Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)

Deployment Guide

Cisco VCS X8.5.2

April 2015

Contents

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 the video network administrator through the series of tasks required to set up the VCSs and then describes how to check that the system is working as expected.
- It provides the required DNS, NAT and firewall configuration information but assumes that the network administrator has a working knowledge of configuring these systems.

Detailed reference information is contained in this document's appendices:

- Appendix 1: Configuration details [p.46] lists the VCS configuration details used in this document.
- Appendix 2: DNS records [p.50] describes the DNS records required for this example deployment.
- Appendix 3: Firewall and NAT settings [p.52] includes details of required NAT and firewall configurations. 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.
- Appendix 4: Advanced network deployments [p.56] explains how to deploy your system with a static NAT and Dual Network Interface architecture.

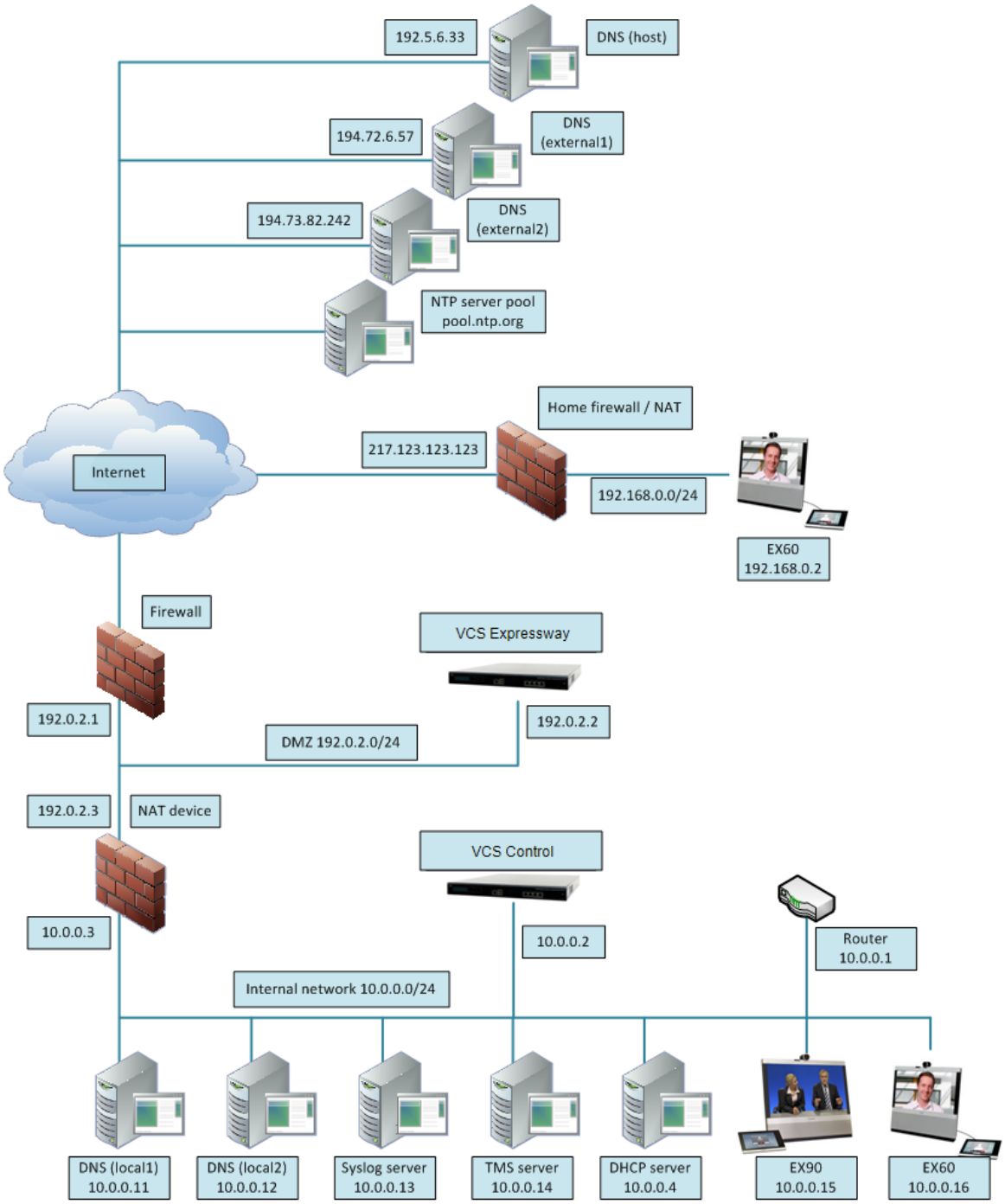
Descriptions of system configuration parameters can be found in *VCS Administrator Guide* and the VCS web application's online field help and page help .

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

- *VCS Cluster Creation and Maintenance Deployment Guide*
- *Cisco TMS Provisioning Extension Deployment Guide*
- *FindMe Express Deployment Guide*
- *VCS IP Port Usage for Firewall Traversal*
- *Device Authentication on VCS Deployment Guide*

Example network deployment

The example network shown below is used as the basis for the deployment described in this document.



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

Network elements

Internal network elements

The internal network elements are devices which are hosted on the organization's local area network.

Elements on the internal network have an internal network domain name. This internal network domain 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).

VCS Control

The VCS Control is a SIP Registrar & Proxy and H.323 Gatekeeper for devices which are located on the internal network.

The VCS Control is configured with a traversal client zone to communicate with the VCS Expressway to allow inbound and outbound calls to traverse the NAT device.

EX90 and EX60

These are 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

The DHCP server provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.

Router

The router device acts as the gateway for all internal network devices to route towards the DMZ (to the NAT device internal address).

Cisco TMS server

A management and scheduling server (see Task 14: Configuring Cisco TMS (optional) [p.36]).

Syslog server

A logging server for Syslog messages (see Task 15: Configuring logging (optional) [p.38]).

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

EX60

An example remote endpoint, which is registering to the VCS Expressway via the internet.

DNS (Host)

The DNS owned by service provider which hosts the external domain example.com.

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:

- 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 [p.52].
- 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 [p.56] 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.

- 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 internal and external infrastructure (VCS Control and VCS Expressway).

The DNS SRV configurations are described in Appendix 2: DNS records [p.50].

Prerequisites and process summary

Prerequisites

Before starting the system configuration, make sure you have access to:

- the *VCS Administrator Guide* and *VCS Getting Started Guide* (for reference purposes)
- your VCS system
- a PC connected via Ethernet to a LAN which can route HTTP(S) traffic to the VCS
- a web browser running on the PC
- a serial interface on the PC and cable (if the initial configuration is to be performed over the serial interface)

The following non-VCS system configuration should also be completed:

- internal and external DNS records (see Appendix 2: DNS records [p.50])
- NAT & firewall configuration (see Appendix 3: Firewall and NAT settings [p.52])
- DHCP server configuration (not described in this document)

Summary of process

The configuration process consists of the following tasks.

VCS system configuration:

- Task 1: Performing initial configuration [p.10]
- Task 2: Setting the system name [p.10]
- Task 3: Configuring DNS [p.11]
- Task 4: Replacing the default server certificate [p.13]
- Task 5: Configuring NTP servers [p.14]
- Task 6: Configuring SIP domains [p.14]

Routing configuration:

- Task 7: Configuring transforms [p.17]
- Task 8: Configuring Local Zone search rules [p.17]
- Task 9: Configuring the traversal zone [p.20]
- Task 10: Configuring traversal zone search rules [p.25]
- Task 11: Configuring the DNS zone [p.28]
- Task 12: Configuring DNS zone search rules [p.29]
- Task 13: Configuring external (unknown) IP address routing [p.30]

Optional configuration tasks:

- Task 14: Configuring Cisco TMS (optional) [p.36]
- Task 15: Configuring logging (optional) [p.38]
- Task 16: Configuring registration restriction policy (optional) [p.38]

VCS system configuration

Task 1: Performing initial configuration

Assuming the VCS is in the factory delivered state, follow the Initial configuration steps described in the *VCS Getting Started Guide* to configure the basic network parameters:

- LAN1 IP (IPv4 or IPv6) address
- Subnet mask (if using IPv4)
- Default Gateway IP address (IPv4 or IPv6)

Note that VCS requires a static IP address (it will not pick up an IP address from a DHCP server).

The initial configuration can be performed in one of three ways:

- using a serial cable
- via the front panel of the VCS appliance
- via the default IP address of 192.168.0.100

See the “Initial configuration” section in *VCS Getting Started Guide* for details.

This deployment guide is based on configuration using the web interface. If you cannot access the VCS using the web interface after completing the initial configuration (assigning the IP address), speak to your network administrator.

The follow configuration values are used in the example deployment:

	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

Task 2: Setting the system name

The **System name** defines the name of the VCS.

The **System name** appears in various places in the web interface, and in the display on the front panel of the appliance (so that you can identify it when it is in a rack with other systems). The system name is also used by Cisco TMS.

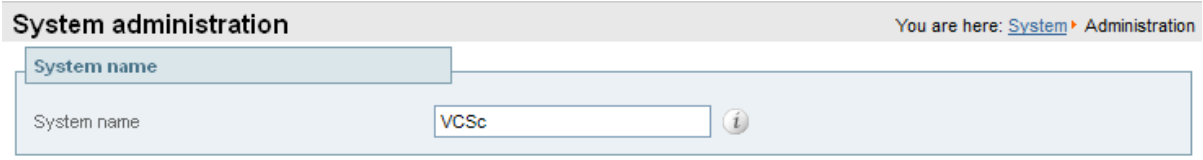
You are recommended to give the VCS a name that allows you to easily and uniquely identify it. If the system name is longer than 16 characters, only the last 16 characters will be shown in the display on the front panel.

To configure the **System name**:

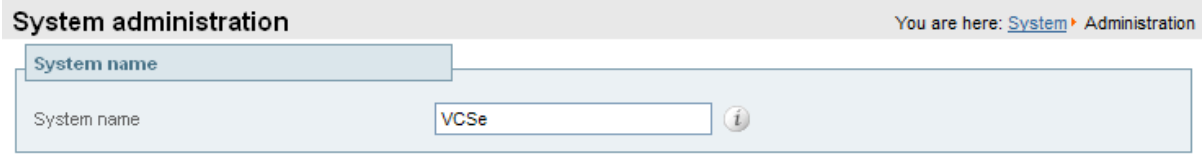
1. Go to **System > Administration**.
2. Configure the **System name** as follows:

	VCS Control	VCS Expressway
System name	Enter `vcsc`	Enter `vcse`

3. Click **Save**.



VCS Control



VCS Expressway

Task 3: 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 `vcsc`	Enter `vcse`

3. Click **Save**.

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 `internal-domain.net`	Enter `example.com`

3. Click **Save**.

DNS servers

The DNS server addresses are the IP addresses of up to 5 domain name servers to use when resolving domain names. You must specify at least one default DNS server to be queried for address resolution if you want to either:

- use FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, neighbor zones and peers)
- use features such as URI dialing or ENUM dialing

The VCS only queries one server at a time; if that server is not available the VCS will try another server from the list.

In the example deployment 2 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.

