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

Deployment Guide

Cisco VCS X7.2

January 2015

Contents

Introduction

The Cisco TelePresence Video Communication Server (VCS) can be deployed as a VCS Control application or as a VCS Expressway™ application.

The VCS Expressway enables business to business communications, empowers remote and home based workers, and gives service providers the ability to provide video communications to customers. The VCS Control provides SIP proxy and call control as well as H.323 gatekeeper services within an organization's corporate network environment.

By combining VCS Expressway and VCS Control products a sophisticated and secure video network solution can be deployed by an organization enabling internal and external video communications.

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 steps 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 lists the configuration details used to configure the VCSs in the example network deployment.
- Appendix 2 includes details of the DNS records required for the system deployment to work as expected.
- Appendix 3 includes details of NAT and firewall configurations required for the system to deployment to work as expected. This document describes a small subset of the numerous NAT and firewall deployment options, made possible using the VCS Expressway dual network interface and NAT features.
- Appendix 4 explains how to deploy your system with a static NAT and Dual Network Interface architecture.

Descriptions of system configuration parameters can be found in the *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 VCSs running Device Provisioning 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*

These documents can be found at: http://www.cisco.com/cisco/web/support/index.html

Example network deployment

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

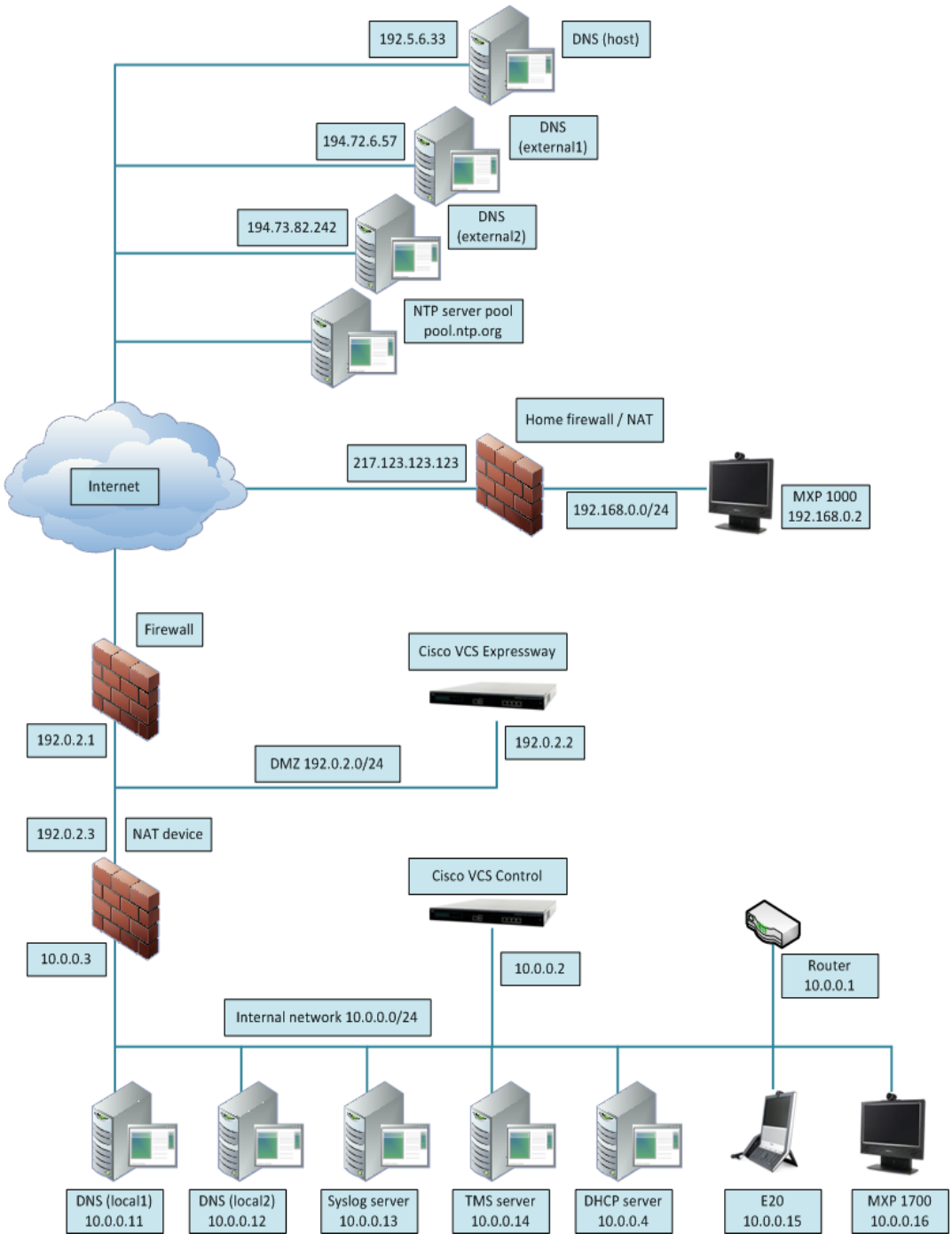


Figure 1: Example network deployment

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

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.

E20 and MXP1700

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).

Syslog server

A logging server for Syslog messages (see Logging server configuration (optional) [p.40]).

Cisco TMS server

A management and scheduling server (see Cisco TMS configuration (optional) [p.37]).

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 road warriors 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

MXP1000

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 configuration [p.54].
- Home firewall NAT (PAT) device which performs port address and firewall functions for network traffic originating from the MXP1000 device.
- See Appendix 4 – Static NAT and Dual Network Interface architectures [p.58] 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 endpoint registered to the internal and external infrastructure (VCS Control and VCS Expressway).

The DNS SRV configurations are described in Appendix 2 – DNS records configuration [p.52].

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)
- a VCS Control running version X5 or later
- 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 configuration [p.52])
- NAT & firewall configuration (see Appendix 3 – Firewall and NAT configuration [p.54])
- DHCP server configuration (not described in this document)

Summary of process

The configuration process consists of the following steps.

VCS system configuration:

Routing configuration:

Optional configuration steps:

Cisco VCS system configuration

Step 1: Initial configuration

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

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

Note that VCSs require static IP addresses (they 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
- 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

Step 2: System name configuration

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 unit (so that you can identify it when it is in a rack with other systems). The system name is also used by Cisco TMS.

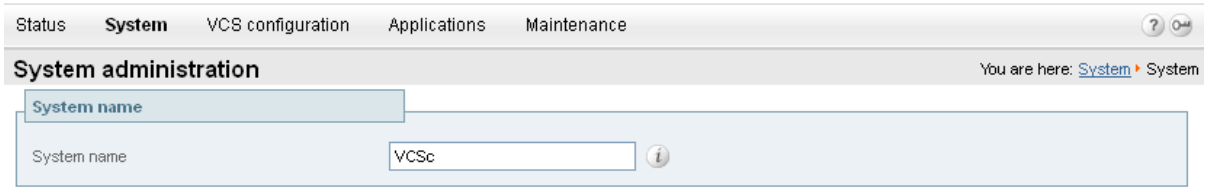
You are recommended to give the VCS a name that allows you to easily and uniquely identify it. If the system name is longer than 16 characters, only the last 16 characters will be shown in the display on the front panel.

To configure the **System name**:

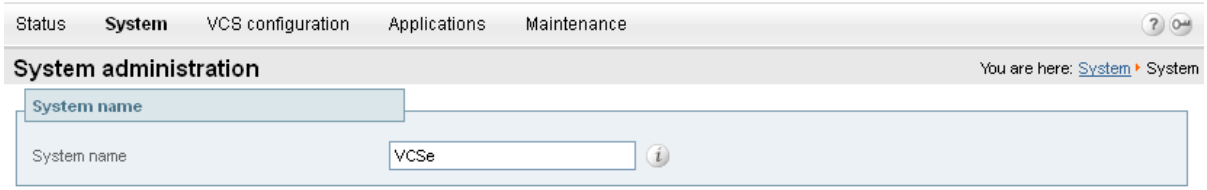
1. Go to the **System administration** page (**System > System**).
2. Configure the **System name** as follows:

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

3. Click **Save**.



VCS Control



VCS Expressway

Step 3: DNS configuration

Local host name

The **Local 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 <**Local host name**>.<**Domain name**> = FQDN of this VCS.

To configure the **Local host name**:

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

	VCS Control	VCS Expressway
Local 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 the **DNS** page (**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.

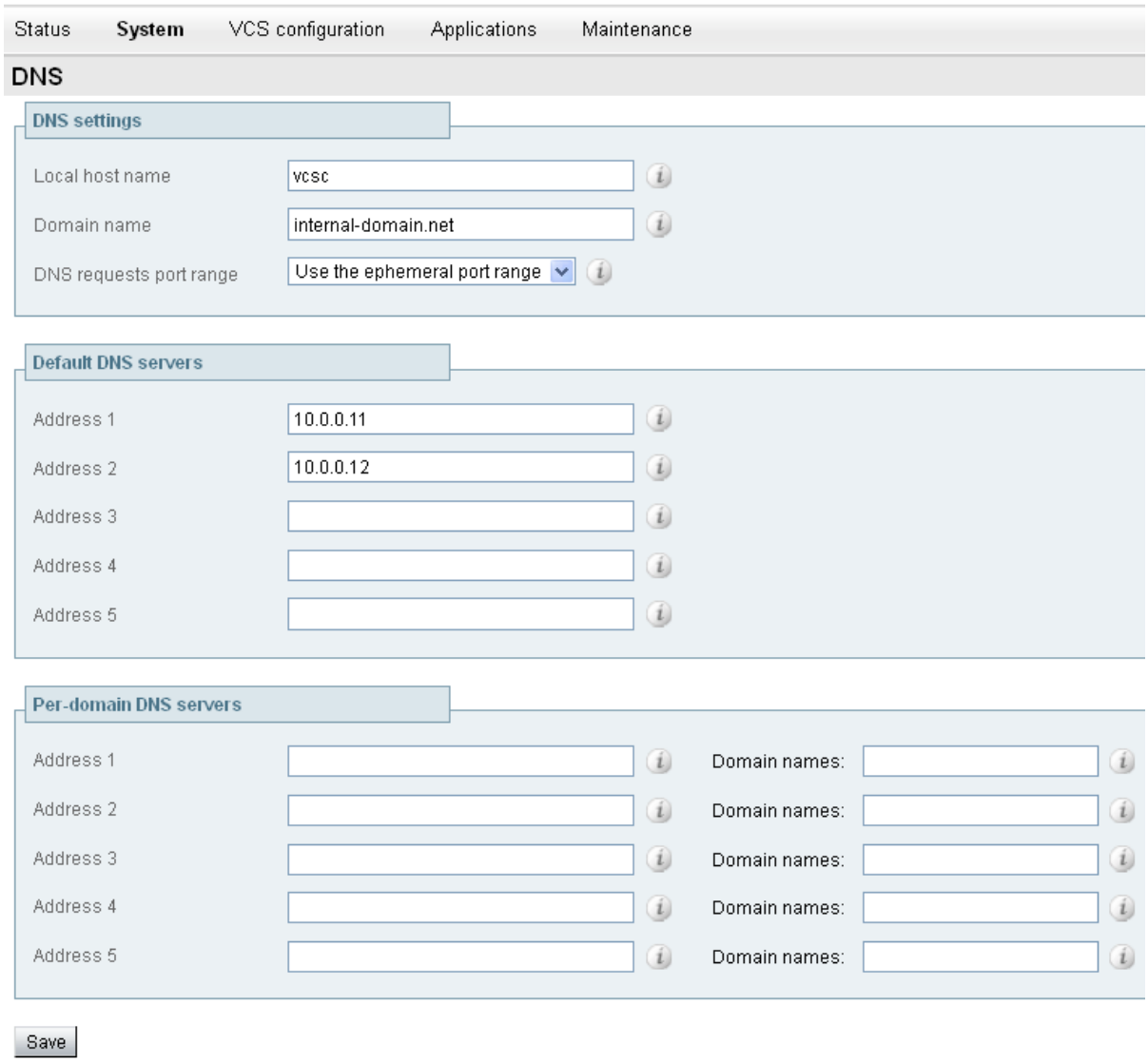
In the example deployment 2 DNS servers are configured for each VCS, which provides a level of DNS server redundancy. The VCS Control is configured with DNS servers which are located on the internal network. The VCS Expressway is configured with DNS servers which are publicly routable.

