 10.0.10.0/24, containing:
 - the internal interface of Firewall A – 10.0.10.1
 - the LAN2 interface of the VCS Expressway – 10.0.10.2
- DMZ subnet 2 – 10.0.20.0/24, containing:
 - the external interface of Firewall B – 10.0.20.1
 - the LAN1 interface of the VCS Expressway – 10.0.20.2
- LAN subnet – 10.0.30.0/24, containing:
 - the internal interface of Firewall B – 10.0.30.1
 - the LAN1 interface of the VCS Control – 10.0.30.2
 - the network interface of the Cisco TMS server – 10.0.30.3
- Firewall A is the outward-facing firewall; it is configured with a NAT IP (public IP) of 64.100.0.10 which is statically NATed to 10.0.10.2 (the LAN2 interface address of the VCS Expressway)
- Firewall B is the internally-facing firewall
- VCS Expressway LAN1 has static NAT mode disabled
- VCS Expressway LAN2 has static NAT mode enabled with Static NAT address 64.100.0.10
- VCS Control has a traversal client zone pointing to 10.0.20.2 (LAN1 of the VCS Expressway)
- Cisco TMS has VCS Expressway added with IP address 10.0.20.2

With the above deployment, there is no regular routing between the 10.0.20.0/24 and 10.0.10.0/24 subnets. The VCS Expressway bridges these subnets and acts as a proxy for SIP/H.323 signaling and RTP/RTCP media.

Static Routes Towards the Internal Network

With a deployment like [Figure 10 Dual Network Interfaces Deployment, page 63](#), you would typically configure the private address of the external firewall (10.0.10.1 in the diagram) as the default gateway of the VCS Expressway. Traffic that has no more specific route is sent out from either VCS Expressway interface to 10.0.10.1.

- **If the internal firewall (B) is doing NAT** for traffic from the internal network (subnet 10.0.30.0 in diagram) to LAN1 of the VCS Expressway (for example traversal client traffic from VCS Control), that traffic is recognized as being from the same subnet (10.0.20.0 in diagram) as it reaches LAN1 of the VCS Expressway. The VCS Expressway will therefore be able to reply to this traffic through its LAN1 interface.

MRA limitation: Due to VCS Expressway security mechanisms, Mobile & Remote Access (MRA) is not compatible with this scenario. If there is source NAT on the packets from VCS Control then edge login requests will fail (destination NAT is unaffected).

- **If the internal firewall (B) is not doing NAT** for traffic from the internal network (subnet 10.0.30.0 in diagram) to LAN1 of the VCS Expressway (for example traversal client traffic from VCS Control), that traffic still has the originating IP address (for example, 10.0.30.2 for traffic from VCS Control in the diagram). You must create a static route towards that source from LAN1 on the VCS Expressway, or the return traffic will go to the default gateway (10.0.10.1). You can do this on the web UI (**System > Network interfaces > Static routes**) or using `xCommand RouteAdd` at the CLI.

If the VCS Expressway needs to communicate with other devices behind the internal firewall (eg. for reaching network services such as NTP, DNS, LDAP/AD and syslog servers), you also need to add static routes from VCS Expressway LAN1 to those devices/subnets.

In this particular example, we want to tell the VCS Expressway that it can reach the 10.0.30.0/24 subnet behind the 10.0.20.1 firewall (router), which is reachable via the LAN1 interface. This is accomplished using the following `xCommand RouteAdd` syntax:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

In this example, the `Interface` parameter could also be set to `Auto` as the gateway address (10.0.20.1) is only reachable via LAN1.

Figure 11 The Web UI for Creating a Static Route

Static routes You are here: [System](#) > [Network interfaces](#) > [Static routes](#)

Create a static route

IP address	★ 10.0.30.0	i
Prefix length	★ 24	i
Address range	10.0.30.0 - 10.0.30.255	
Gateway	★ 10.0.20.1	i
Interface	LAN 1 i	

Create route

The `xCommand RouteAdd` command and the equivalent web UI, are detailed in the VCS help and the *VCS Administrator Guide*.