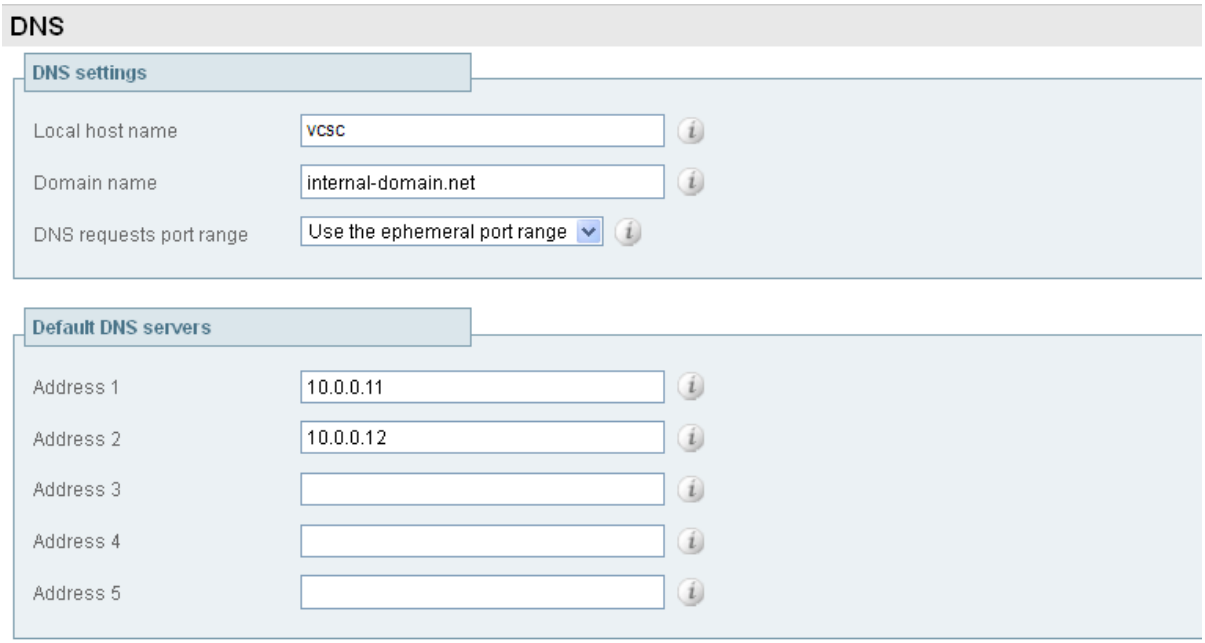
To configure the **Default DNS server** addresses:

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

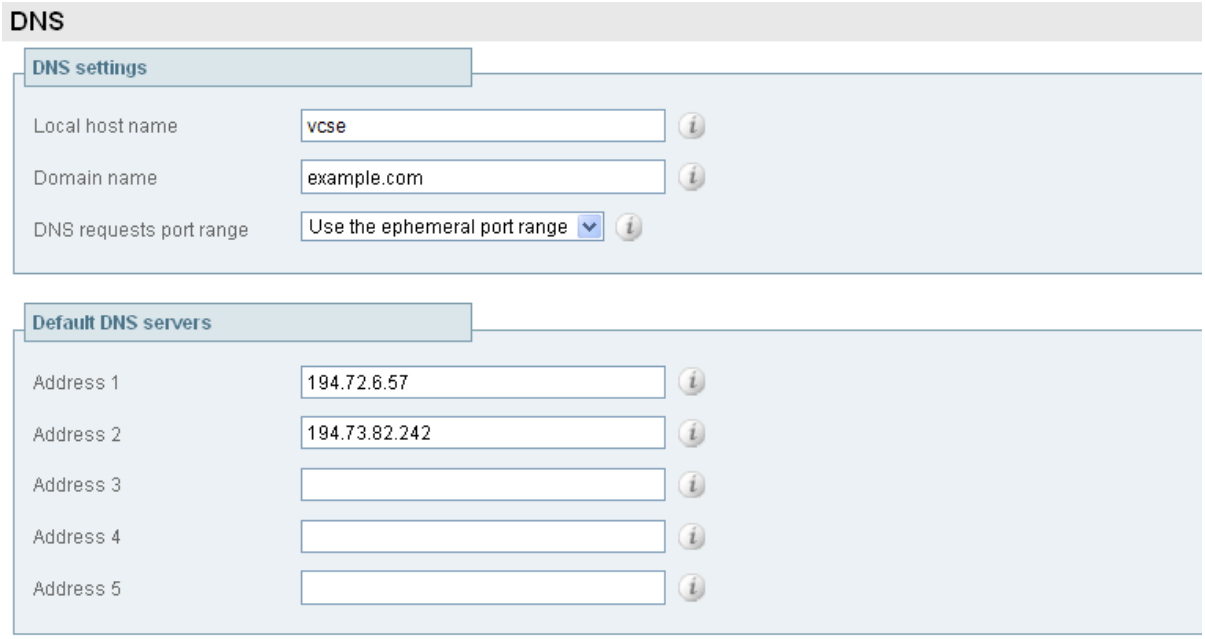
	VCS Control	VCS Expressway
Address 1	Enter `10.0.0.11`	Enter `194.72.6.57`
Address 2	Enter `10.0.0.12`	Enter `194.73.82.242`

3. Click **Save**.

VCS Control has a Fully Qualified Domain Name of vcsc.internal-domain.net



VCS Expressway has a Fully Qualified Domain Name of vcse.example.com



Task 4: 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.

The VCS allows you to install appropriate files so that it can act 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 and obtain 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 that your system is working correctly before you attempt to secure the connection with TLS. You are

also recommended to use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

Note: be careful not to allow your CA certificates or CRLs to expire as 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*.

Task 5: 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.

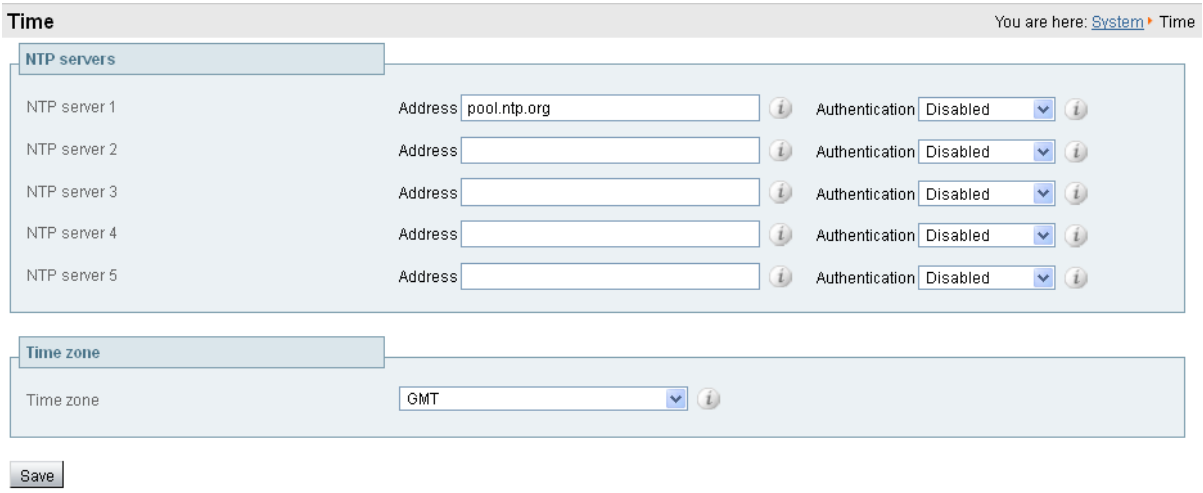
The **Time zone** sets the local time zone of the VCS.

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**.



Task 6: 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.

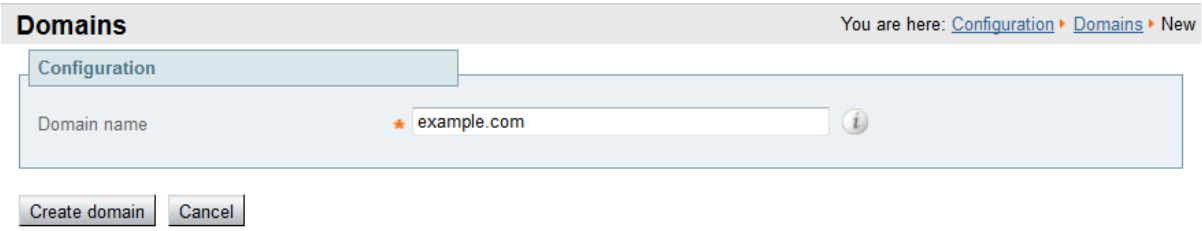
- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See Task 16: Configuring registration restriction policy (optional) [p.38].
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

1. Go to **Configuration > Domains**.
2. Click **New**.
3. 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`

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



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 17: Configuring device authentication policy (optional) [p.39].

Routing configuration

Pre-search transforms

Pre-search transform configuration allows the destination alias (called address) in an incoming search request to be modified. The transformation is applied by the VCS 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 will 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 will automatically append 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.

- Pre-search transforms should be used 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 is 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 SIP (and H.323) 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 7: 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.

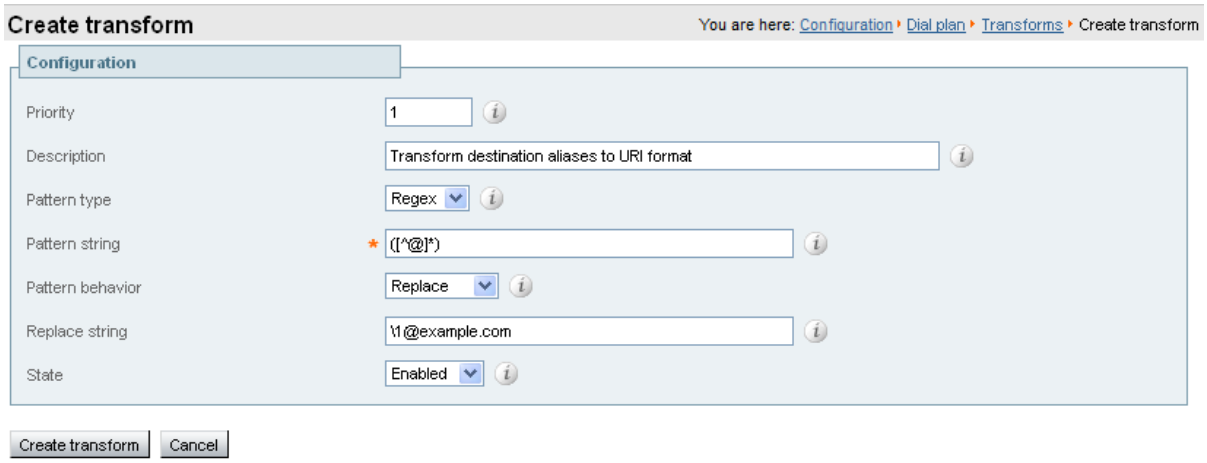
The following transform modifies the destination alias of all call attempts made to destination aliases which do not contain an '@'. The old destination alias has @example.com appended to it. This has the effect of standardizing all called destination aliases into a SIP URI format.

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**.