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

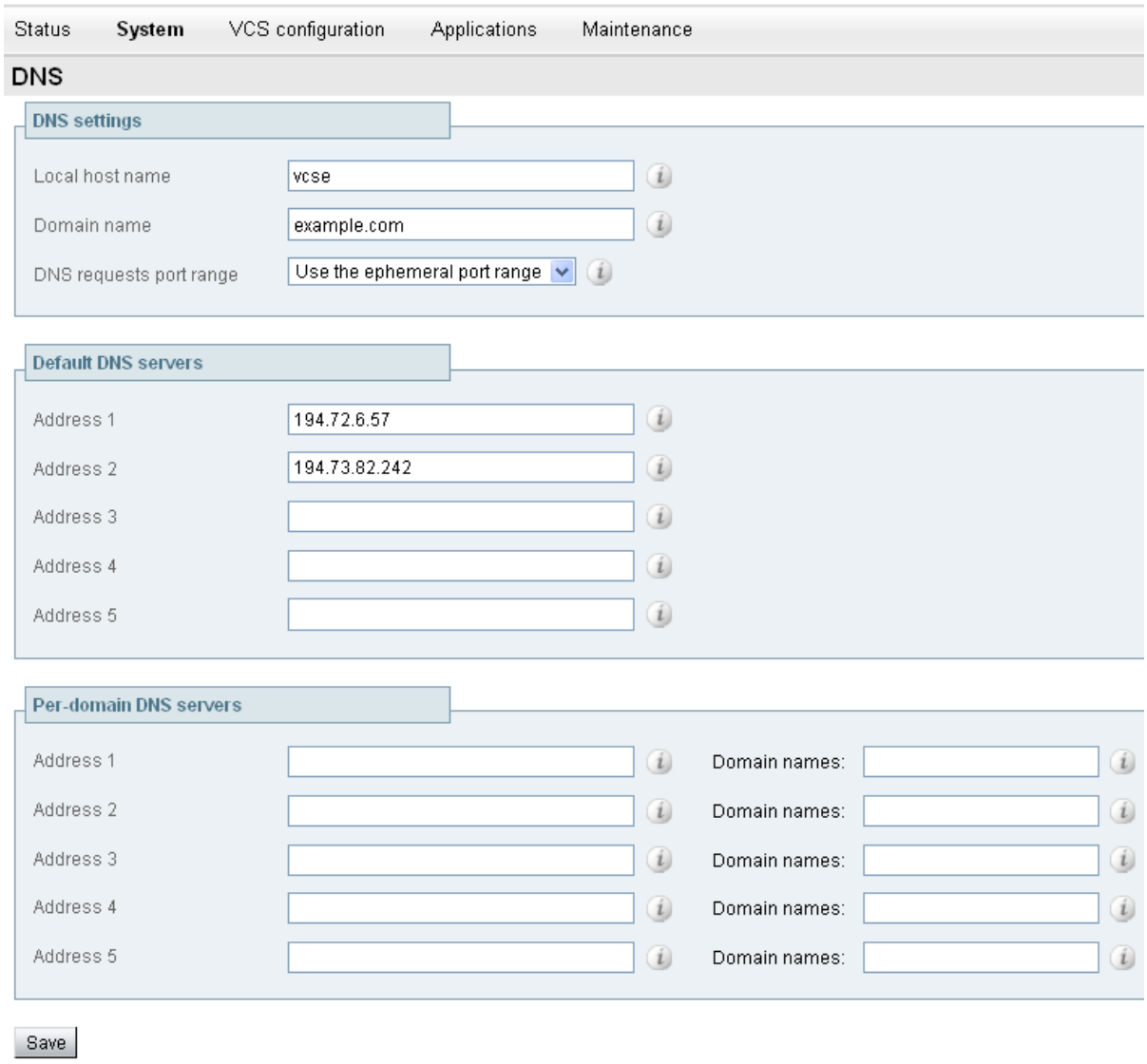
1. Go to the **DNS** page (**System > DNS**).
2. Configure the DNS server **Address** fields as follows:

	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

Step 4: Time configuration

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.

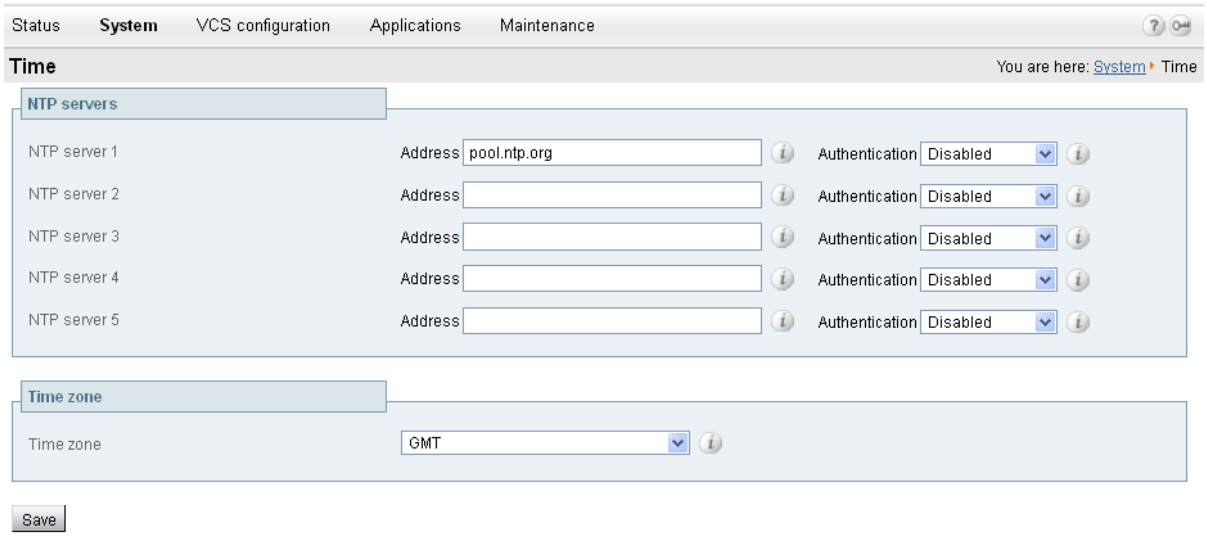
The **Time zone** sets the local time zone of the VCS.

To configure the NTP server address and Time zone:

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

	VCS Control	VCS Expressway
NTP server 1	Enter `pool.ntp.org`	Enter `pool.ntp.org`
Time zone	Select *GMT*	Select *GMT*

3. Click **Save**.



Step 5: SIP domain configuration

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.

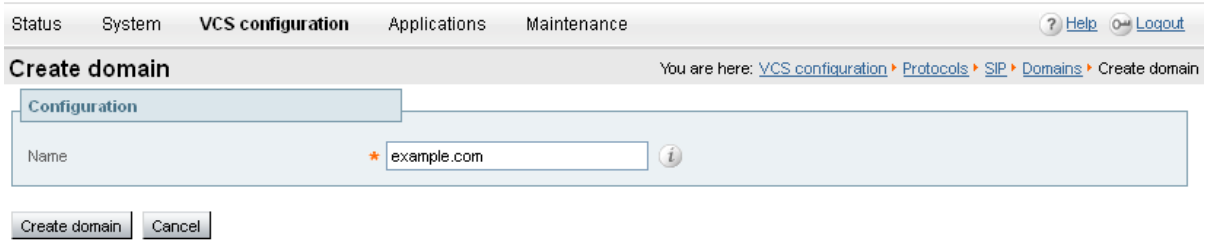
- Registration restriction (Allow or Deny) rules can be configured to limit acceptable registrations. See Registration restriction configuration (optional) [p.41].
- If authentication is enabled, only devices that can properly authenticate themselves will be allowed to register.

To configure a SIP domain:

1. Go to the **Domains** page (**VCS configuration > Protocols > SIP > Domains**).
2. Click **New**.
3. Enter the domain name into the **Name** field (on both VCS Control and 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.



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.

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.

This is carried out to make the call searches the same for calls from H.323 endpoints and SIP endpoints.

- Pre-search transforms should be used with care because they apply to all signaling messages – if they match, they will affect the routing of 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

The search rules configuration defines 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 configuration described in this document is used to ensure 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 searching 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 Expressway)	Registered devices (VCS Control or Expressway)
Registered devices (VCS Control or Expressway)	External domains and un-registered devices (via VCS Expressway using DNS zone)
Registered devices (VCS Control or Expressway)	Public external IP addresses (via VCS Expressway)
External domains and un-registered devices	Registered devices (VCS Control or 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).

It is possible to 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 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.

Step 6: Transform configuration

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

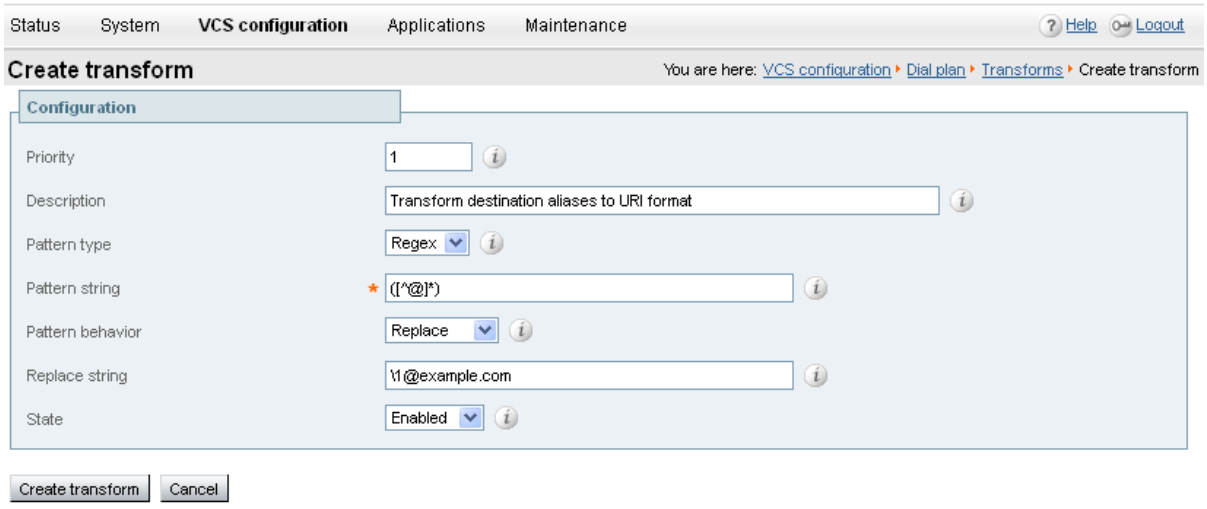
The following transform configuration modifies the destination alias of all call attempts made to destination aliases which do not contain an '@'. The old destination alias has @example.com appended to it. This has the effect of standardizing all called destination aliases into a SIP URI form.