Background Information

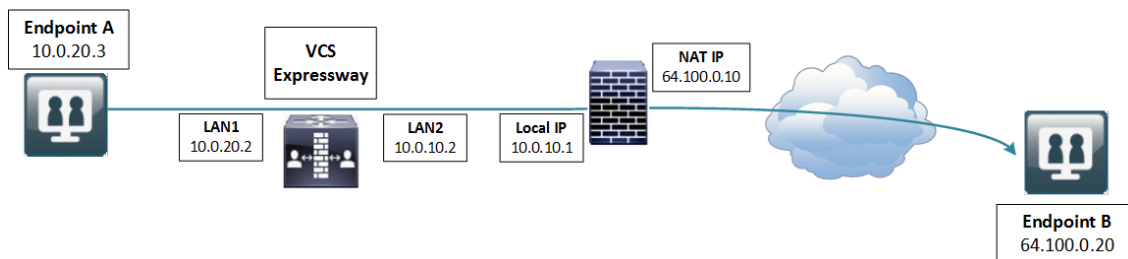
The Challenge of NAT for SIP and H.323 Applications

When deploying a VCS Expressway for business to business communications, or for supporting home workers and travelling workers, it is usually desirable to deploy the VCS Expressway in a NATed DMZ rather than having the VCS Expressway configured with a publicly routable IP address.

Network Address Translation (NAT) poses a challenge with SIP and H.323 applications, as with these protocols, IP addresses and port numbers are not only used in OSI layer 3 and 4 packet headers, but are also referenced within the packet payload data of H.323 and SIP messages themselves.

This usually breaks SIP/H.323 call signaling and RTP media packet flows, since NAT routers/firewalls will normally translate the IP addresses and port numbers of the headers, but leave the IP address and port references within the SIP and H.323 message payloads unchanged.

To provide an example of this, assume you have a VCS Expressway deployed behind a NAT router and two endpoints. The VCS Expressway has static NAT disabled on LAN2, but the NAT router is configured with a static 1:1 NAT, NATing the public address 64.100.0.10 to the VCS Expressway LAN2 IP address 10.0.10.2:

Figure 12 Example Deployment with Static NAT on Firewall

- NAT router with local IP address 10.0.10.1 and NAT IP address 64.100.0.10, statically NATed to 10.0.10.2
- VCS Expressway LAN1 (internally-facing interface) with IP address 10.0.20.2

Appendix 4: Advanced Network Deployments

- VCS Expressway LAN2 (externally-facing interface) with IP address 10.0.10.2 (and with static NAT disabled)
- VCS Expressway default gateway set to 10.0.10.1 (inside address of NAT firewall, reachable via LAN2)
- Endpoint A with IP address 10.0.20.3, registered to VCS Expressway
- Endpoint B with IP address 64.100.0.20, located on the Internet, not registered to the VCS Expressway

Assume that endpoint A places a SIP call towards endpoint B. The call will arrive at the VCS Expressway, which will proxy the SIP INVITE towards endpoint B. The VCS Expressway to Endpoint B will then be a traversal call, which means that the VCS Expressway will take both signaling and media, and the packet carrying the SIP INVITE message will have the following contents as it arrives at the NAT router (the actual INVITE contents have been simplified for ease of reading):

SIP INVITE Arriving at NAT Router

```

Packet header:
Source IP: 10.0.10.2
Destination IP: 64.100.0.20
SIP payload:
INVITE sip: 64.100.0.20 SIP/2.0
Via: SIP/2.0/TLS 10.0.10.2:5061
Via: SIP/2.0/TLS 10.0.20.3:55938
Call-ID: 20ec9fd084eb3dd2@127.0.0.1
CSeq: 100 INVITE
Contact: <sip:EndpointA@10.0.20.3:55938;transport=tls>
From: "Endpoint A" <sip:EndpointA@cisco.com>;tag=9a42af
To: <sip: 64.100.0.20>
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 2825

v=0
o=tandberg 1 2 IN IP4 10.0.10.2
s=-
c=IN IP4 10.0.10.2
b=AS:2048
...
...

```

In the example above, the SDP (session description protocol) within the SIP payload contains a reference to the VCS Expressway IP address, marked in yellow: **c=IN IP4 10.0.10.2**.