Task 8: Configuring Local Zone search rules

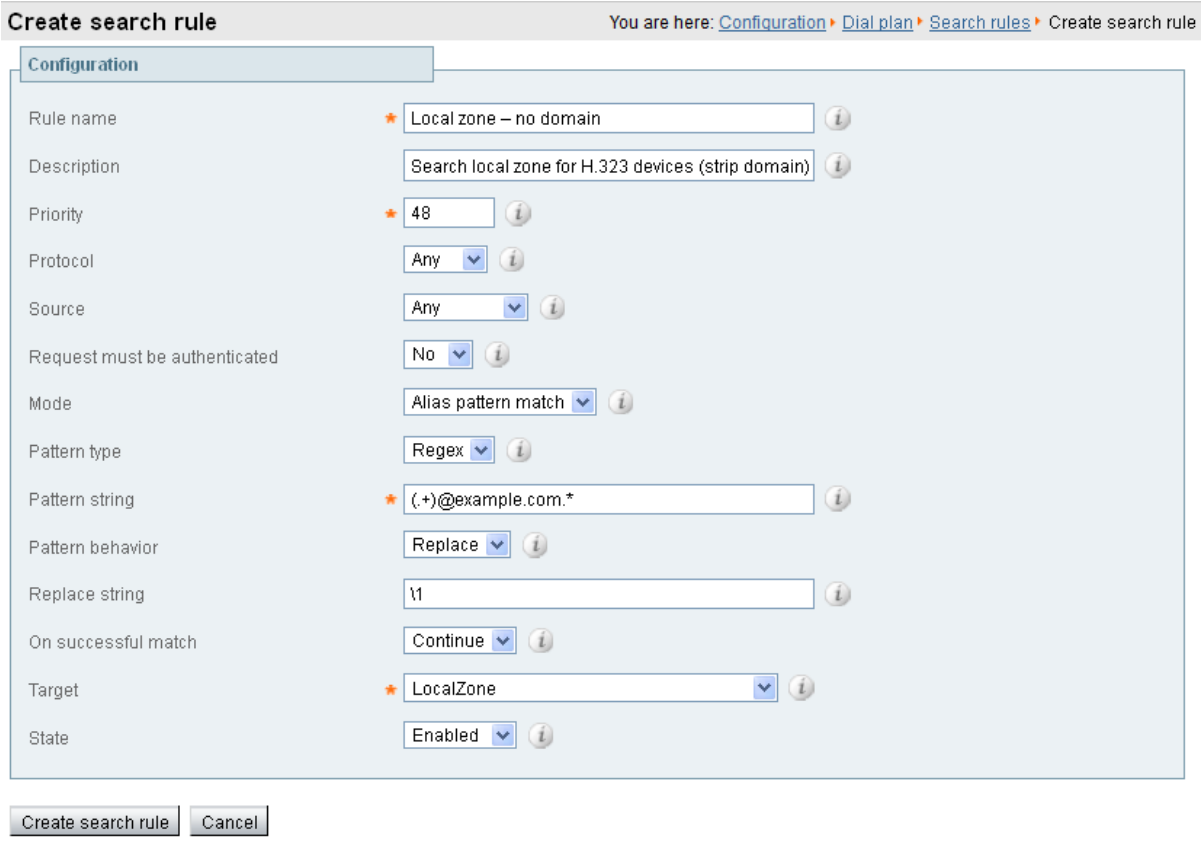
To configure the search rules to route calls to the Local Zone (to locally registered endpoint aliases):

1. Go to **Configuration > Dial plan > Search rules**.
2. Select the check box next to the default search rule (**LocalZoneMatch**).

3. Click **Delete**.
   (The default search rule is being deleted and replaced with a more specific configuration.)
4. Click **OK**.
5. Click **New**.
6. Configure the search rule fields as follows:

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

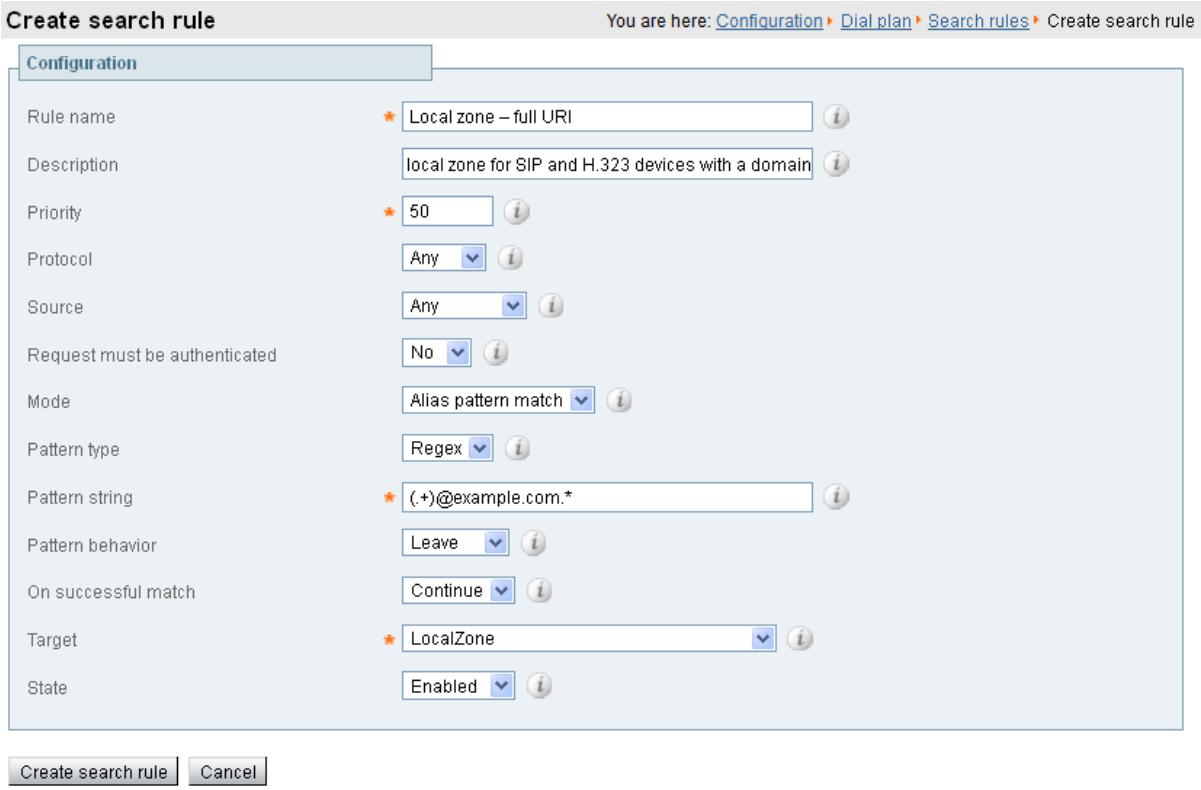
7. Click **Create search rule**.



8. Click **New**.
9. Configure the search rule fields as follows:

	VCS Control	VCS Expressway
Rule name	Enter `Local zone – full URI`	Same as VCS Control
Description	Enter `Search local zone for SIP and H.323 devices with a domain`	
Priority	Enter `50`	
Protocol	*Any*	
Source	*Any*	
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	*LocalZone*	
State	*Enabled*	

10. Click **Create search rule**.



Task 9: 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.
- The VCS Control is configured with a traversal client zone, and the VCS Expressway with a traversal server zone.

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 `Traversal zone`	Enter `Traversal zone`
Type	*Traversal client*	*Traversal server*
Username	Enter `exampleauth`	Enter `exampleauth`
Password	Enter `ex4mpl3.c0m`	Not applicable
H.323 Mode	*On*	*On*

	VCS Control	VCS Expressway
H.323 Protocol	*Assent*	*Assent*
H.323 Port	Enter `6001`	Enter `6001`
H.323 H.460.19 demultiplexing mode	Not applicable	*Off*
SIP Mode	*On*	*On*
SIP Port	Enter `7001`	Enter `7001`
SIP Transport	*TLS*	*TLS*
SIP TLS verify mode	*Off*	*Off*
SIP Accept proxied registrations	*Allow*	*Allow*
Location Peer 1 address	Enter `192.0.2.2`	Not applicable

4. Click **Create zone**.

Create zone

You are here: Configuration ▸ Zones ▸ Zones ▸ Create zone

Configuration

Name *	TraversalZone
Type *	Traversal client
Hop count *	15

Connection credentials

Username *	exampleauth
Password *	••••••••••••

H.323

Mode	On
Protocol	Assent
Port *	6001

SIP

Mode	On
Port *	7001
Transport	TLS
TLS verify mode	Off
Accept proxied registrations	Allow
Media encryption mode	Auto
ICE support	Off
Poison mode	Off

Authentication

Authentication policy	Do not check credentials

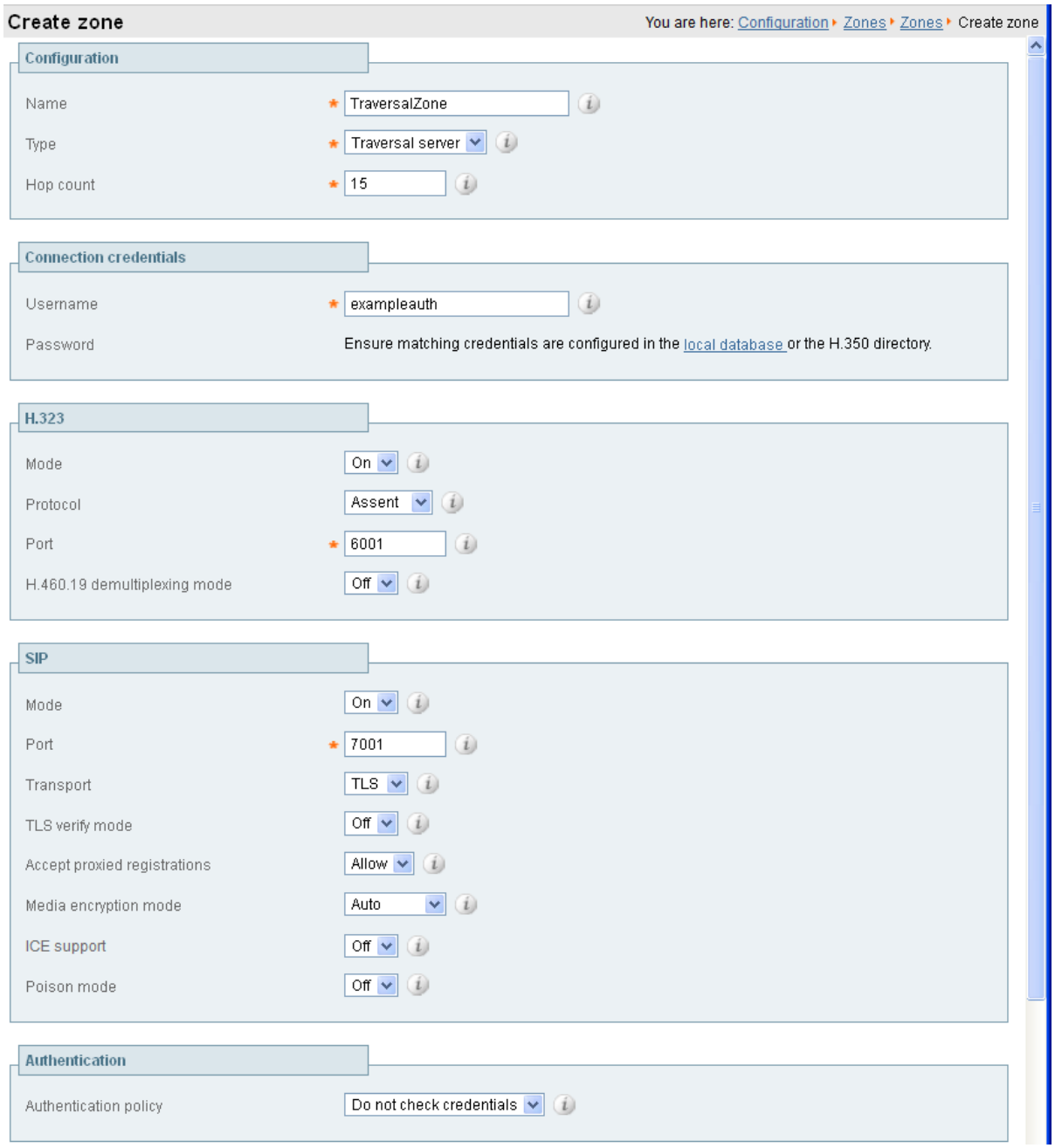
Client settings

Retry interval *	120

Location

Peer 1 address	192.0.2.2

VCS Control



VCS Expressway

To configure the authentication credentials in the **Local authentication database** (which are configured in the VCS Expressway only):