To configure the transform:

1. Go to the **Transforms** page (**VCS 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	Select *Regex*	
Pattern string	Enter `([^@]*)`	
Pattern behavior	Select *Replace*	
Replace string	Enter `\1@example.com`	
State	Select *Enabled*	

4. Click **Create transform**.



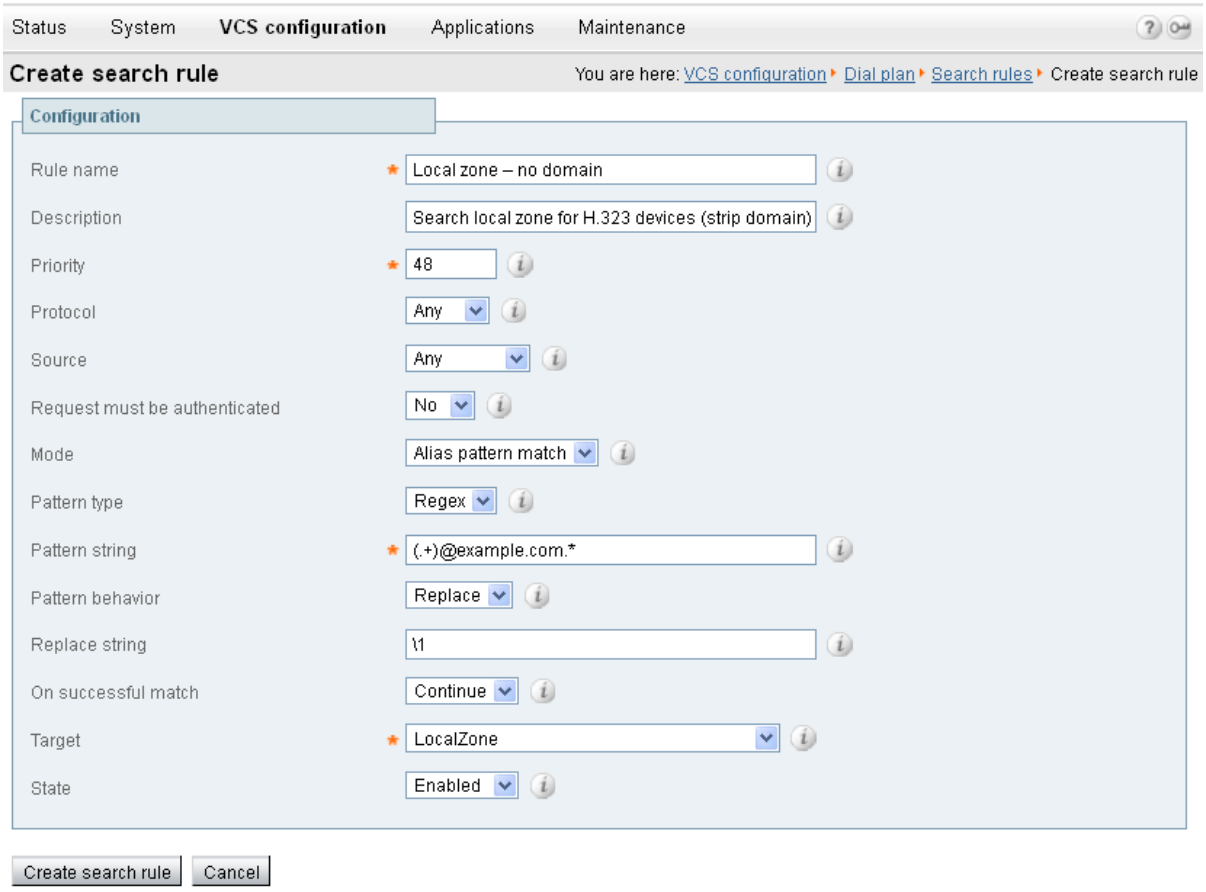
Step 7: Local zone search rules configuration

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

1. Go to the **Search rules** page (**VCS 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	Select *Any*	
Source	Select *Any*	
Request must be authenticated	Select *No*	
Mode	Select *Alias pattern match*	
Pattern type	Select *Regex*	
Pattern string	Enter `(.+)@example.com.*`	
Pattern behavior	Select *Replace*	
Replace string	Enter `\1`	
On successful match	Select *Continue*	
Target	Select *LocalZone*	
State	Select *Enabled*	

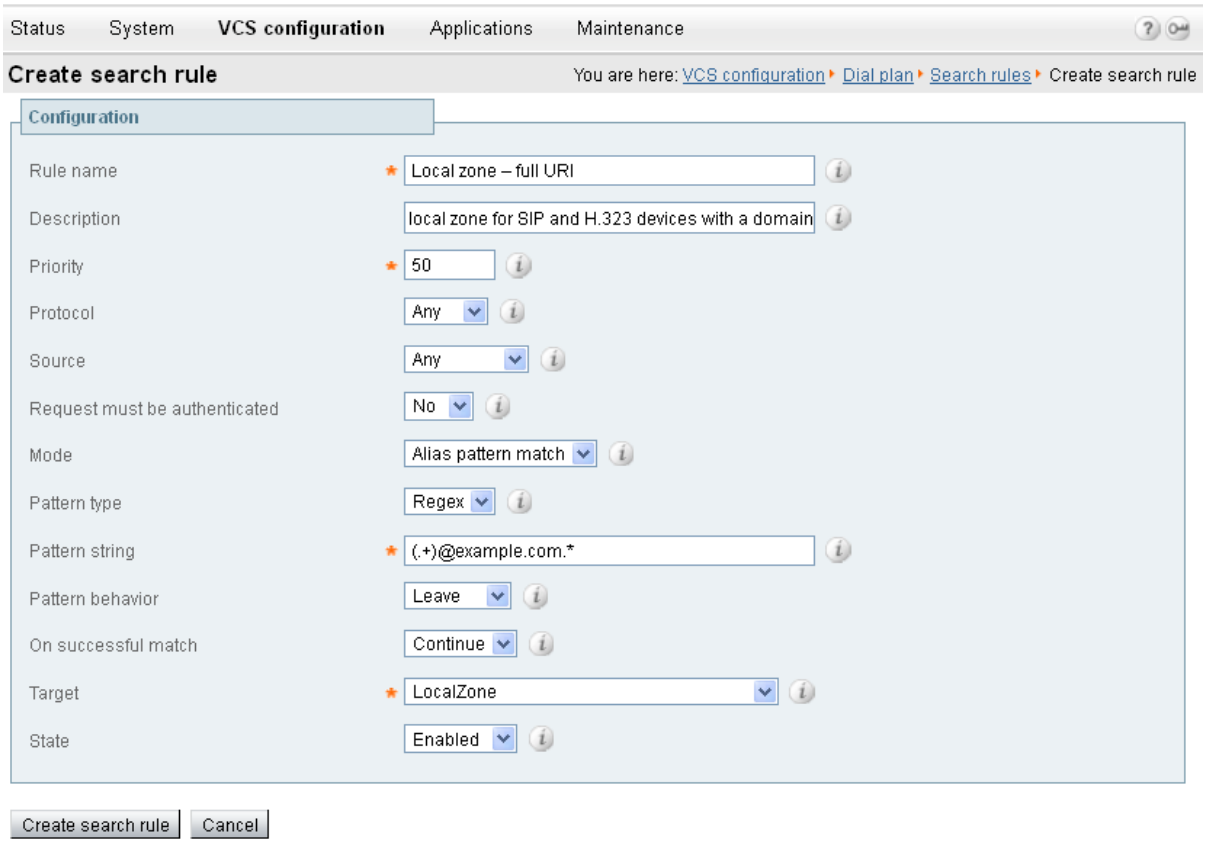
7. Click **Create search rule**.



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	Select *Any*	
Source	Select *Any*	
Request must be authenticated	Select *No*	
Mode	Select *Alias pattern match*	
Pattern type	Select *Regex*	
Pattern string	Enter `(.+)@example.com.*`	
Pattern behavior	Select *Leave*	
On successful match	Select *Continue*	
Target	Select *LocalZone*	
State	Leave as *Enabled*	

10. Click **Create search rule**.



Step 8: Traversal zone including authentication (connection credentials) configuration

The traversal zone configuration defines a connection between the VCS Control and VCS Expressway platforms.

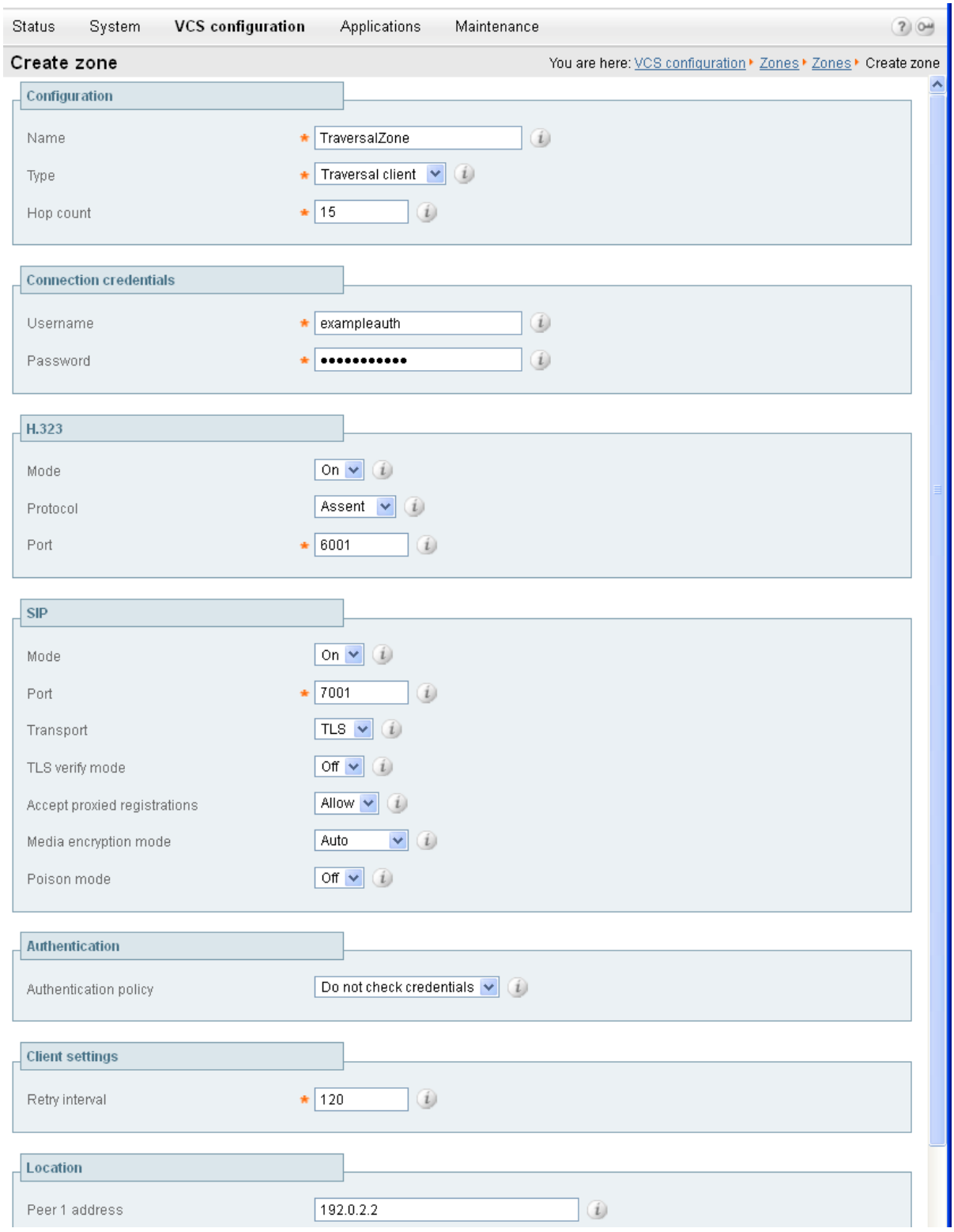
- A traversal zone connection allows firewall traversal for signaling and media between the two platforms.
- The VCS Control is configured with a traversal client zone, and the VCS Expressway with a traversal server zone.