Upon receiving the SIP INVITE packet, the NAT router will rewrite the layer 3 source IP address header (marked in green: **10.0.10.2**) and replace 10.0.10.2 (VCS Expressway LAN2 IP address) with its own public NAT address (**64.100.0.10**) and route the packet out to the Internet, so that the SIP INVITE message will have the following contents as it arrives at endpoint B:

SIP INVITE Arriving at Endpoint B

```

Packet header:
Source IP: 64.100.0.10
Destination IP: 64.100.0.20
SIP payload:
INVITE sip:64.100.0.20 SIP/2.0
Via: SIP/2.0/TLS 10.0.10.2:5061
Via: SIP/2.0/TLS 10.0.20.3:55938
Call-ID: 20ec9fd084eb3dd2@127.0.0.1
CSeq: 100 INVITE
Contact: <sip:EndpointA@10.0.20.3:55938;transport=tls>
From: "Endpoint A" <sip:EndpointA@cisco.com>;tag=9a42af
To: <sip:64.100.0.20>

```

Appendix 4: Advanced Network Deployments

```

Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 2825

```

```

v=0
s=-
c=IN IP4 10.0.10.2

```

```

b=AS:2048
...
...
...

```

As can be seen from the example above, endpoint B will see that the SIP INVITE was received from IP 64.100.0.10 (NAT router), so the endpoint will know where to send its reply messages for the INVITE itself.

The c-line within the SDP of the SIP INVITE is however still set to `c=IN IP4 10.0.10.2`, which means that endpoint B will attempt to send RTP media to the IP address 10.0.10.2, an address which is not routable on the Internet.

The result in this scenario will therefore be that endpoint A will never receive media sent by endpoint B (while endpoint B will normally receive media from endpoint A, since endpoint B is assigned with a publicly routable IP address).

Similar behavior will be seen in H.323 calls, since H.323 uses the same principles as SIP in terms of embedding IP address and port references within the message payload.

How Does VCS Expressway Address This Challenge?

To ensure that call signaling and media connectivity remains functional in scenarios where the VCS Expressway is deployed behind a NAT (as in the example above), the VCS Expressway will have to modify the parts of SIP and H.323 messages which contain references to its actual LAN2 network interface IP address (10.0.10.2) and replace these with the public NAT address of the NAT router (64.100.0.10).

This can be achieved by enabling **Static NAT mode** on selected network interfaces on the VCS Expressway. The Static NAT mode feature on the VCS Expressway is made available with the **Advanced Networking** option key.

This option key allows the use of two network interfaces (LAN1 and LAN2), and on a VCS Expressway it allows Static NAT mode to be enabled on one or both of these interfaces. You do not have to use both interfaces, but we recommend that you do. If you choose to use a single interface, and enable static NAT on that interface, read [Why We Advise Against Using These Types of Deployment, page 72](#).

When static NAT has been enabled on an interface, the VCS will apply static NAT for all outbound SIP and H.323 traffic for this interface, which means that H.323 and SIP devices have to communicate with this interface using the static NAT address rather than the local interface address.

When the **Advanced Networking** key is installed on the VCS Expressway, the **IP** configuration page (**System > Network interfaces > IP**) has additional options, allowing the user to decide whether to **Use dual network interfaces**, to nominate which interface is the **External LAN interface**, to enable **Static NAT mode** on selected interfaces and configure an **IPv4 static NAT address** for each interface.

Appendix 4: Advanced Network Deployments

Figure 13 VCS Expressway Configuration for the Example Deployment

The screenshot shows the VCS Expressway configuration interface. At the top, there's a breadcrumb 'You are here: System > IP'. The 'IP' section is active, showing 'IP protocol' set to 'IPv4', 'Use dual network interfaces' set to 'Yes', and 'External LAN interface' set to 'LAN2'. Below this, 'IPv4 gateway' is set to '10.0.10.1' and 'IPv6 gateway' is empty. The 'LAN 1' section shows 'IPv4 address' as '10.0.20.2', 'IPv4 subnet mask' as '255.255.255.0', 'IPv4 subnet range' as '10.0.20.0 - 10.0.20.255', 'IPv4 static NAT mode' as 'Off', and 'IPv6 address' is empty. The 'LAN 2' section shows 'IPv4 address' as '10.0.10.2', 'IPv4 subnet mask' as '255.255.255.0', 'IPv4 subnet range' as '10.0.10.0 - 10.0.10.255', 'IPv4 static NAT mode' as 'On', 'IPv4 static NAT address' as '64.100.0.10', and 'IPv6 address' is empty. Each field has an information icon (i) to its right.