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

3. Configure the fields as follows:

	VCS Control	VCS Expressway
Name	Not applicable	Enter `exampleauth`
Password	Not applicable	Enter `ex4mpl3.c0m`

4. Click **Create credential**.

Configuring traversal zones for Unified Communications

To support Unified Communications features such as mobile and remote access or Jabber Guest, there must be a secure traversal zone connection between the VCS Control and the 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 a VCS Control, or a traversal server zone when selected on a 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.

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 IP addresses in these fields. If you use FQDNs instead, each FQDN must be different and must resolve to a single IP address for each peer.
- 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 10: Configuring traversal zone search rules

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

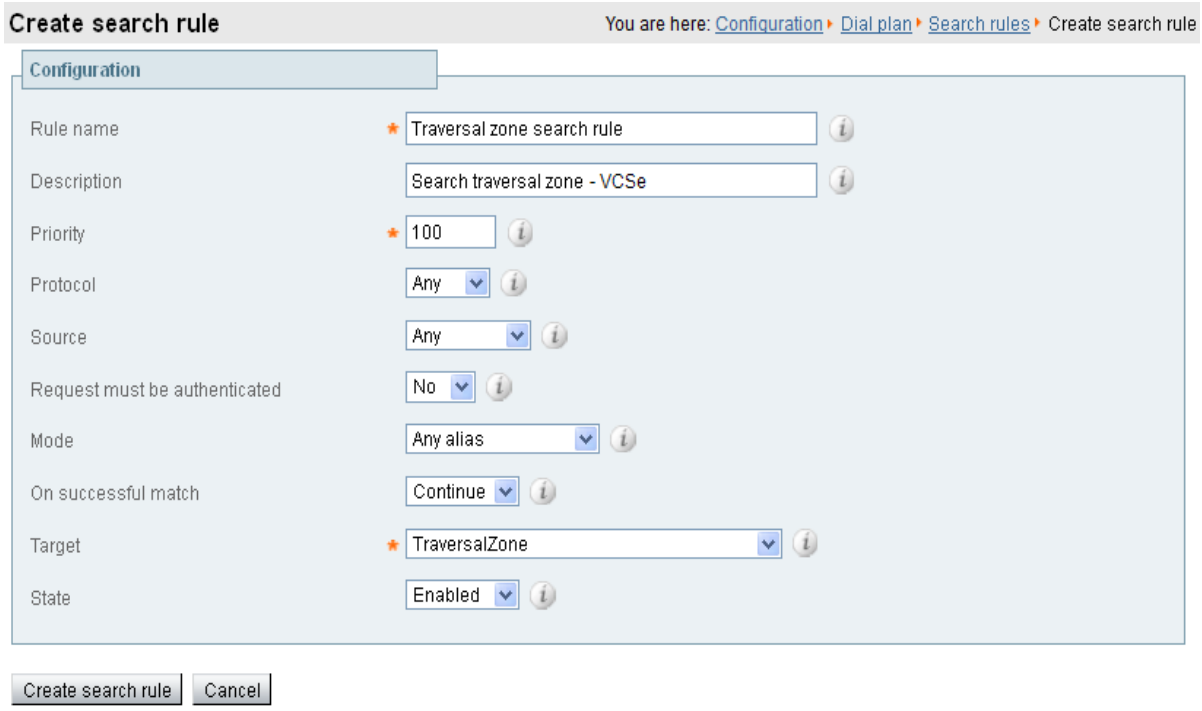
1. Go to **Configuration > Dial plan > Search rules**.
2. Click **New**.
3. Configure the fields as follows:

	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	*Any*	*Any*
Source	*Any*	*Any*
Request must be authenticated	*No*	*No*
Mode	*Any alias*	*Any alias**
On successful match	*Continue*	*Continue*
Target	*Traversal zone*	*Traversal zone*

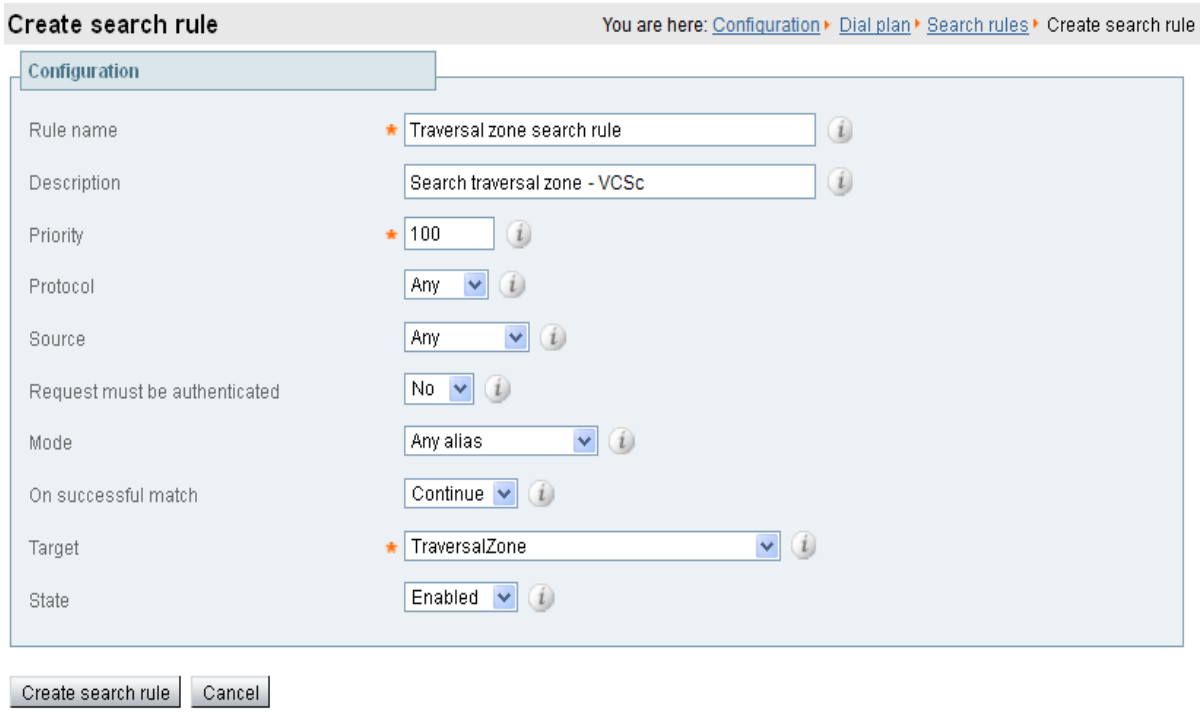
	VCS Control	VCS Expressway
State	*Enabled*	*Enabled*

* 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**.



VCS Control



VCS Expressway

Task 11: Configuring the DNS zone

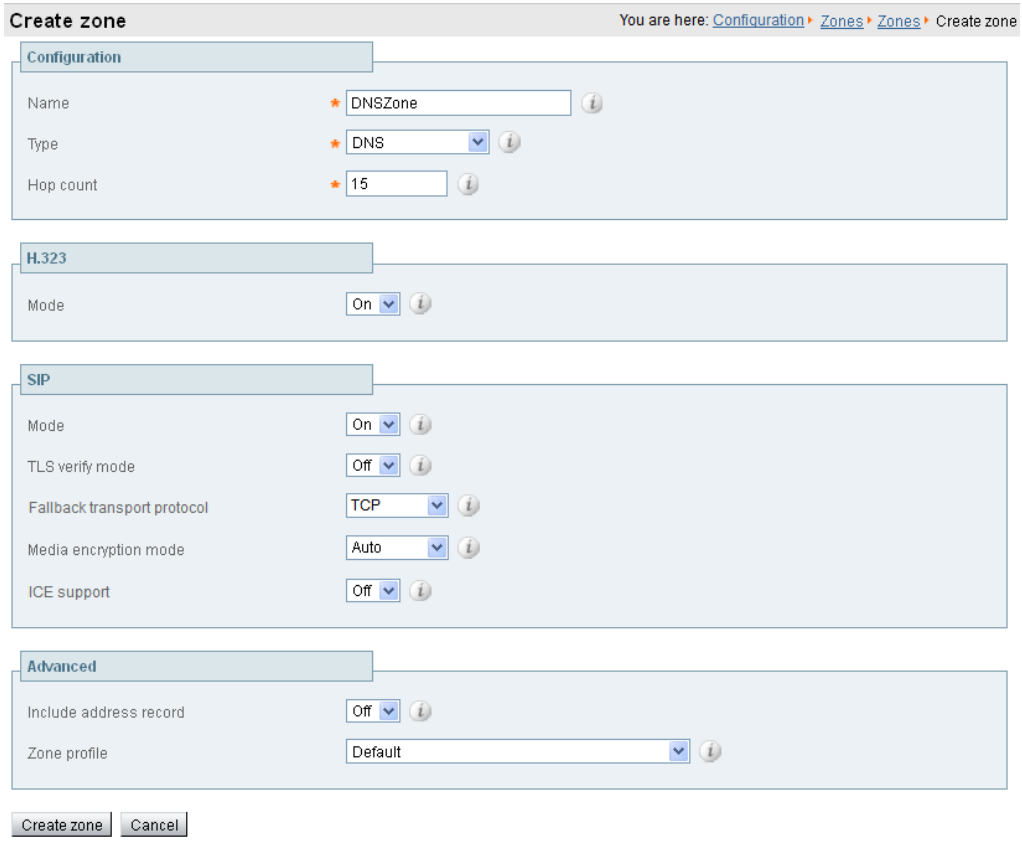
The DNS zone is used to search for externally hosted systems (which are not locally registered, such as for business to business calling). Destination aliases are searched for by a name using a DNS lookup.