To configure the traversal zone:

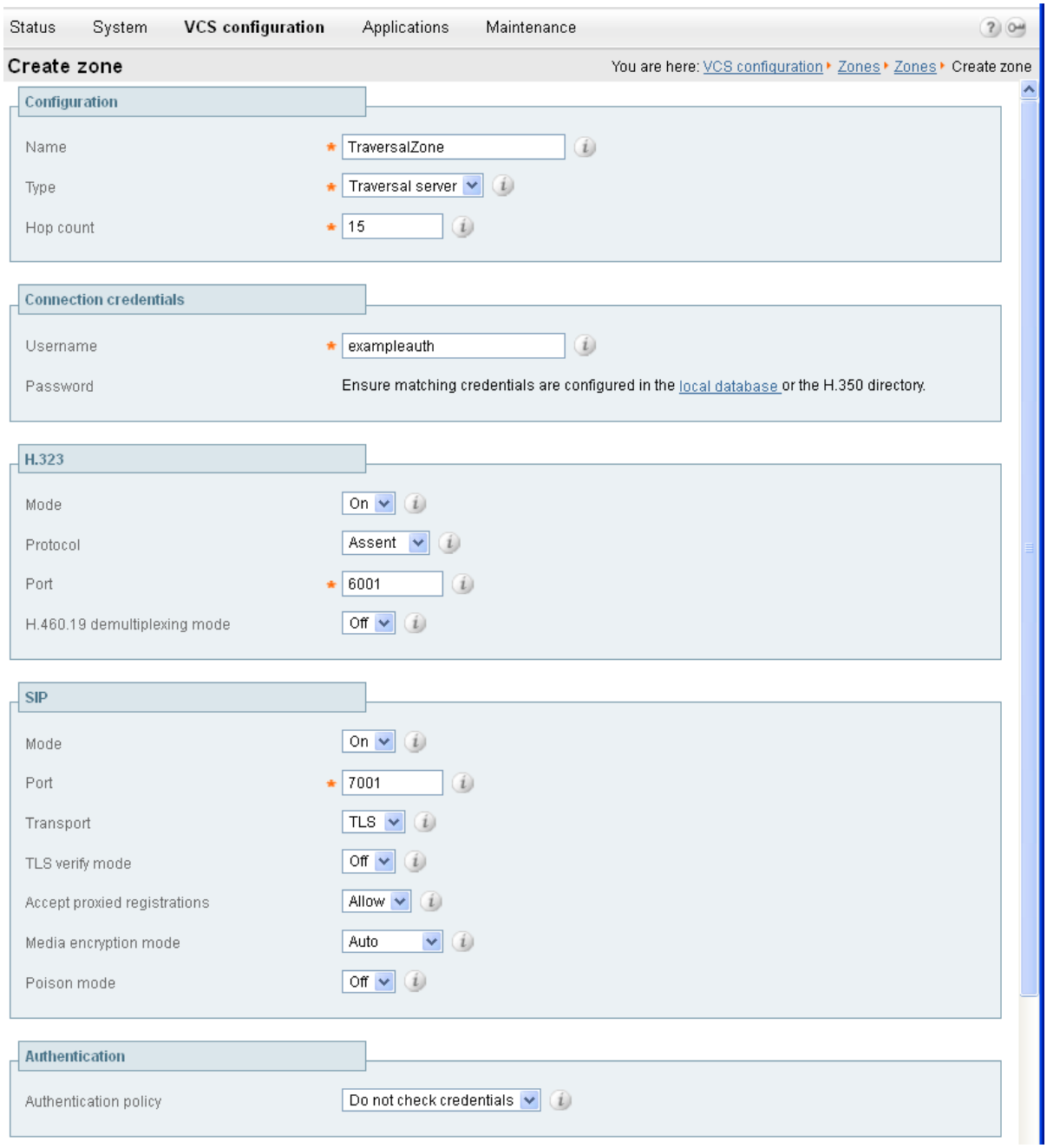
1. Go to the **Zones** page (**VCS configuration > Zones > Zones**).
2. Click **New**.
3. Configure the fields as follows (leave all other fields with default values):

	VCS Control	VCS Expressway
Name	Enter `TraversalZone`	Enter `TraversalZone`
Type	Select *Traversal client*	Select *TraversalServer*
Hop count	Enter `15`	Enter `15`
Username	Enter `exampleauth`	Enter `exampleauth`
Password	Enter `ex4mpl3.c0m`	Not applicable
H.323 Mode	Select *On*	Select *On*
H.323 Protocol	Select *Assent*	Select *Assent*
H.323 Port	Enter `6001`	Enter `6001`
H.323 H.460.19 demultiplexing mode	Not applicable	Select *Off*
SIP Mode	Select *On*	Select *On*
SIP Port	Enter `7001`	Enter `7001`
SIP Transport	Select *TLS*	Select *TLS*
SIP TLS verify mode	Select *Off*	Select *Off*
SIP Accept proxied registrations	Select *Allow*	Select *Allow*
Media encryption mode	Select *Auto*	Select *Auto*
SIP Poison mode	Select *Off*	Select *Off*
Authentication policy	Select *Do not check credentials*	Select *Do not check credentials*
Client settings Retry interval	Enter `120`	Not applicable
Location Peer 1 address	Enter `192.0.2.2`	Not applicable

4. Click **Create zone**.


Status System VCS configuration Applications Maintenance
Create zone
You are here: VCS 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
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

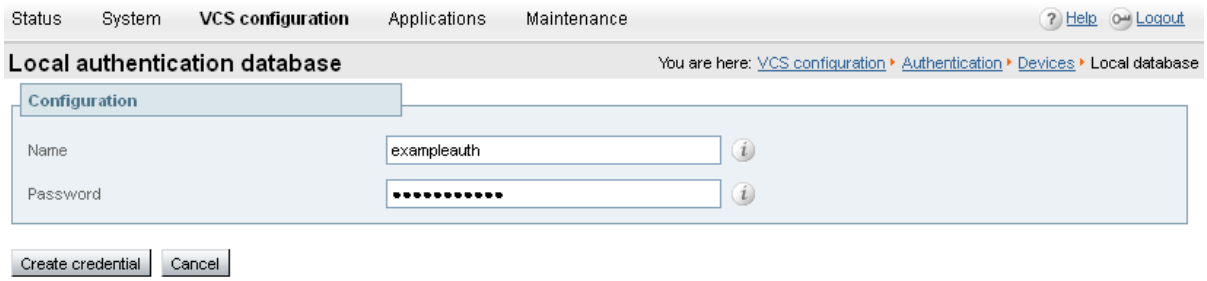
To configure the authentication credentials in the **Local authentication database** (which are configured in the VCS Expressway only):

1. Go to the **Local authentication database** page (**VCS 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**.



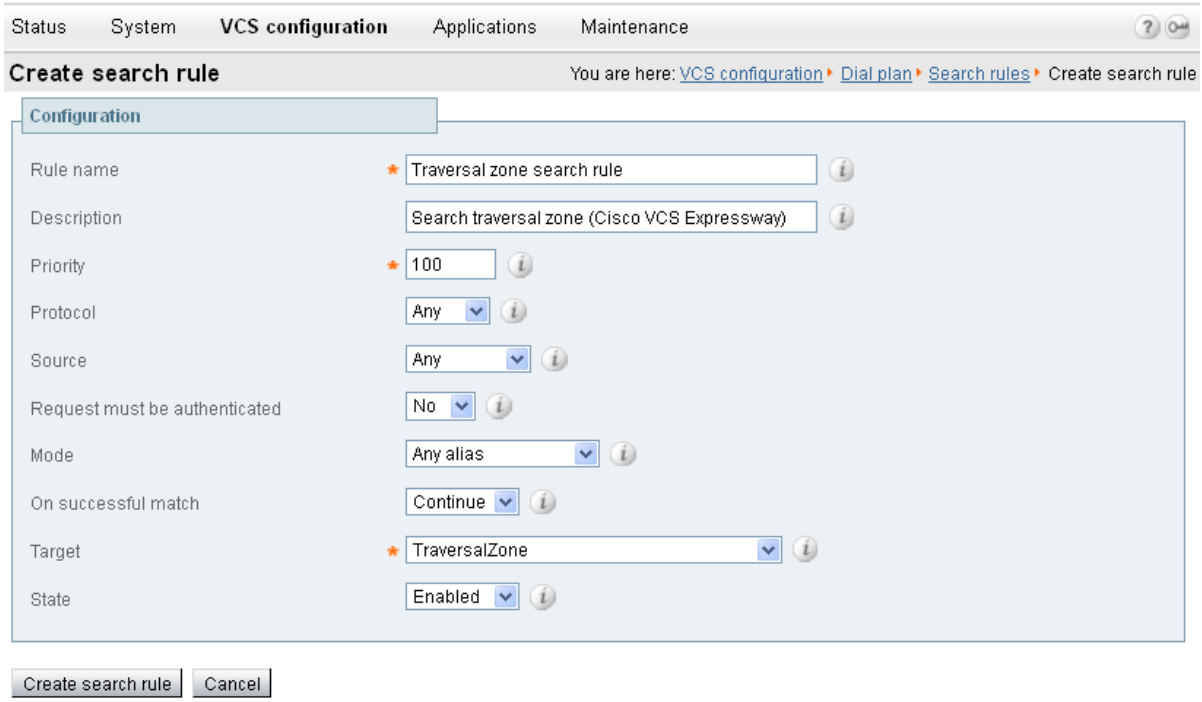
Step 9: Traversal zone search rules configuration