- Dual interfaces are selected and the external LAN interface is set to *LAN2*
- Configuration > IPv4 gateway is set to 10.0.10.1, the local IP address of the NAT router
- LAN1 > IPv4 address is set to 10.0.20.2
- LAN1 > IPv4 static NAT mode is set to *Off*
- LAN2 > IPv4 address is set to 10.0.10.2
- LAN2 > IPv4 static NAT mode is set to *On*
- LAN2 > IPv4 static NAT address is set to 64.100.0.10, the public NAT address of the NAT router

When enabling **IPv4 static NAT mode** on an interface (LAN2 in our example), the VCS Expressway will modify the payload of H.323 and SIP messages sent out via this interface, so that references to the LAN2 interface address (10.0.10.2) are replaced with the IPv4 static NAT address configured for this interface (64.100.0.10). This means that when looking at the payload of SIP and H.323 messages sent out via this interface, it will appear as if the LAN2 interface has a public IP address (64.100.0.10).

It is important to note that the VCS Expressway will not modify the layer 3 source address of outgoing H.323 and SIP packets sent out of this interface, as this will be done by the NAT router.

With this configuration in place, the SIP INVITE shown in Figure 4 will now look as follows as it arrives at endpoint B:

SIP INVITE Arriving at Endpoint B - Static NAT Mode Enabled

Packet header:

Source IP: 64.100.0.10

Appendix 4: Advanced Network Deployments

```

Destination IP: 64.100.0.20
SIP payload:
INVITE sip: 64.100.0.20 SIP/2.0
Via: SIP/2.0/TLS 10.0.10.2:5061
Via: SIP/2.0/TLS 10.0.20.3:55938
Call-ID: 20ec9fd084eb3dd2@127.0.0.1
CSeq: 100 INVITE
Contact: <sip:EndpointA@10.0.20.3:55938;transport=tls>
From: "Endpoint A" <sip:EndpointA@cisco.com>;tag=9a42af
To: <sip: 64.100.0.20>
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 2825

v=0
s=-
c=IN IP4 64.100.0.10

b=AS:2048
...
...
...

```

With static NAT enabled on LAN2 of the VCS Expressway, the c-line of the SIP INVITE has now been rewritten to **c=IN IP4 64.100.0.10**, and this means that when endpoint B sends outbound RTP media to endpoint A, this will be sent to IP address 64.100.0.10, the public NAT address of the NAT router, which is 1:1 NATed to the LAN2 IP address of the VCS Expressway, 10.0.10.2. As RTP media from endpoint B arrives at the NAT router with a destination IP address of 64.100.0.10, the NAT router will forward these packets to the VCS Expressway at 10.0.10.2 and two-way media is achieved.

What About Routers/Firewalls with SIP/H.323 ALG?

Some routers and firewalls have SIP and H.323 ALG capabilities. ALG is also referred to as Fixup, Inspection, Application Awareness, Stateful Packet Inspection, Deep Packet Inspection and so forth. This means that the router/firewall is able to identify SIP and H.323 traffic as it passes through and inspect, and in some cases modify, the payload of the SIP and H.323 messages. The purpose of modifying the payload is to help the H.323 or SIP application from which the message originated to traverse NAT, i.e. to perform a similar process to what the VCS Expressway does.

The challenge with router/firewall-based SIP and H.323 ALGs is that these were originally intended to aid relatively basic H.323 and SIP applications to traverse NAT, and these applications had, for the most part, very basic functionality and often only supported audio.

Over the years, many H.323 and SIP implementations have become more complex, supporting multiple video streams and application sharing (H.239, BFCP), encryption/security features (H.235, DES/AES), firewall traversal (Assent, H.460) and other extensions of the SIP and H.323 standards.

For a router/firewall to properly perform ALG functions for SIP and H.323 traffic, it is therefore of utmost importance that the router/firewall understands and properly interprets the full content of the payload it is inspecting. Since H.323 and SIP are standards/recommendations which are in constant development, it is not likely that the router/firewall will meet these requirements, resulting in unexpected behavior when using H.323 and SIP applications in combination with such routers/firewalls.

There are also scenarios where the router/firewall normally will not be able to inspect the traffic at all, for example when using SIP over TLS, where the communication is end-to-end secure and encrypted as it passes through the router/firewall.