To configure the DNS zone:

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

Field name	Value on VCS Control	Value on VCS Expressway
Name	Not applicable	Enter `DNSZone` for example
Type	Not applicable	*DNS*
H.323 Mode	Not applicable	*On*
SIP Mode	Not applicable	*On*
Fallback transport protocol	Not applicable	*TCP*
Include address record	Not applicable	*Off*

4. Click **Create zone**.



Task 12: Configuring DNS zone search rules

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

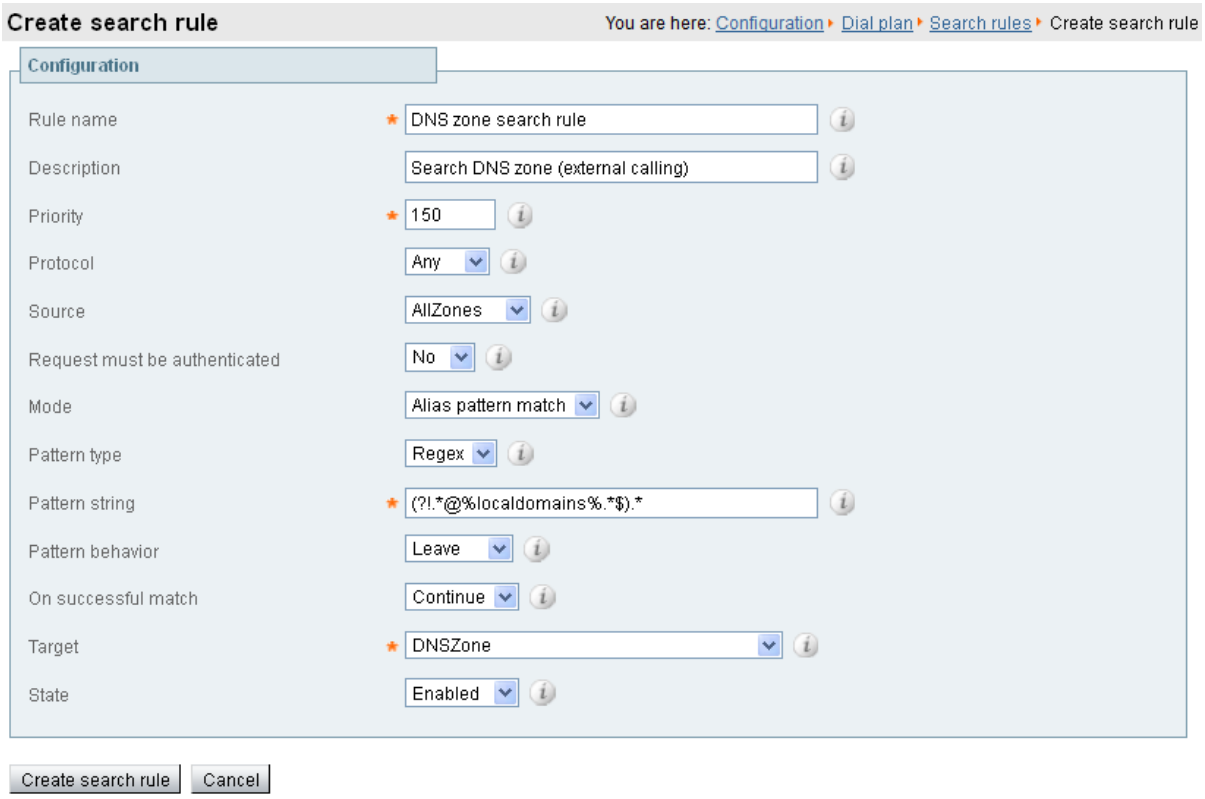
A specific regular expression is configured which will prevent searches being made using the DNS zone (i.e. on the public internet) for destination addresses (URIs) using any SIP domains which are configured on the local network (local domains).

To create the search rules to route via DNS:

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

Field name	Value on VCS Control	Value on VCS Expressway
Rule name	Not applicable	Enter `DNS zone search rule` for example
Description	Not applicable	Enter `Search DNS zone (external calling)` for example
Priority	Not applicable	`150`
Protocol	Not applicable	*Any*
Source	Not applicable	*All zones*
Request must be authenticated	Not applicable	*No*
Mode	Not applicable	*Alias pattern match*
Pattern type	Not applicable	*Regex*
Pattern string	Not applicable	Enter `(?!.*@%localdomains%.*$).*`
Pattern behavior	Not applicable	*Leave*
On successful match	Not applicable	*Continue*
Target	Not applicable	*DNSZone*
State	Not applicable	*Enabled*

4. Click **Create search rule**.



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

(.*) = match all pattern strings

(?!.*@%localdomains%.*$).* = do not match any pattern strings ending in @localdomains

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 13: 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.

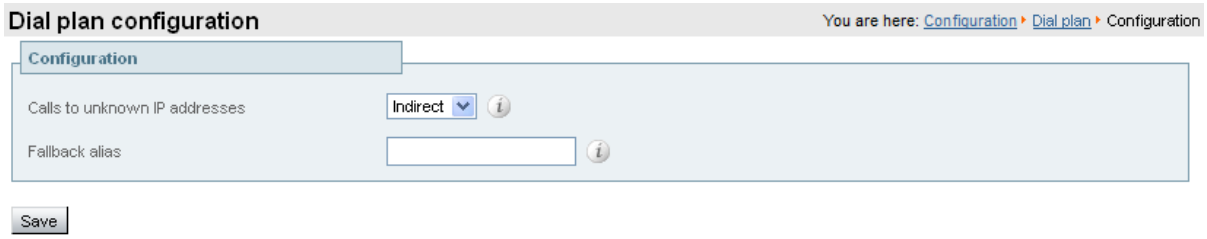
- All requests destined for external IP addresses, originating at the VCS Control are routed to the VCS Expressway using a search rule.
- The VCS Expressway then attempts to open a connection directly to the IP address.

To configure how the VCS will handle calls to unknown IP addresses:

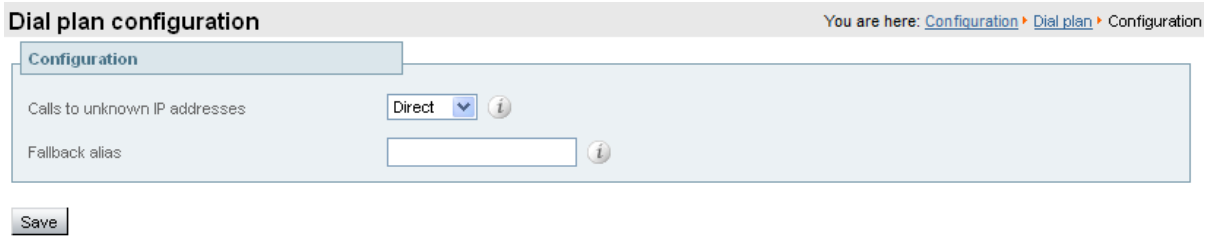
1. Go to **Configuration > Dial plan > Configuration**.
2. Configure the fields as follows:

	VCS Control	VCS Expressway
Calls to unknown IP addresses	*Indirect*	*Direct*

3. Click **Save**.



VCS Control



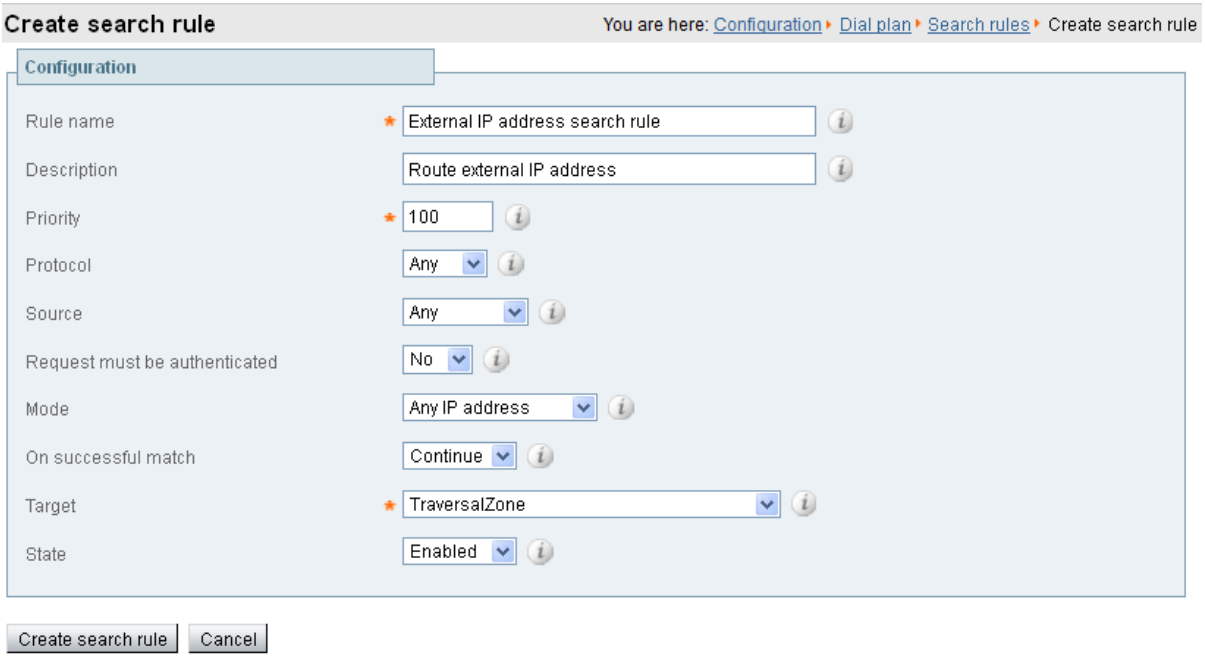
VCS Expressway

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**.
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	*Traversal Zone*	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
Create search rule
Cancel

Endpoint registration

There are three endpoints shown in the example network configuration diagram.

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

Following the system configuration, endpoint registration should be possible using the following 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

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 via **Configuration > Zones > Zones**.

If the traversal zone is not active:

- Review the traversal zone configuration.
- Confirm 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 [p.52]).
- Confirm 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 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?
- Review the SIP domains (Task 6: Configuring SIP domains [p.14]).
- Review any registration restriction configuration applied to the VCS (optional, see Task 16: Configuring registration restriction policy (optional) [p.38]).

Home endpoints may fail to register when using SRV records in some instances: if the endpoint is using the home router for its DNS server (this also applies to the DNS server being used by a PC when Jabber Video is running on it) and the DNS server software on the router does not support look up of SRV records.

In this case there are two alternatives:

- Change the DNS server on the endpoint to use a publicly available DNS server (for example Google – 8.8.8.8) which can resolve SRV record lookups.

or

- Change the SIP/H.323 server address on the endpoint to use the FQDN of one of the nodes in the VCS cluster, rather than the SRV record of the cluster; the device will now perform 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**).

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 14: Configuring Cisco TMS (optional)

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

Further configuration tasks are required on Cisco TMS to fully integrate the VCS with the Cisco TMS server – see *Cisco TMS Administrator Guide*.