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

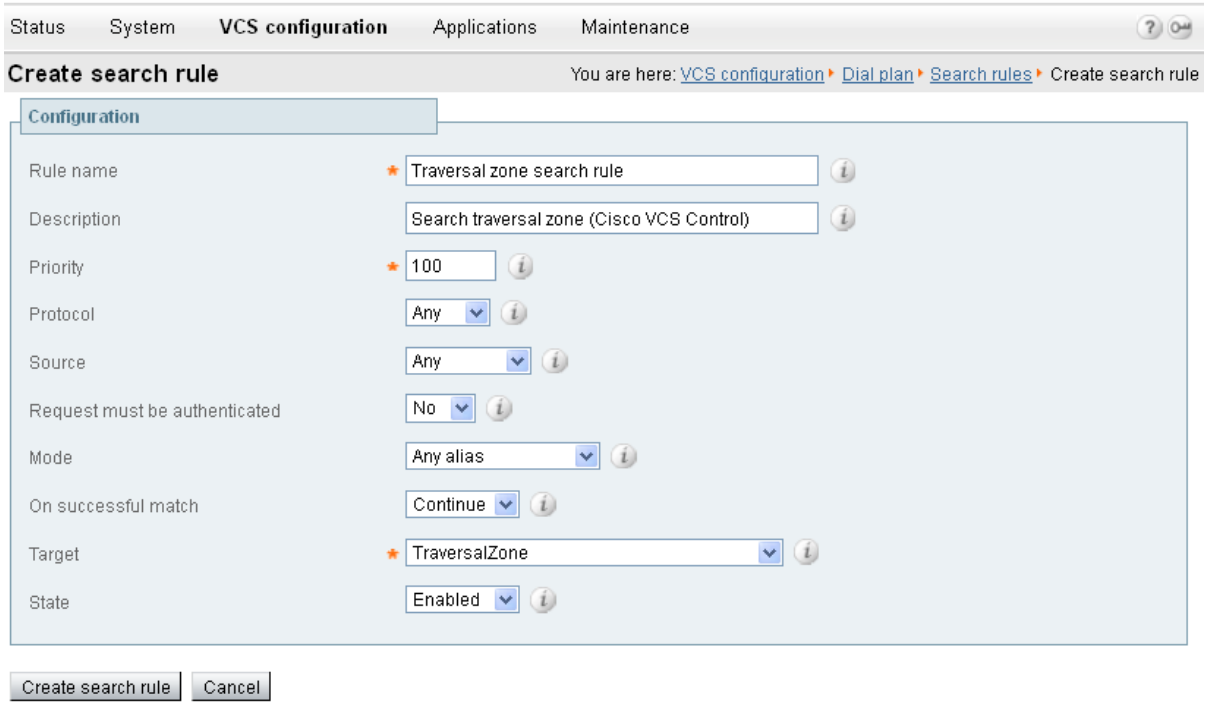
1. Go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**).
2. Click **New**.
3. Configure the fields as follows:

	VCS Control	VCS Expressway
Rule name	Enter `Traversal zone search rule`	Enter `Traversal zone search rule`
Description	Enter `Search traversal zone (Cisco VCS Expressway)`	Enter `Search traversal zone (Cisco VCS Control)`
Priority	Enter `100`	Enter 100
Protocol	Select *Any*	Select *Any*
Source	Select *Any*	Select *Any*
Request must be authenticated	Select *No*	Select *No*
Mode	Select *Any alias*	Select *Any alias*
On successful match	Select *Continue*	Select *Continue*
Target	Select *TraversalZone*	Select *TraversalZone*
State	Select *Enabled*	Select *Enabled*

4. Click **Create search rule**.



VCS Control



VCS Expressway

Step 10: DNS zone configuration

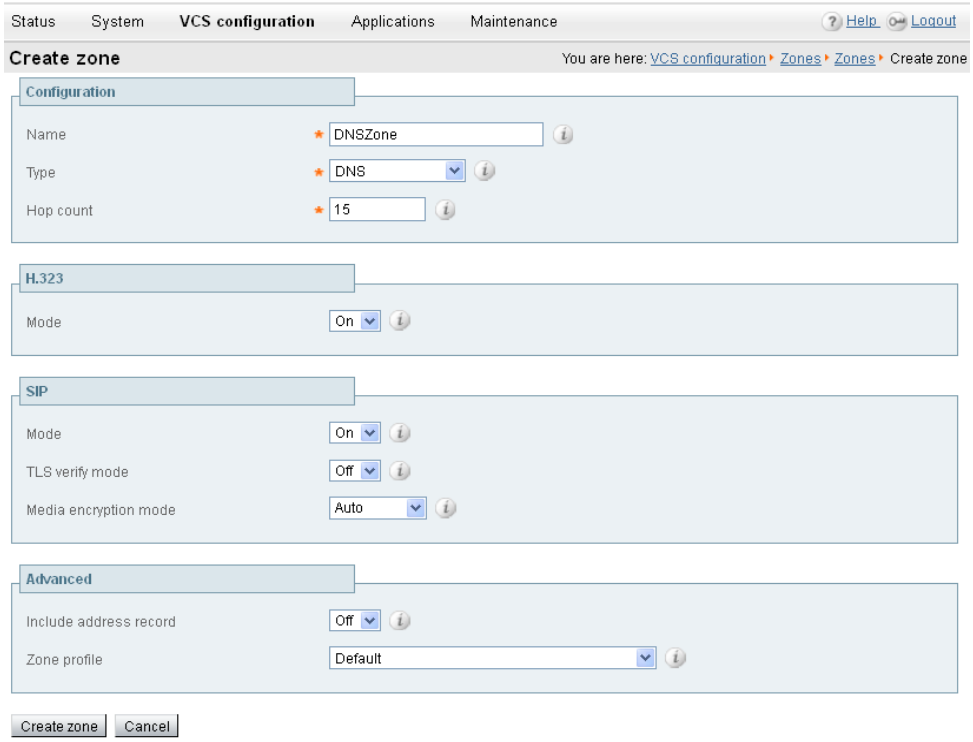
The DNS zone is used to search for externally hosted systems (which are not registered to the VCS Control or VCS Expressway, such as for business to business calling). Destination aliases are searched for by a name using a DNS lookup.

To configure the DNS zone:

1. Go to the **Zones** page (**VCS configuration > Zones > Zones**).
2. Click **New**.
3. Configure the fields as follows:

	VCS Control	VCS Expressway
Name	Not applicable	Enter `DNSZone`
Type	Not applicable	Select *DNS*
Hop count	Not applicable	Enter `15`
H.323 Mode	Not applicable	Select *On*
SIP Mode	Not applicable	Select *On*
TLS verify mode	Not applicable	Select *Off*
Media encryption mode	Not applicable	Select *Auto*
Include address record	Not applicable	Select *Off*
Zone profile	Not applicable	Select *Default*

4. Click **Create zone**.


Status System VCS configuration Applications Maintenance Help Logout
Create zone
You are here: VCS configuration Zones Zones Create zone
Configuration
Name * DNSZone
Type * DNS
Hop count * 15
H.323
Mode On
SIP
Mode On
TLS verify mode Off
Media encryption mode Auto
Advanced
Include address record Off
Zone profile Default
Create zone Cancel

Step 11: DNS search rule configuration

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

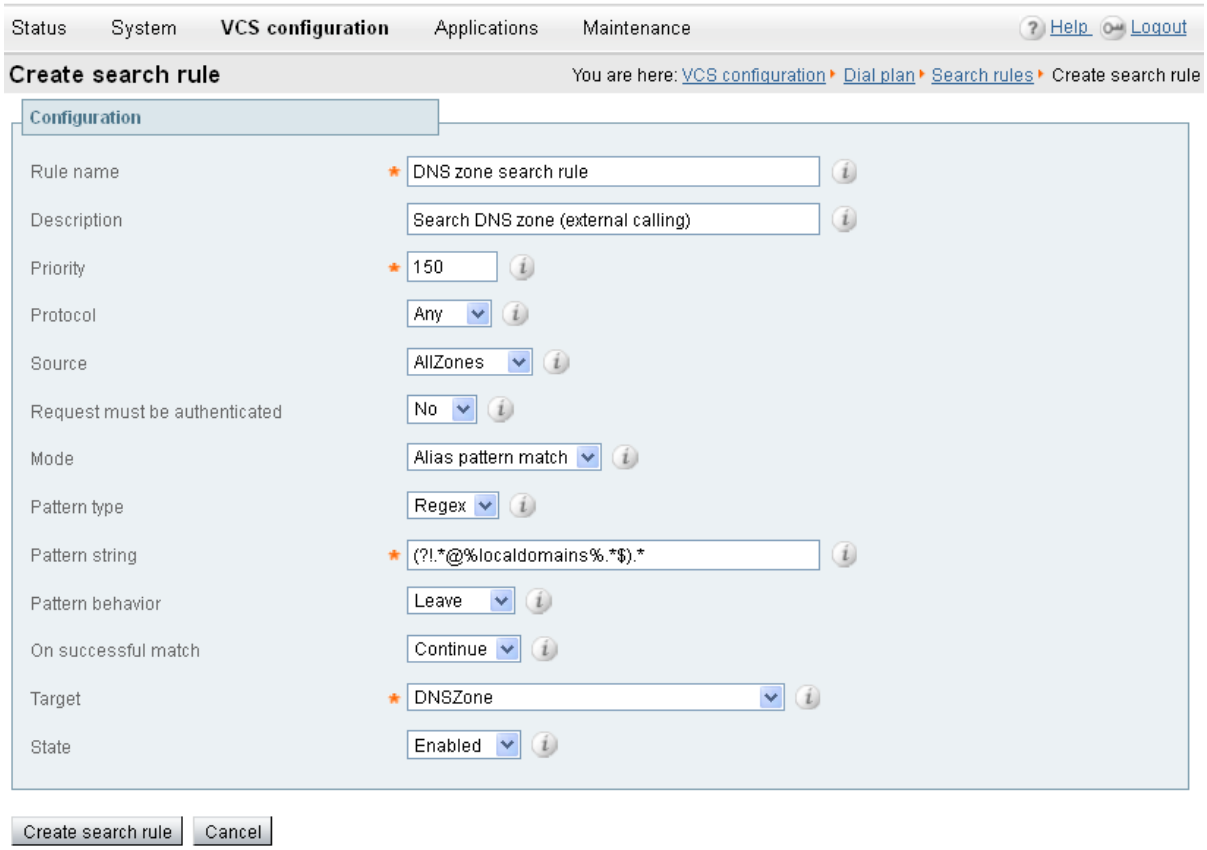
A specific regular expression is configured which will prevent searches being made using the DNS zone (i.e. on the public internet) for destination addresses (URIs) using any SIP domains which are configured on the local network (local domains).

To create the search rules to route via DNS:

1. Go to the **Search rules** page (**VCS configuration > Dial plan > Search rules**).
2. Click **New**.
3. Configure the fields as follows:

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

Step 12: External (unknown) IP address routing configuration

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.