As per the Prerequisites section of this appendix, you should disable SIP and H.323 ALGs on routers/firewalls carrying network traffic to or from a VCS Expressway. We do not support this functionality, as, when enabled, it is frequently found to negatively affect the built-in firewall/NAT traversal functionality of the VCS Expressway itself. This is also mentioned in *Appendix 3: Firewall and NAT Settings*.

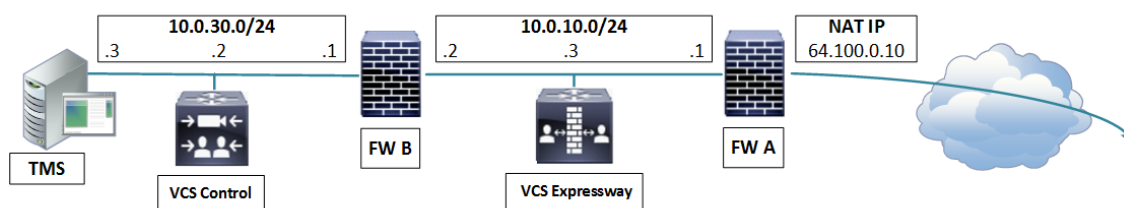
Other Deployment Examples

Note: Using the VCS Expressway as shown in these examples could have a serious impact on your network bandwidth, and may contravene your security policy. We strongly recommend that you use the [Recommended: Dual NIC Static NAT Deployment, page 63](#). Read [Why We Advise Against Using These Types of Deployment, page 72](#).

Single Subnet DMZ Using Single VCS Expressway LAN Interface and Static NAT

In this case, FW A can route traffic to FW B (and vice versa). VCS Expressway allows video traffic to be passed through FW B without pinholing FW B from outside to inside. VCS Expressway also handles firewall traversal on its public side.

Figure 14 Single Subnet DMZ - Single LAN Interface and Static NAT



This deployment consists of the following elements:

- Single subnet DMZ (10.0.10.0/24) with the following interfaces:
 - Internal interface of firewall A - 10.0.10.1
 - External interface of firewall B - 10.0.10.2
 - LAN1 interface of VCS Expressway - 10.0.10.3
- LAN subnet (10.0.30.0/24) with the following interfaces:
 - Internal interface of firewall B - 10.0.30.1
 - LAN1 interface of VCS Control - 10.0.30.2
 - Network interface of Cisco TMS - 10.0.30.3

A static 1:1 NAT has been configured on firewall A, NATing the public address 64.100.0.10 to the LAN1 address of the VCS Expressway. **Static NAT mode** is enabled for LAN1 on the VCS Expressway, with a static NAT address of 64.100.0.10.

Note:

You must enter the FQDN of the VCS Expressway, as it is seen from outside the network, as the peer address on the VCS Control's secure traversal zone. The reason for this is that in static NAT mode, the VCS Expressway requests that incoming signaling and media traffic should be sent to its external FQDN, rather than its private name.

This also means that the external firewall must allow traffic from the VCS Control to the VCS Expressway's external FQDN. This is known as NAT reflection, and may not be supported by all types of firewalls.

So, in this example, firewall A must allow NAT reflection of traffic coming from the VCS Control that is destined for the external address, that is 64.100.0.10, of the VCS Expressway. The traversal zone on the VCS Control must have 64.100.0.10 as the peer address.

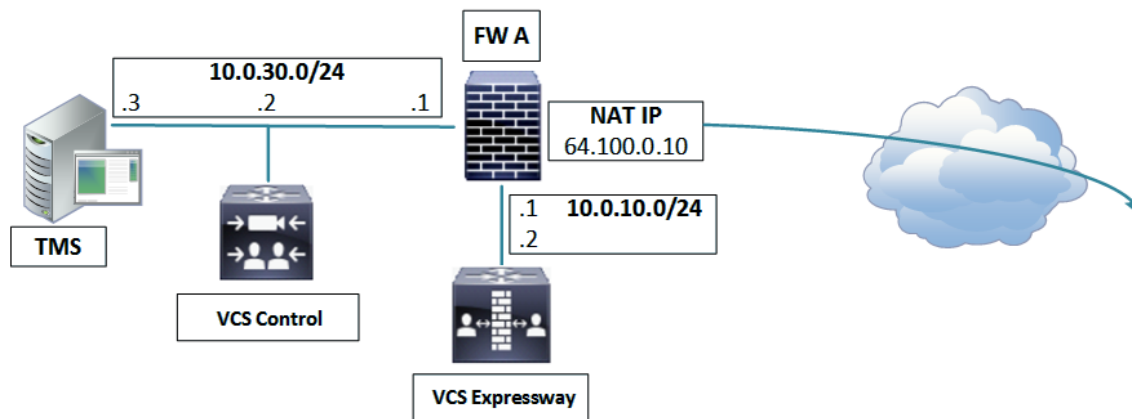
The VCS Expressway should be configured with a default gateway of 10.0.10.1. Whether or not static routes are needed in this scenario depends on the capabilities and settings of FW A and FW B. VCS Control to VCS Expressway