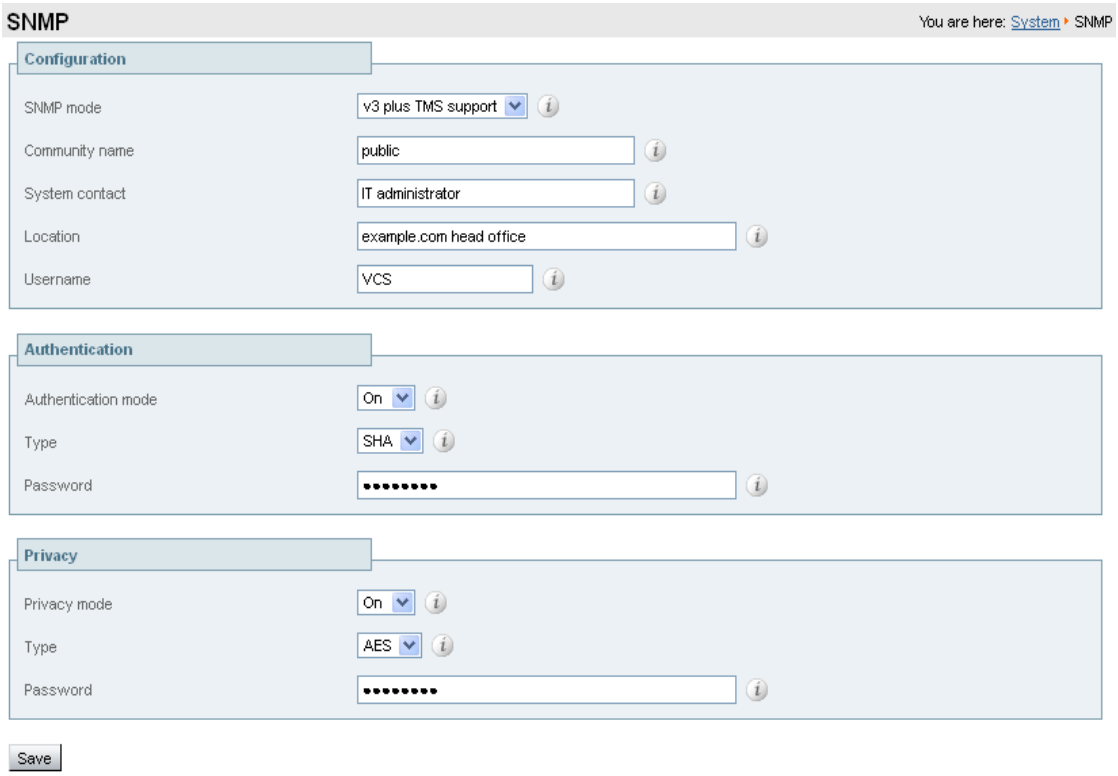
- Enabling SNMP speeds up the VCS - Cisco TMS integration process but is not essential.
- VCS Expressway integration with Cisco TMS requires additional firewall / NAT configuration – See Appendix 3: Firewall and NAT settings [p.52] (VCS Expressway needs to access port 80/443 on Cisco TMS from outside the firewall).

To enable and configure SNMP:

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

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

3. Click **Save**.



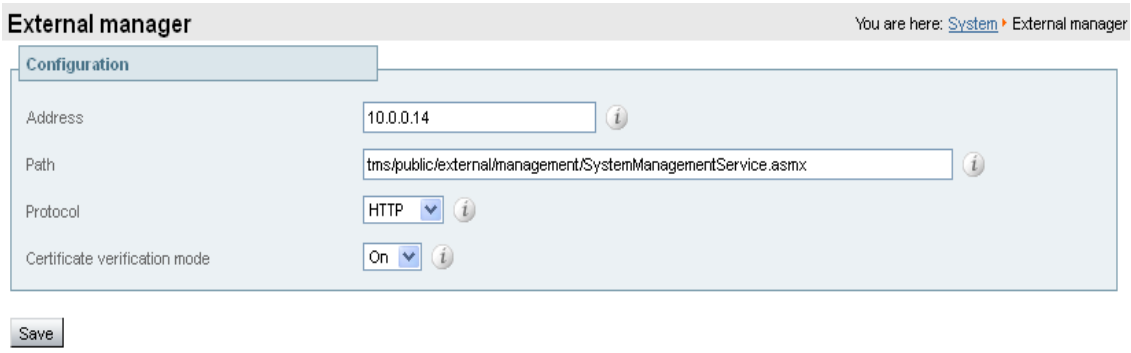
To configure the necessary external manager (Cisco TMS) parameters:

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 *HTTP* or *HTTPS*	
Certificate verification mode	Select *On* or *Off* (see Note below)	

Note that the certificate is only verified if the value is *On* and the protocol is set to *HTTPS*. If you switch this on then Cisco TMS and VCS must have appropriate certificates.

3. Click **Save**.



Task 15: Configuring logging (optional)

The following configuration will enable event logs to be sent to an external logging server (using the SYSLOG protocol).

- The **Log level** controls the granularity of event logging. 1 is the least verbose, 4 the most.
- A minimum log level of 2 is recommended, as this level provides both system and basic signaling message logging.

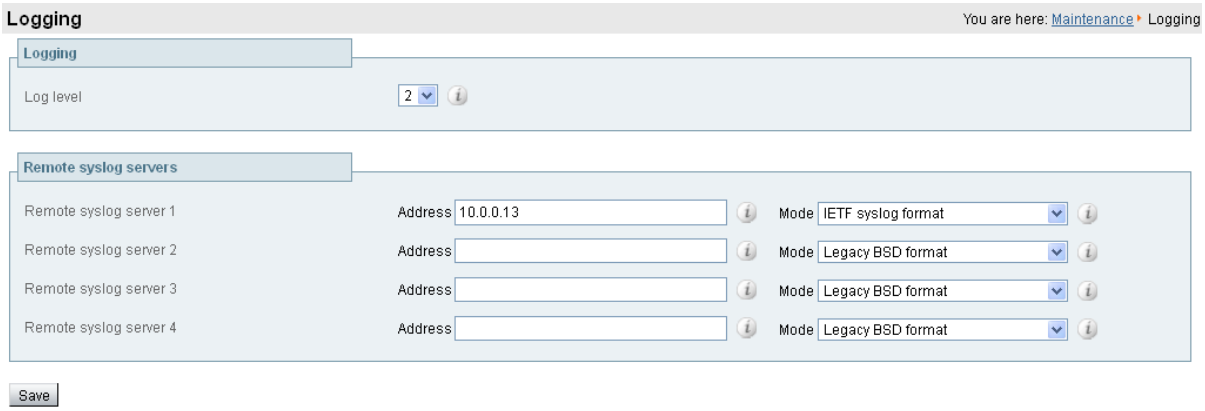
VCS Expressway external logging server configuration requires additional firewall / NAT configuration – See Appendix 3: Firewall and NAT settings [p.52].

To configure a logging server:

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

	VCS Control	VCS Expressway
Log level	*2*	*2*
Remote syslog server 1: Address	Enter `10.0.0.13`	Enter `10.0.0.13`
Remote syslog server 1: Mode	*IETF syslog format*	*IETF syslog format*

3. Click **Save**.



Task 16: Configuring registration restriction policy (optional)

The aliases that endpoints can register can be limited using either an Allow list or a Deny list.

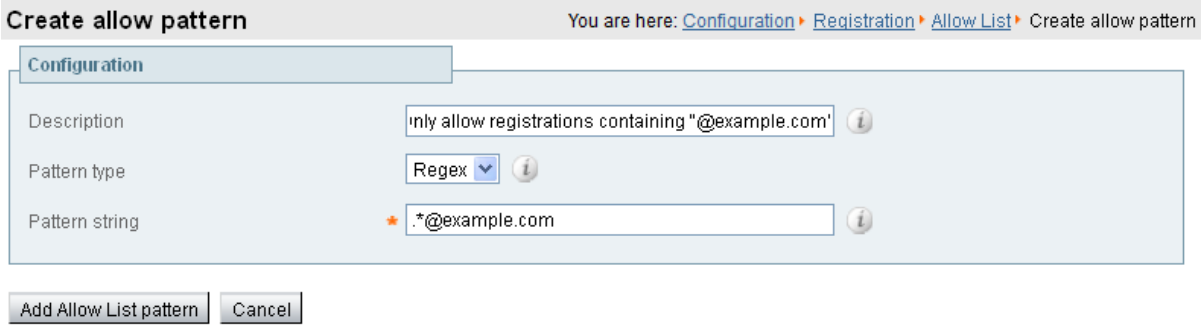
The following configuration will limit registrations (on both VCS Control and VCS Expressway) to endpoints which register with an identity that contains “@example.com”.

To configure Allow List registration restrictions:

1. Go to **Configuration > Registration > Allow List**.
2. Click **New**.
3. Create an allow pattern by configuring the fields as the follows:

	VCS Control	VCS Expressway
Description	Enter `Only allow registrations containing "@example.com"`	Same as VCS Control
Pattern type	*Regex*	
Pattern string	Enter `.*@example.com`	

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

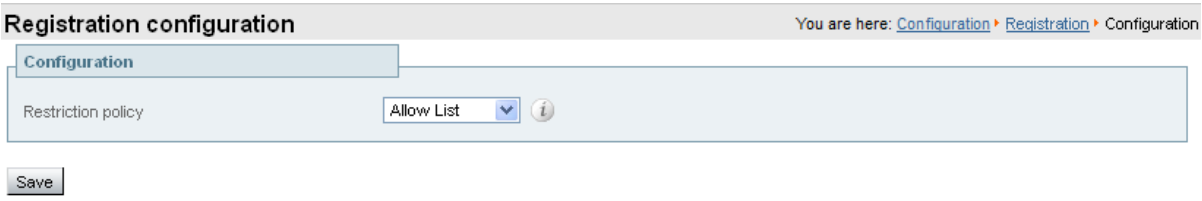


To activate the registration restriction:

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

	VCS Control	VCS Expressway
Restriction policy	*Allow List*	*Allow List*

3. Click **Save**.



Task 17: 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 either *Check credentials*, *Do not check credentials*, or *Treat as authenticated*.

- Registration authentication is controlled by the Default Subzone (or relevant alternative subzone) configuration.
- 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:

- 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 18: Restricting access to ISDN gateways (optional)

VCS users are recommended to take appropriate action to restrict unauthorized access to any ISDN gateway resources (also known as toll-fraud prevention). This optional step shows some methods in which this can be achieved.