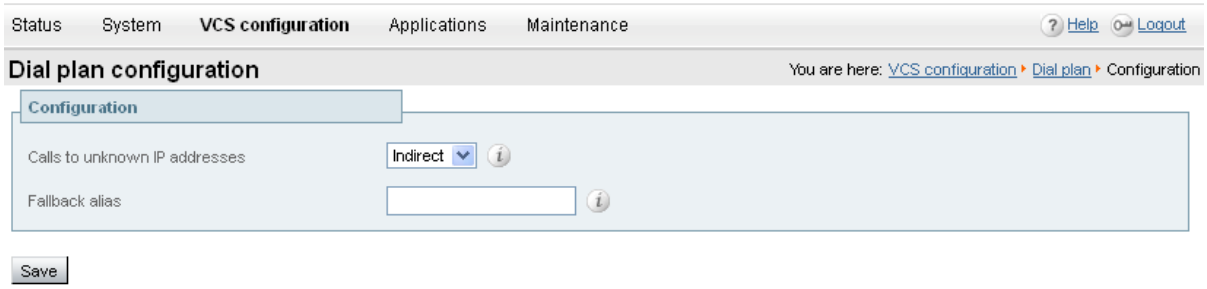
- All requests destined for external IP addresses, originating at the VCS Control are routed to the VCS Expressway using a search rule.
- The VCS Expressway then attempts to open a connection directly to the IP address.

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

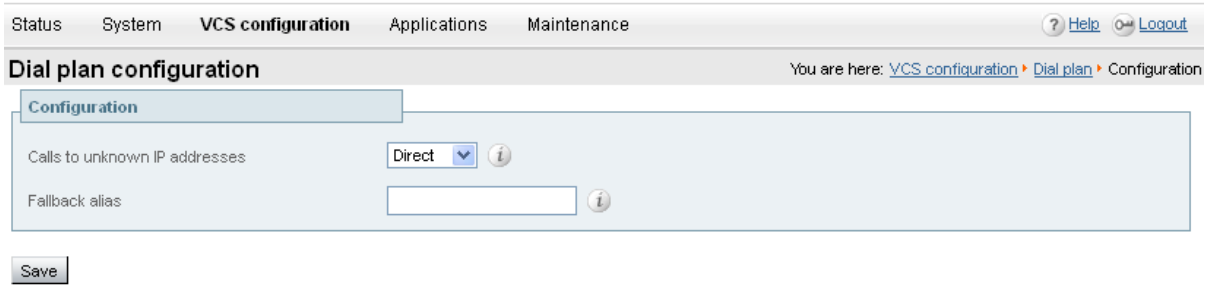
1. Go to the **Dial plan configuration** page (**VCS configuration > Dial plan > Configuration**).
2. Configure the fields as follows:

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

3. Click **Save**.



VCS Control



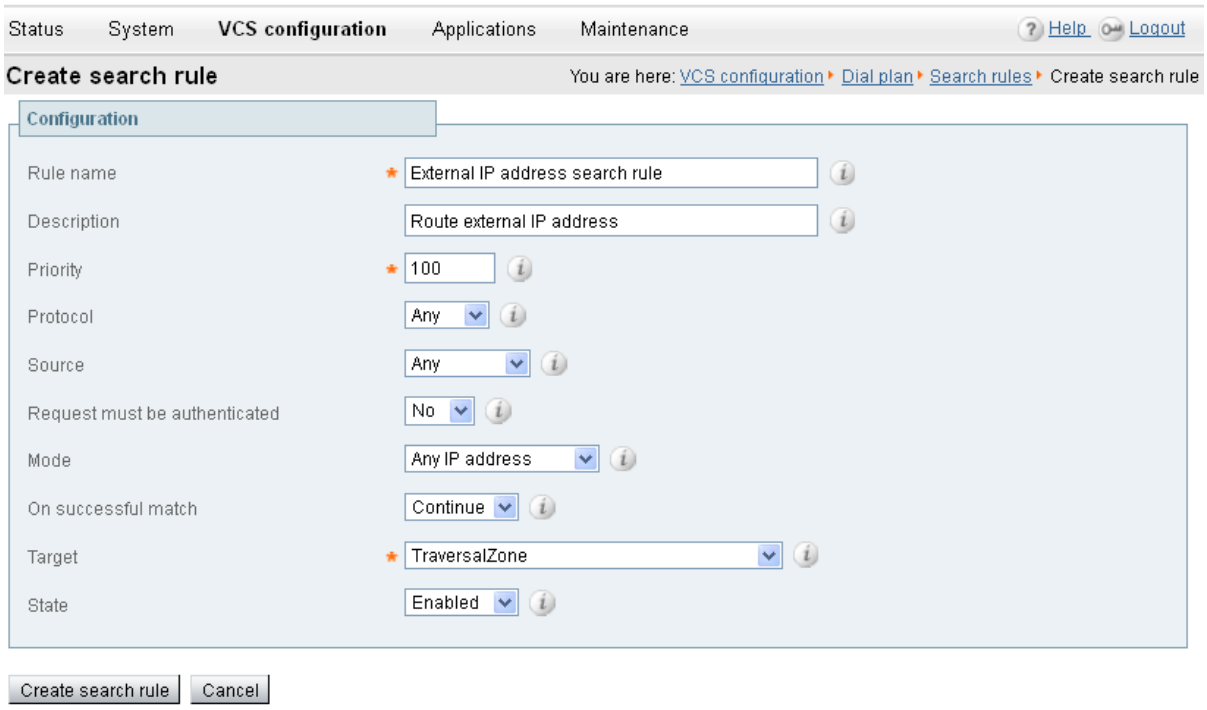
VCS Expressway

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

1. Go to the **Search rules** page (**VCS 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	Select *Any*	Not applicable
Source	Select *Any*	Not applicable
Request must be authenticated	Select *No*	Not applicable
Mode	Select *Any IP address*	Not applicable
On successful match	Select *Continue*	Not applicable
Target	Select *Traversal Zone*	Not applicable
State	Select *Enabled*	Not applicable

4. Click **Create search rule**.



Endpoint registration

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

Endpoint	IP address	Network
E20	10.0.0.15	Internal network
MXP1700	10.0.0.16	Internal network
MXP1000	192.168.0.2	Home user network

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

E20 (uses SIP protocol)	
SIP URI	user.one.e20@example.com
SIP Proxy1	vcsc.internal-domain.net
MXP1700 (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
MXP1000 (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

Check on both VCS Control and VCS Expressway that the traversal zone is **Active** on the **Zones status** page (**Status > Zones**).

The status of the zone can also be seen on the **Zones** configuration page (**VCS 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 configuration [p.54])
- confirm that the authentication and client authentication usernames (and passwords) are configured correctly (and match) on VCS Control and 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 will be listed in the **Registrations by device** status page (**Status > Registrations > By device**).

If the expected endpoints are not registered:

- review the endpoint's registration configuration
  - is the endpoint configured to register with the VCS Expressway if located on the external network / internet?
  - is the endpoint configured to register with the VCS Control if located on the internal network?
- review the SIP domain configuration (Step 5)
- review any registration restriction configuration applied to the VCS (optional, see Registration restriction configuration (optional) [p.41])

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 Cisco Jabber / Movi 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; in this case the device will be able to 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

System backup

To create a system backup:

1. Go to the **Backup and restore** page (**Maintenance > Backup and restore**).
2. Click **Create system backup file**.
3. Wait for file download dialog to appear.
4. Click **Save**, to save the backup file archive to your local PC.

For more information, see *VCS Administrator Guide*.

Optional configuration steps

Cisco TMS configuration (optional)

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

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

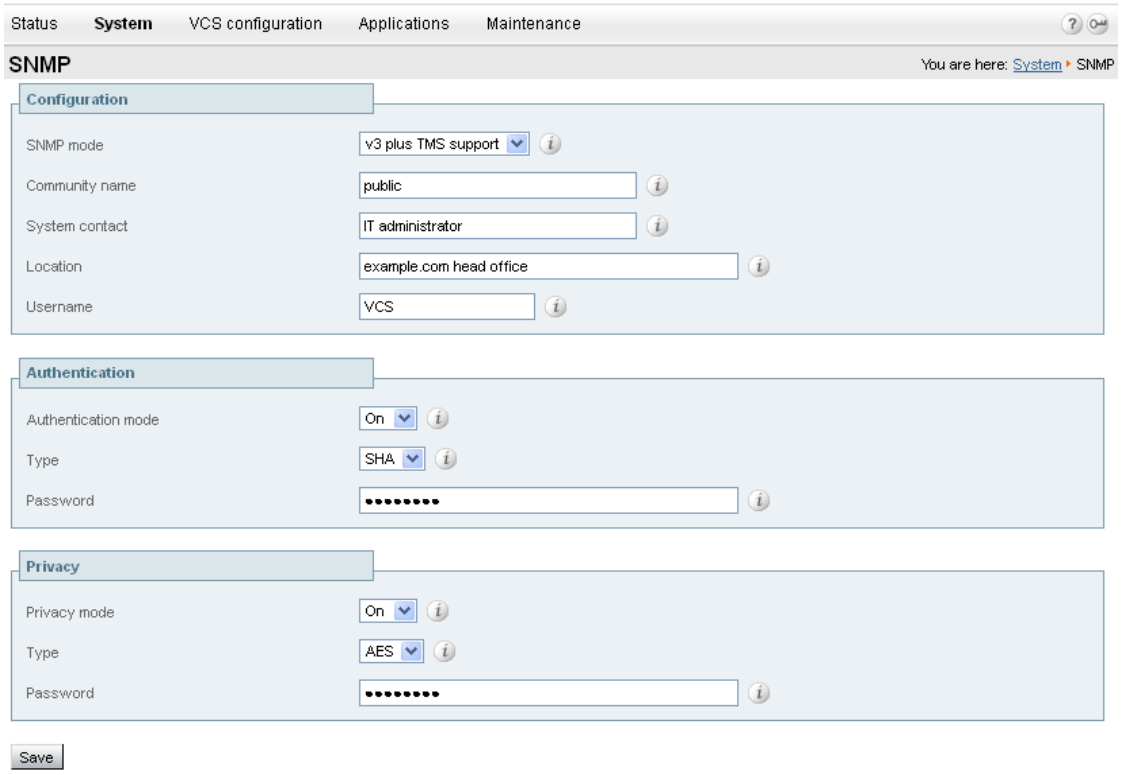
- Enabling SNMP speeds up the VCS - Cisco TMS integration process but is not essential.
- VCS Expressway integration with Cisco TMS requires additional firewall / NAT configuration – See Appendix 3 – Firewall and NAT configuration [p.54] (VCS Expressway needs to access port 80/443 on Cisco TMS from outside the firewall).