Appendix 4: Advanced Network Deployments

communications will be to the 64.100.0.10 address of the VCS Expressway. The return traffic from the VCS Expressway to VCS Control might have to go through the default gateway. If a static route is added to the VCS Expressway so that reply traffic goes from the VCS Expressway and directly through FW B to the 10.0.30.0/24 subnet, asymmetric routing occurs. Which may or may not work, depending on the firewall capabilities.

The VCS Expressway can be added to Cisco TMS using its internal IP address (10.0.10.3). This is because static NAT mode settings on the VCS Expressway do not affect Cisco TMS management communications. You could add the VCS Expressway's external interface to TMS instead (64.100.0.10 in the diagram) if FW A allows it.

3-port Firewall DMZ Using Single VCS Expressway LAN Interface



In this deployment, a 3-port firewall is used to create the following:

- DMZ subnet (10.0.10.0/24) with the following interfaces:
 - DMZ interface of firewall A - 10.0.10.1
 - LAN1 interface of VCS Expressway - 10.0.10.2
- LAN subnet (10.0.30.0/24) with the following interfaces:
 - LAN interface of firewall A - 10.0.30.1
 - LAN1 interface of VCS Control - 10.0.30.2
 - Network interface of Cisco TMS - 10.0.30.3

A static 1:1 NAT has been configured on firewall A, NATing the public address 64.100.0.10 to the LAN1 address of the VCS Expressway. Static NAT mode is enabled for LAN1 on the VCS Expressway, with a static NAT address of 64.100.0.10.

The VCS Expressway should be configured with a default gateway of 10.0.10.1. Since this gateway must be used for all traffic leaving the VCS Expressway, no static routes are needed in this type of deployment.

Note: The traversal client zone on the VCS Control needs to be configured with a peer address which matches the static NAT address of the VCS Expressway, in this case 64.100.0.10, for the same reasons as described in [Single Subnet DMZ Using Single VCS Expressway LAN Interface and Static NAT, page 70](#).

This means that firewall A must allow traffic from the VCS Control with a destination address of 64.100.0.10. This is also known as NAT reflection, and it should be noted that this is not supported by all types of firewalls.

The VCS Expressway can be added to Cisco TMS with the IP address 10.0.10.2 (or with IP address 64.100.0.10 if FW A allows this), since Cisco TMS management communications are not affected by static NAT mode settings on the VCS Expressway.