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

VCS Expressway

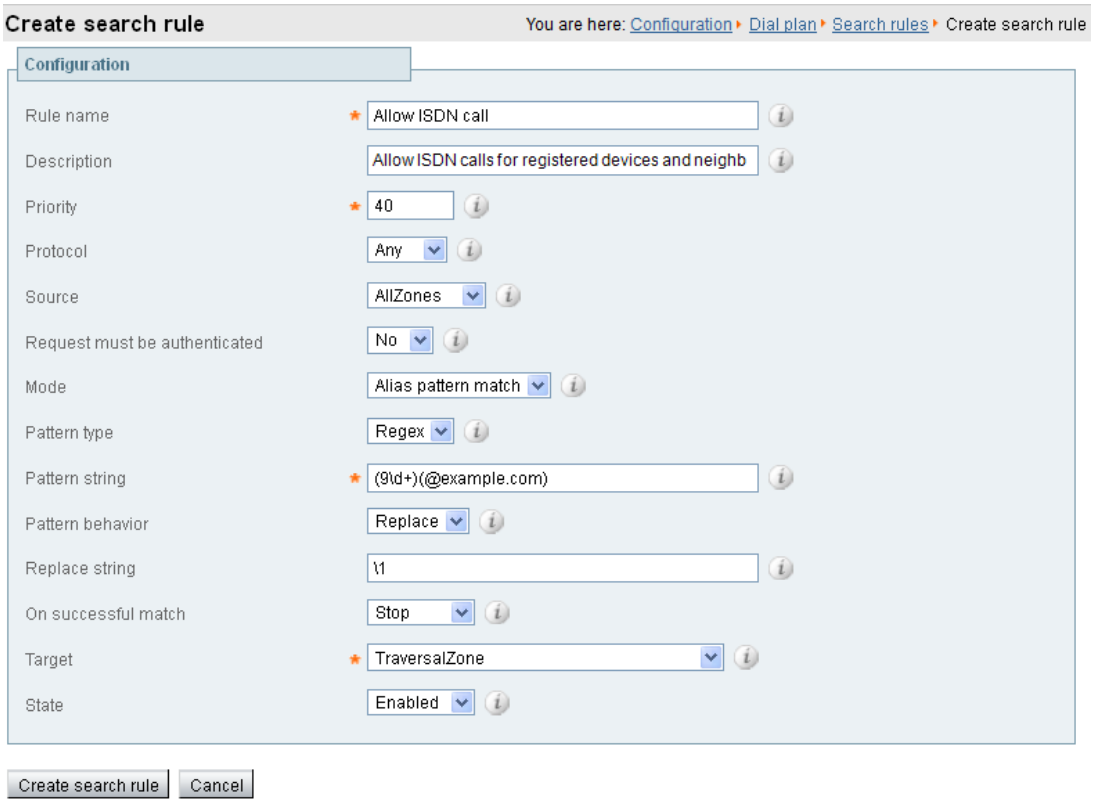
Two search rules are created on the VCS Expressway:

- both search rules have a pattern string that matches calls directed at the ISDN gateway — in this example, calls that are prefixed by a 9
- the first rule has a **Source** of *All zones*; this allows calls from registered endpoints and neighbor zones to be passed through to the traversal zone
- the second rule is similar to the first rule but has a **Source** of *All*; this means that non-registered endpoints (which are excluded from the previous rule) are included by this rule and 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**.
3. Configure the fields as follows:

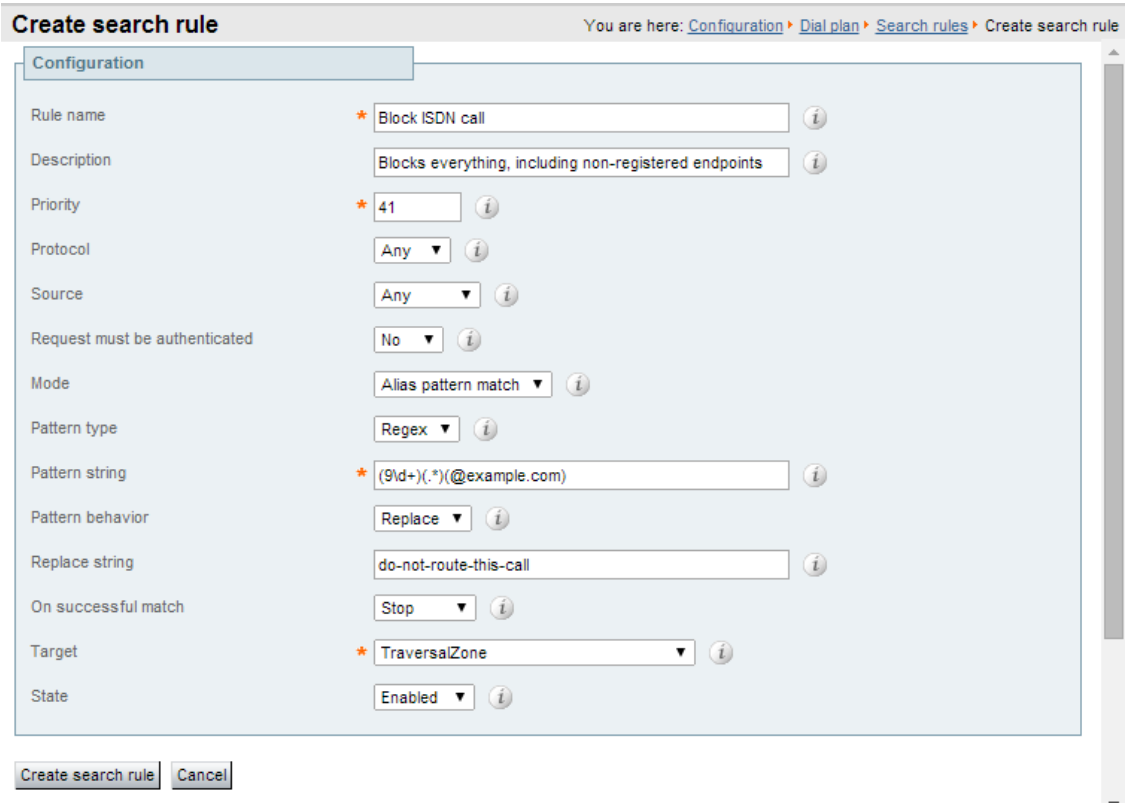
	VCS Expressway
Rule name	Enter `Allow ISDN call` for example
Description	Enter `Allow ISDN calls for registered devices and neighbors`
Priority	Enter `40` (these rules must be the highest priority in the search rule configuration)
Protocol	*Any*
Source	*All zones*
Request must be authenticated	*No*
Mode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



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

6. Configure the fields as follows:

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



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
☐	40	✔ Enabled	Allow ISDN call	Any	AllZones	No	Alias pattern match	Regex	(9\d+)(@example.com)	Replace	Stop	TraversalZone	View/Edit
☐	41	✔ Enabled	Block ISDN call	Any	Any	No	Alias pattern match	Regex	(9\d+)(@example.com)	Replace	Stop	TraversalZone	View/Edit
☐	50	✔ Enabled	LocalZoneMatch	Any	Any	No	Any alias				Continue	LocalZone	View/Edit

VCS Control

This example shows how to configure the VCS Control to stop calls coming in via the gateway from being able to route calls back out of the gateway. This is done by loading some specially constructed CPL onto the VCS Control and configuring its **Call policy mode** to use *Local CPL*.

Creating a CPL file

The CPL file to be uploaded onto the VCS can be created in a text editor.

Here are 2 example sets of CPL. In these examples:

- “GatewayZone” is the neighbour 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 will not ring devices that use the gateway – for example, calls forwarded to a mobile phone will be disallowed

This example CPL excludes any checking of whether the calling party is authenticated or not:

```
<?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 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:

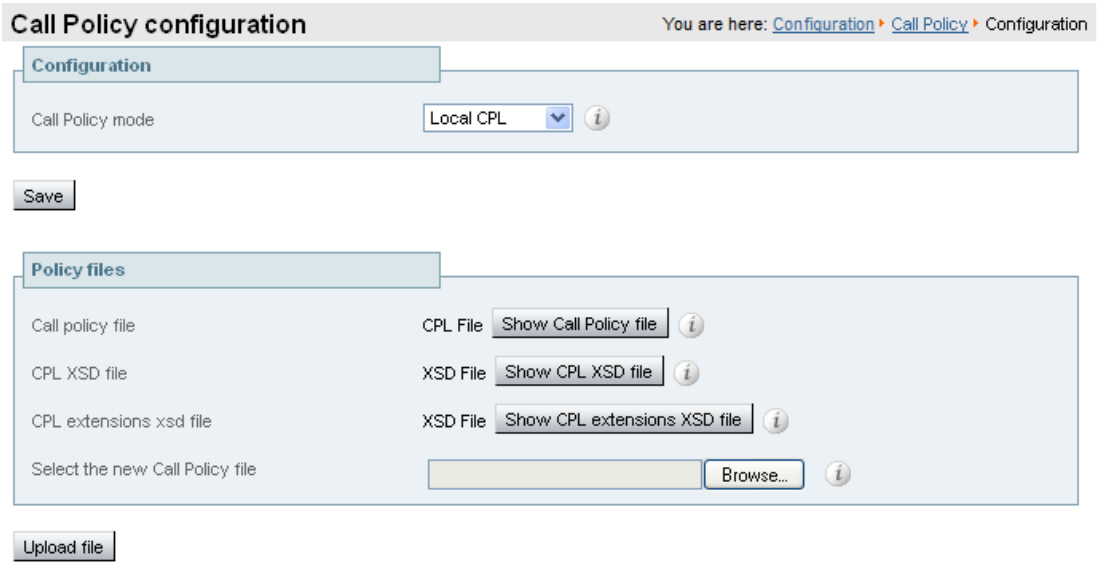
```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
```

```
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:

1. Go to **Configuration > Call Policy > Configuration**.
2. Click **Browse...** and select your CPL file (created above) from your file system.
3. Click **Upload file**.
   - You should receive a "File upload successful" message.
   - If you receive an "XML invalid" message then you must 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
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	VCSc	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
Priority	100	Configuration > Dial plan > Search rules

Configuration item	Value	VCS page
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		
Zone Name	TraversalZone	Configuration > Zones > Zones

Configuration item	Value	VCS page
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	((?!*@%localdomains%$).*)	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

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 to allow:

- 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 VM server 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.

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 *

* 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 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
H.323 endpoints registering with public IP addresses							

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
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)							
DNS	VCSe	DNS server	192.0.2.2	>=1024	UDP	DNS servers	53

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
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

This section discusses network deployments that use static NAT or Dual Network Interface architectures.

Prerequisites

Deploying a VCS Expressway behind a NAT **mandates** the use of the **Advanced Networking** option key. It enables the static NATing functionality of the VCS Expressway as well as dual network interfaces. Although certain call scenarios involving a VCS Expressway behind NAT could potentially work with the help of router/firewall-based ALGs, proper functionality cannot be guaranteed; you must use the VCS to perform the static NATing on its own interface. More background on this can be found in the Routers/firewalls with SIP/H.323 ALG [p.60] section later in this appendix.

When deploying a VCS Expressway behind a NAT with static NAT configuration in place on the VCS Expressway, it is highly recommended to disable SIP and H.323 ALGs (SIP / H.323 awareness) on routers/firewalls carrying network traffic to or from the VCS Expressway (experience shows that these tend to be unable to handle video traffic properly).

Although the **Advanced Networking** option is available for both the VCS Expressway and VCS Control, only the VCS Expressway supports static NAT.

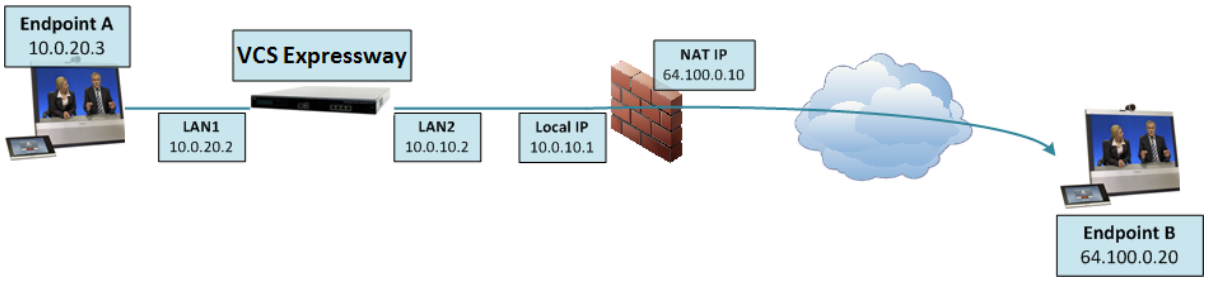
Background

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:



- 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
- 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):

```
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
…
…
…
```

Figure 3: SIP INVITE arriving at NAT router

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:

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

v=0
s=-
c=IN IP4 10.0.10.2

b=AS:2048
…
…
…
```

Figure 4: SIP INVITE arriving at Endpoint B

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.

Solution

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).

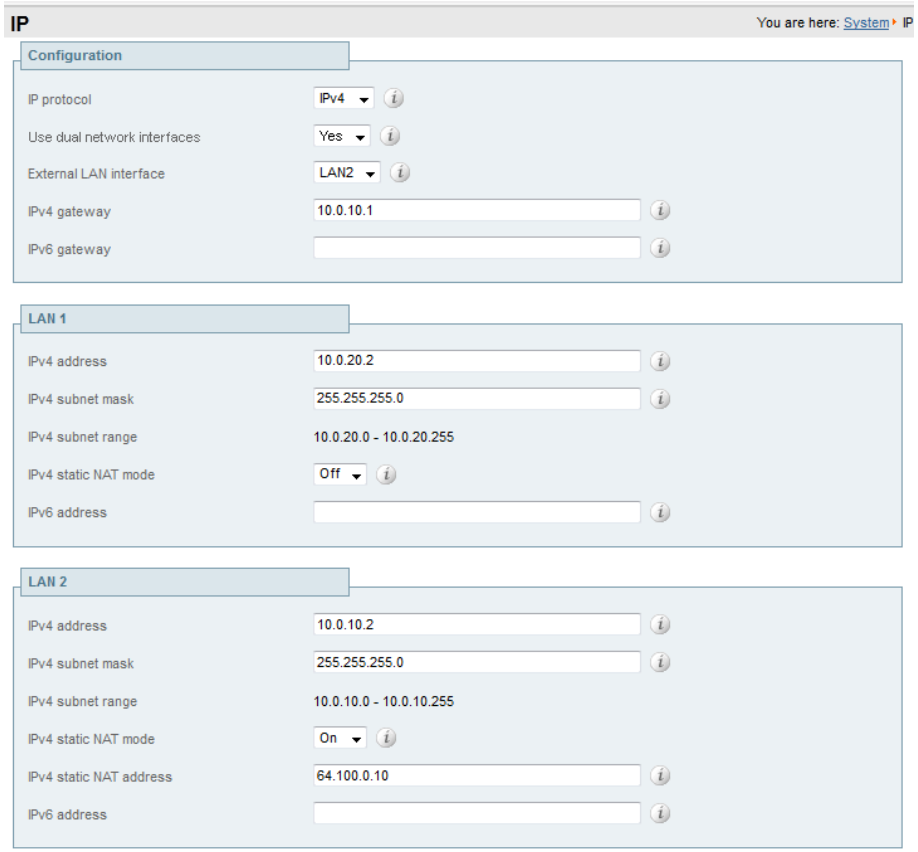
This can be achieved by enabling **Static NAT mode** on selected network interfaces on the VCS Expressway. The Static NAT mode feature on the VCS Expressway is made available with the **Advanced Networking** option key.

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. It is not compulsory to use both interfaces; you may use only a single interface and have Static NAT mode enabled on that.

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.

Using the example deployment above, the VCS Expressway would be configured as follows:



- 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 an IP address of 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:

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

v=0
s=-
c=IN IP4 64.100.0.10

b=AS:2048
…
…
…
```

Figure 5: SIP INVITE arriving at Endpoint B - Static NAT mode enabled

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.

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 recommendations in the Introduction section of this appendix, it is highly recommended to disable SIP and H.323 ALGs on routers/firewalls carrying network traffic to or from a VCS Expressway, as, when enabled this 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 [p.52].

General guidelines and design principles

With VCS Expressway deployments involving NAT and/or dual network interfaces, some general guidelines and principles apply, as described below.

Non-overlapping subnets

If the VCS Expressway will be configured to use 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 clustering VCSs that have the **Advanced Networking** option installed, cluster peers have to be addressed with their LAN1 interface address. In addition, clustering must be configured on an interface that does not have **Static NAT mode** enabled.

We therefore recommend that you use LAN2 as the externally facing interface, and that LAN2 is used as the static NAT interface where applicable.

External LAN interface setting

The **External LAN interface** configuration setting on the **IP** configuration page controls on which network interface TURN relays are allocated. In a dual network interfaces VCS Expressway configuration, this should normally be set to the externally-facing LAN interface on the VCS Expressway.

Dual network interfaces

The following diagram shows an example deployment involving the use of a VCS Expressway with dual network interfaces and static NAT, a VCS Control acting as a traversal client, and two firewalls/routers. Typically in this DMZ configuration, FW A cannot route traffic to FW B, and devices such as the dual interface VCS Expressway are required to validate and forward traffic from FW A's subnet to FW B's subnet (and vice versa).

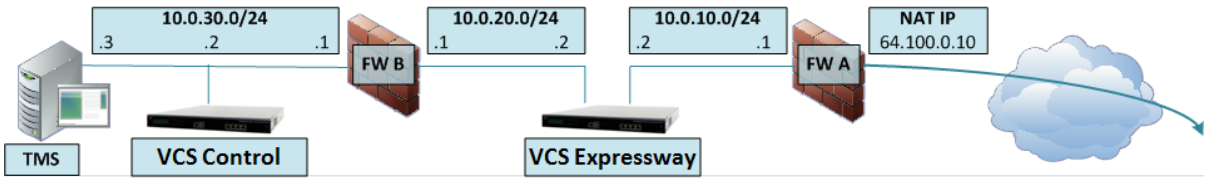


Figure 6: Dual network interfaces deployment

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 publicly-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

With a deployment such as that shown in Figure 6, the VCS Expressway should be configured with a default gateway address of 10.0.10.1. This means that all traffic sent out via LAN2 will by default be sent to the IP address 10.0.10.1.

If Firewall B is doing NAT for traffic sent from the 10.0.30.0 subnet to the LAN1 interface of the VCS Expressway (for example traversal client traffic from VCS Control or management traffic from TMS), this means that this traffic will appear as coming from the external interface of firewall B (10.0.20.1) as it reaches LAN1 of the VCS Expressway. The VCS Expressway will therefore be able to reply to this traffic via its LAN1 interface, since the apparent source of that traffic is located on the same subnet.

If firewall B is not doing NAT however, traffic sent from the VCS Control to LAN1 of the VCS Expressway will appear as coming from 10.0.30.2. If the VCS does not have a static route added for the 10.0.30.0/24 subnet, it will send replies for this traffic to its default gateway (10.0.10.1) out from LAN2, as it has not been told that the 10.0.30.0/24 subnet is located behind the 10.0.20.1 firewall. Therefore, a static route needs to be added, using the **`xCommand RouteAdd`** CLI command, which is run from an admin SSH shell on the VCS.

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.

If firewall B is not doing NAT and the VCS Expressway needs to communicate with devices in subnets other than 10.0.30.0 which are also located behind firewall B (for example for communicating with management stations for HTTPS and SSH management or for reaching network services such as NTP, DNS, LDAP/AD and syslog servers), static routes will also have to be added for these devices/subnets.

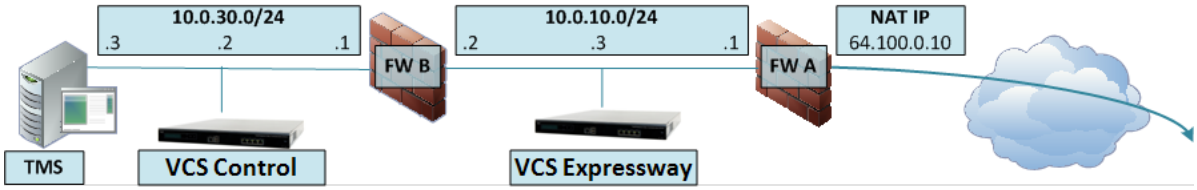
The **`xCommand RouteAdd`** command and syntax is described in full detail in *VCS Administrator Guide*.

Example deployments

The following section contains additional reference designs which depict other possible deployment scenarios.

Single subnet DMZ using single VCS Expressway LAN interface

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.



This deployment consists of:

- a single subnet DMZ – 10.0.10.0/24, containing:
  - the internal interface of firewall A – 10.0.10.1
  - the external interface of firewall B – 10.0.10.2
  - the LAN1 interface of the VCS Expressway – 10.0.10.3
- a 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 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 theVCS Expressway. **Static NAT mode** has been 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.

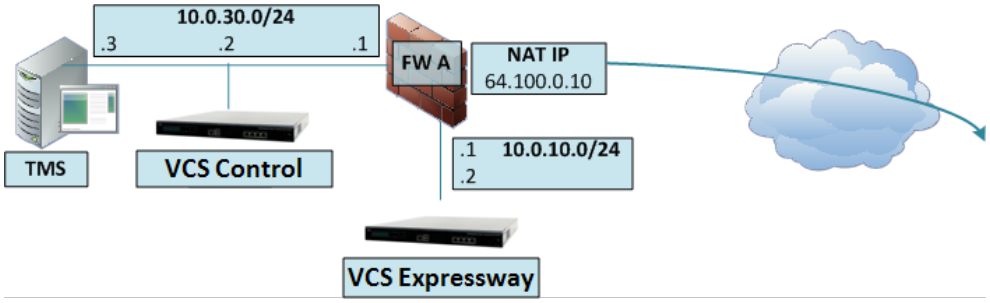
So, in this example, firewall A must allow NAT reflection of traffic coming from the VCS Control that is destined for the external address, that is 64.100.0.10, of the VCS Expressway. The traversal zone on the VCS Control must have 64.100.0.10 as the peer address.

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 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 via 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, this will mean that asymmetric routing will occur and this may or may not work, depending on the firewall capabilities.

The VCS Expressway can be added to Cisco TMS with the IP address 10.0.10.3 (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.

3-port firewall DMZ using single VCS Expressway LAN interface



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

- a DMZ subnet (10.0.10.0/24), containing:
  - the DMZ interface of firewall A - 10.0.10.1
  - the LAN1 interface of the VCS Expressway - 10.0.10.2
- a LAN subnet (10.0.30.0/24), containing
  - the LAN interface of firewall A - 10.0.30.1
  - the LAN1 interface of the VCS Control – 10.0.30.2
  - the 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 has been enabled for LAN1 on the VCS Expressway, with a static NAT address of 64.100.0.10.

TheVCS 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.

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 those described in the previous example deployment, "Single subnet DMZ using single VCS Expressway LAN interface".

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.

Technical support

If you cannot find the answer you need in the documentation, check the website at www.cisco.com/cisco/web/support/index.html where you will be able to:

- Make sure that you are running the most up-to-date software.
- Get help from the Cisco Technical Support team.

Make sure you have the following information ready before raising a case:

- Identifying information for your product, such as model number, firmware version, and software version (where applicable).
- Your contact email address or telephone number.
- A full description of the problem.

To view a list of Cisco TelePresence products that are no longer being sold and might not be supported, visit: www.cisco.com/en/US/products/prod_end_of_life.html and scroll down to the TelePresence section.

Document revision history

Date	Description
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.