Appendix 4: Advanced Network Deployments

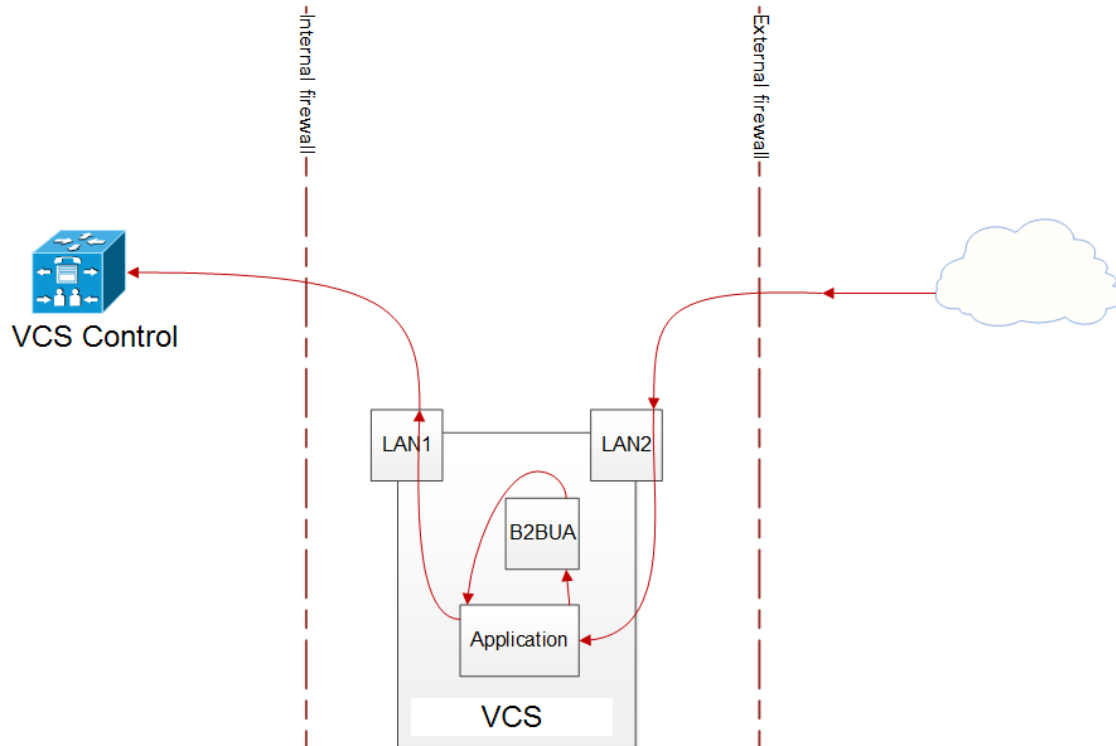
Why We Advise Against Using These Types of Deployment

For deployments that use only one NIC on the VCS Expressway, but also require static NAT for the public address, the media must "hairpin" or reflect on the external firewall whenever media is handled by the VCS Expressway's back to back user agent (B2BUA).

For all calls coming in on a Unified Communications Traversal Server zone, or another zone where SIP **Media encryption mode** is not *Auto*, the VCS Expressway's B2BUA could be engaged to decrypt or encrypt the media packets. In these deployments, the B2BUA sees the public IP address of the VCS Expressway instead of its private IP address, so the media stream must go through the network address translator to get to the private IP address.

- Not all firewalls will allow this reflection, and it is considered by some to be a security risk.
- Each call where the B2BUA is engaged will consume three times as much bandwidth as it would using the recommended dual NIC deployment. This could adversely affect call quality.

Figure 15 Media Path in Dual NIC Static NAT Example (Recommended)



Appendix 4: Advanced Network Deployments

Figure 16 Media Path in Single NIC Static NAT Example

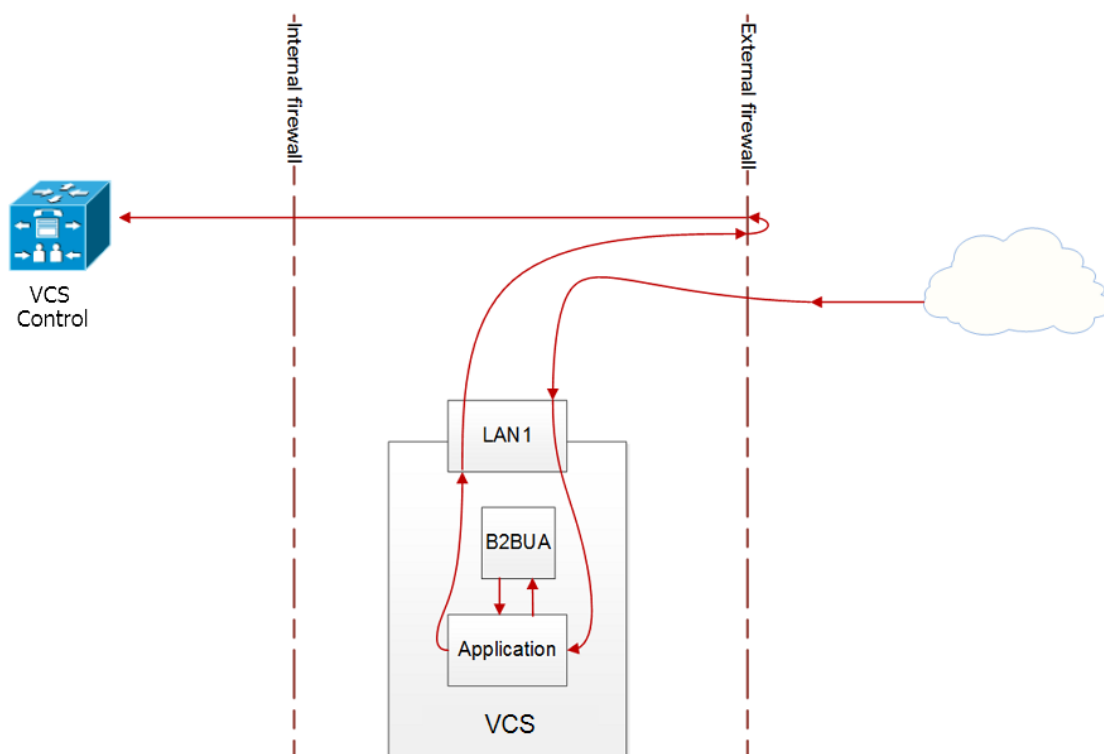
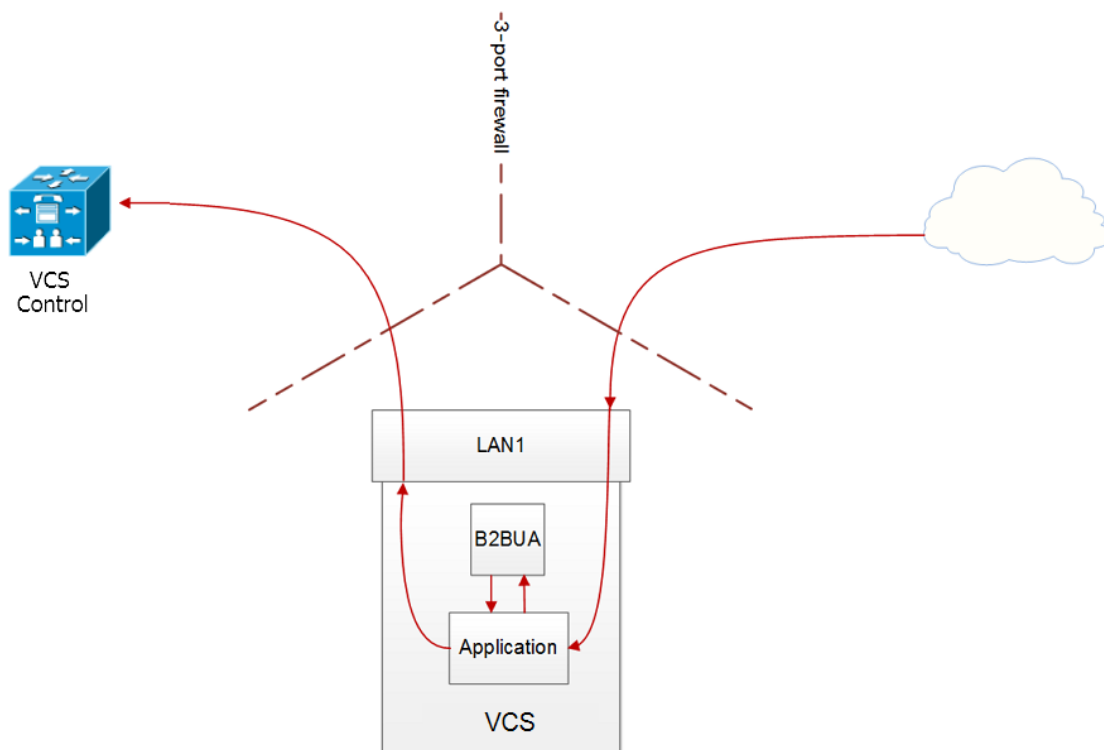


Figure 17 Media Path in 3-port Firewall Static NAT Example



Appendix 4: Advanced Network Deployments

The 3-port Firewall Static NAT diagram, above, shows the traffic flow in the case where a Cisco ASA 8.4 and later series, has been configured to allow traffic to flow from LAN1 through the 3-port firewall.

Other vendors' firewalls may not have a similar configuration option.

Obtaining Documentation and Submitting a Service Request

Use the [Cisco Notification Service](#) to create customized flexible notification alerts to be sent to you via email or by RSS feed.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2016 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)