To enable and configure SNMP:

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

	VCS Control	VCS Expressway
SNMP mode	Select *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	Select *On*	
Type	Select *SHA*	
Password	Enter `ex4mpl3.c0m`	
Privacy mode	Select *On*	
Type	Select *AES*	
Password	Enter `ex4mpl3.c0m`	

3. Click **Save**.

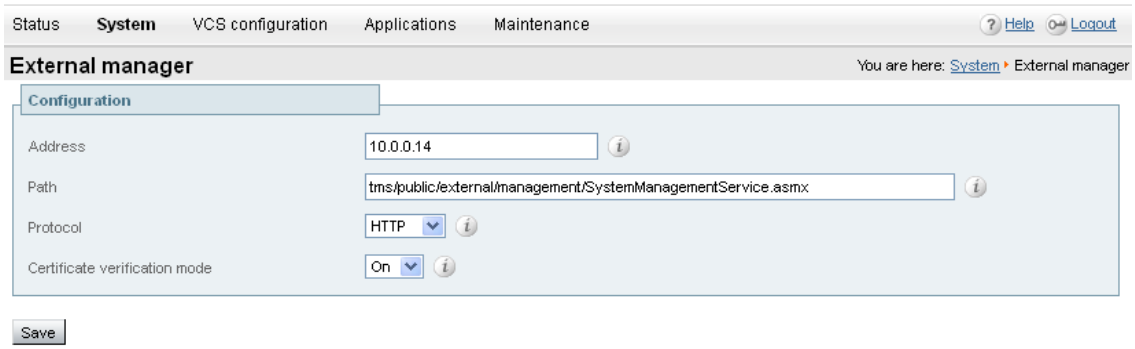


To configure the necessary external manager (Cisco TMS) parameters:

1. Go to the **External manager** page (**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**.


Status
System
VCS configuration
Applications
Maintenance
Help
Logout
External manager
You are here: System External manager
Configuration
Address
10.0.0.14
Path
tms/public/external/management/SystemManagementService.asmx
Protocol
HTTP
Certificate verification mode
On
Save

Logging server configuration (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.

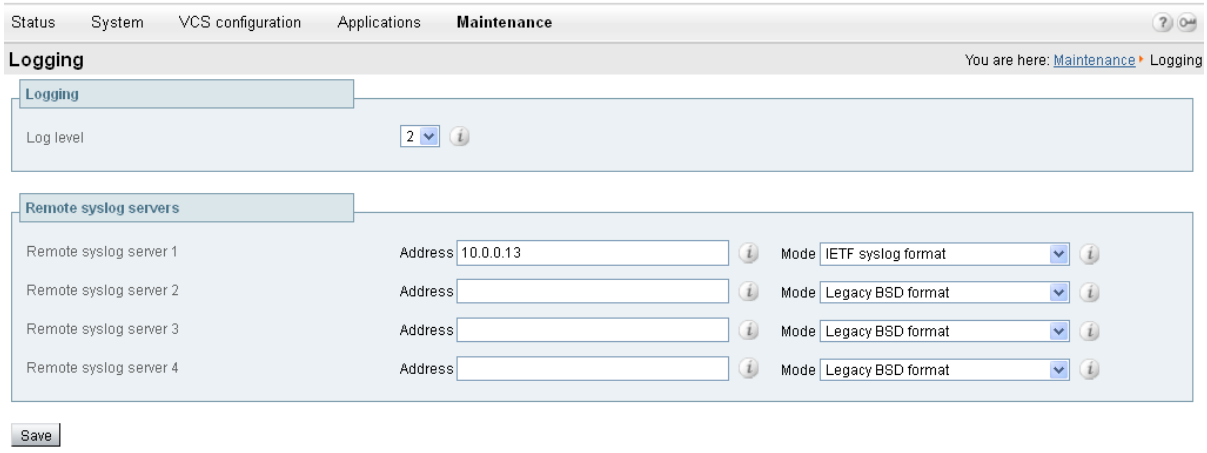
VCS Expressway external logging server configuration requires additional firewall / NAT configuration – See Appendix 3 – Firewall and NAT configuration [p.54].

To configure a logging server:

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

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

3. Click **Save**.



Registration restriction configuration (optional)

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

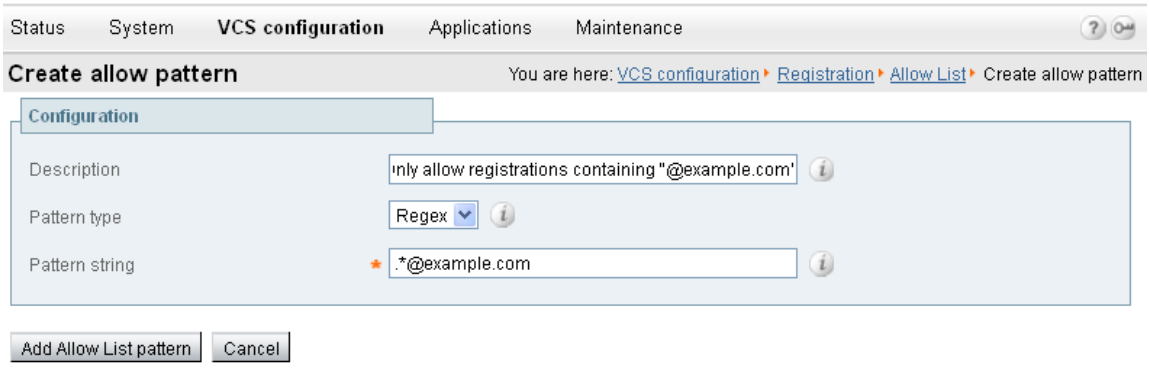
The following configuration will limit registrations (on both VCS Control and VCS Expressway) to endpoints which register with an identity that contains “@example.com”.

To configure Allow List registration restrictions:

1. Go to the **Allow List** page (**VCS 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	Select Regex	
Pattern string	Enter `.*@example.com`	

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

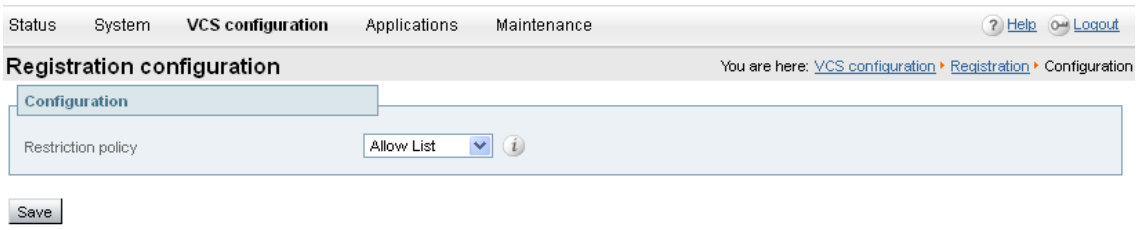


To activate the registration restriction:

1. Go to the **Registration configuration** page (**VCS configuration > Registration > Configuration**).
2. Configure the **Restriction policy** as follows:

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

3. Click **Save**.



Restrict 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

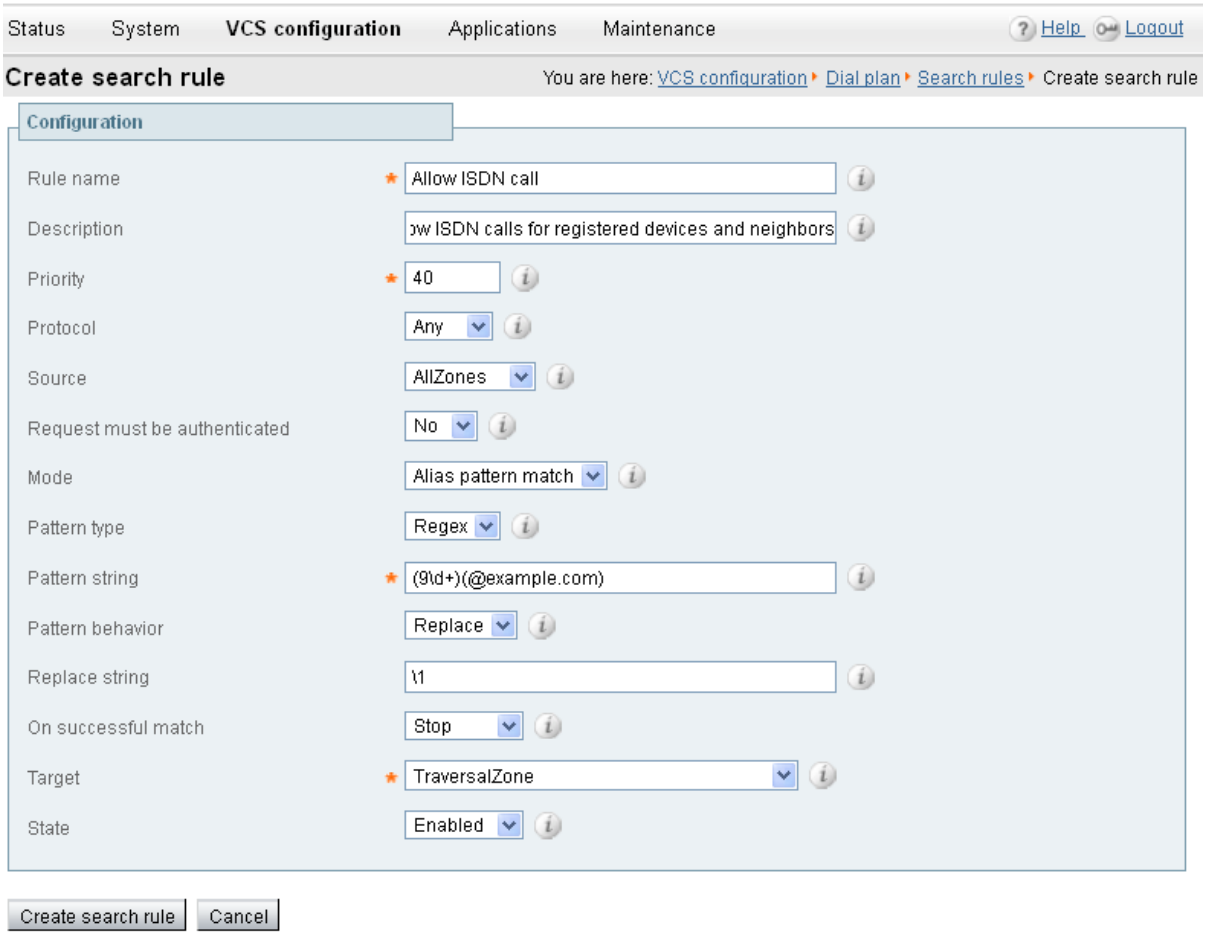
Two search rules are created on the VCS Expressway:

- 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 the **Search rules** page (**VCS configuration > Dial plan > Search rules**).
2. Click **New**.
3. Configure the fields as follows:

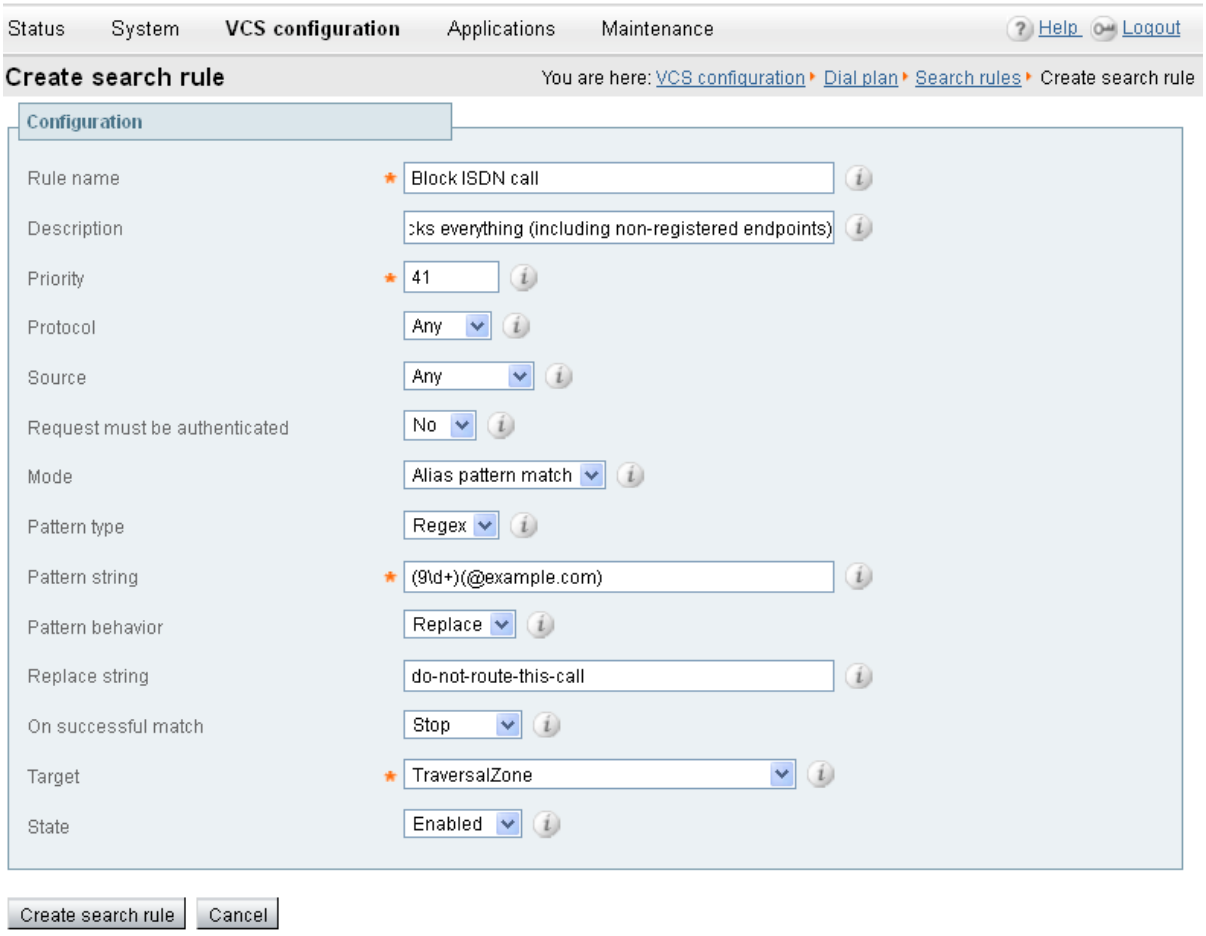
	VCS Expressway
Rule name	Enter `Allow ISDN call`
Description	Enter `Allow ISDN calls for registered devices and neighbors`
Priority	Enter `40` (these rules must be the highest priority in the search rule configuration)
Protocol	Select *Any*
Source	Select *All zones*
Request must be authenticated	Select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



4. Click **Create search rule**.
5. Click **New**.
6. Configure the fields as follows:

	VCS Expressway
Rule name	Enter `Block ISDN call`
Description	Enter `Blocks everything (including non-registered endpoints)`
Priority	Enter `41`
Protocol	Select *Any*
Source	Select *Any*
Request must be authenticated	Select *No*
Mode	Select *Alias pattern match*
Pattern type	Select *Regex*
Pattern string	Enter `(9\d+)(@example.com)`

	VCS Expressway
Pattern behavior	Select *Replace*
Replace string	Enter `do-not-route-this-call`
On successful match	Select *Stop*
Target	Select *TraversalZone*
State	Select *Enabled*



7. Click **Create search rule**.

VCS Control

This example shows how to configure the VCS Control to stop calls coming in from 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*.

Create 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 are not allowed to send calls back out of this g
ateway -->
      <!-- 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 are not allowed to send calls back out of this g
ateway -->
      <!-- 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:

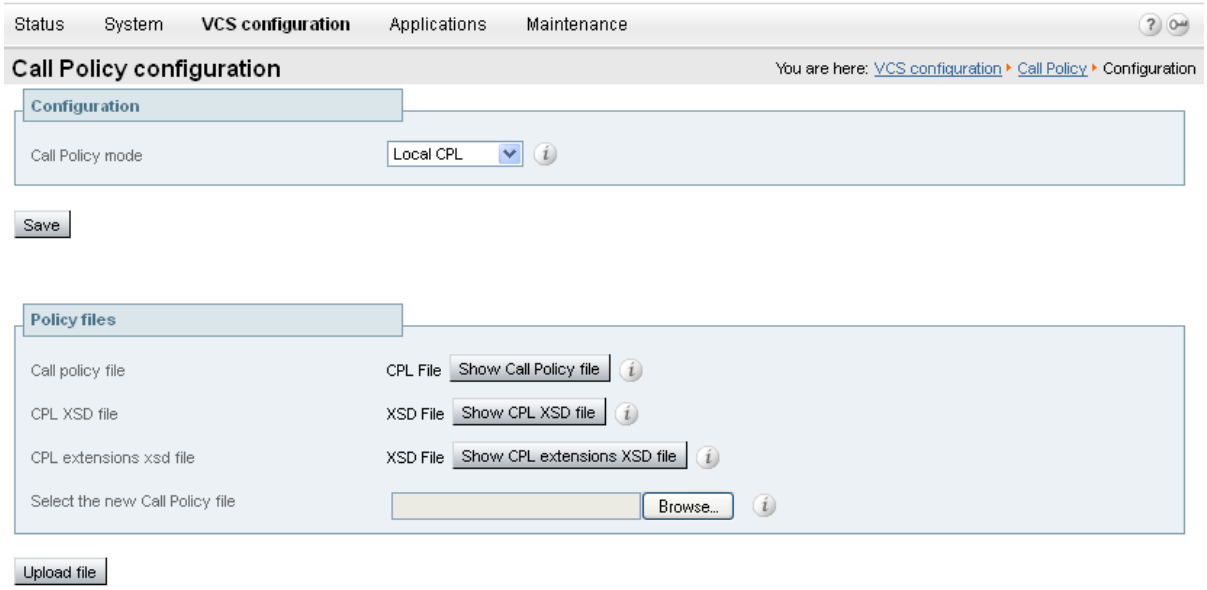
```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
xmlns:taa="http://www.tandberg.net/cpl-extensions"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <taa:rule-switch>
    <!-- Check that calling 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 are not allowed to hairpin and send calls 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 are not allowed to hairpin and send calls 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>
```

Load the CPL onto VCS Control

To configure the VCS Control to use the CPL:

1. Go to the **Call Policy configuration** page (**VCS 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**.


Status
System
VCS configuration
Applications
Maintenance
Call Policy configuration
You are here: VCS 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 Expressway. It is broken down into 3 sections:

- VCS Control (configuration that has to be applied only to the VCS Control)
- VCS Expressway (configuration that has to be applied only to the VCS Expressway)
- VCS Control and Expressway (configuration that has to be applied to both the VCS Control and Expressway

VCS Control configuration details

Configuration item	Value	VCS page
System configuration		
System name	VCSc	System > System
LAN1 IPv4 address	10.0.0.2	System > IP
IPv4 gateway	10.0.0.1	System > IP
LAN1 subnet mask	255.255.255.0	System > 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 Local 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	VCS configuration > Protocols > SIP > Domains
Traversal zone		
Zone Name	TraversalZone	VCS configuration > Zones > Zones
Zone Type	Traversal client	VCS configuration > Zones > Zones
Protocol SIP port	7001	VCS configuration > Zones > Zones
Protocol H.323 port	6001	VCS configuration > Zones > Zones
Location Peer 1 address	192.0.2.2	VCS configuration > Zones > Zones
Authentication username	exampleauth	VCS configuration > Zones > Zones
Authentication password	ex4mpl3.c0m	VCS configuration > Authentication > Devices > Local database
Traversal search rule		
Rule name	Traversal zone search rule	VCS configuration > Dial plan > Search rules

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

VCS Expressway configuration details

Configuration item	Value	VCS page
System configuration		
System name	VCSe	System > System
LAN1 IPv4 address	192.0.2.2	System > IP
IPv4 gateway	192.0.2.1	System > IP
LAN1 subnet mask	255.255.255.0	System > 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 Local host name	vcse	System > DNS
NTP server 1	pool.ntp.org	System > Time
Time zone	GMT	System > Time
Protocol configuration		

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

Configuration item	Value	VCS page
Calls to unknown IP addresses	Direct	VCS configuration > Dial plan > Configuration

VCS Control and Expressway configuration details

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

Appendix 2 – DNS records configuration

DNS configuration on host server

The following records are required to be configured 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	TTL	Type	Data
vcse.example.com	86400	A	192.0.2.2

DNS SRV records

Service	Protocol	Host	Port	Notes
h323cs	tcp	_h323cs._tcp.example.com	1720	
h323ls	udp	_h323ls._udp.example.com	1719	
sip	tcp	_sip._tcp.example.com	5060	
sip	udp	_sip._udp.example.com	5060	
sips	tcp	_sips._tcp.example.com	5061	
sips	tls	_sips._tls.example.com	5061	For E20 TE2.1
sip	tls	_sip._tls.example.com	5061	For MXP F8.2, T150 L6.0, Movi prior to version 3.1
turn	udp	_turn._udp.example.com	3478	Should match port setting on **VCS configuration > Expressway > TURN**

For each DNS SRV record the following values are common:

Name	example.com
TTL	86400
Type	SRV
Priority	10
Weight	10
Target	vcse.example.com.

DNS configuration (internal DNS server)

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

Local DNS A record

Host	TTL	Type	Data
vcsc.internal-domain.net	86400	A	10.0.0.2

Local DNS SRV records

Service	Protocol	Host	Port	Notes
h323cs	tcp	_h323cs._tcp.internal-domain.net	1720	
h323ls	udp	_h323ls._udp. internal-domain.net	1719	
sip	tcp	_sip._tcp.internal-domain.net	5060	
sip	udp	_sip._udp.internal-domain.net	5060	
sips	tcp	_sips._tcp.internal-domain.net	5061	
sips	tls	_sips._tls.internal-domain.net	5061	For E20 TE2.1
sip	tls	_sip._tls.internal-domain.net	5061	For MXP F8.2, T150 L6.0, Movi prior to version 3.1

For each DNS SRV record the following values are common:

Name	internal-domain.net
TTL	86400
Type	SRV
Priority	10
Weight	10
Target	vcsc.internal-domain.net.

Appendix 3 – Firewall and NAT configuration

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*.

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
RTCP Assent	VCSc	VCSe	Any	50000 to 54999	UDP	192.0.2.2	2777
RTP Assent	VCSc	VCSe	Any	50000 to 54999	UDP	192.0.2.2	2776
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
RTCP Assent	VCSc	VCSe	10.0.0.2	50000 to 54999	UDP	192.0.2.2	2777
RTP Assent	VCSc	VCSe	10.0.0.2	50000 to 54999	UDP	192.0.2.2	2776

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.

- 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.
- If a Cisco TMS server and a Syslog logging server are deployed (see the Optional configuration steps section) then the following NAT configuration is required:

Inbound (DMZ > Internal network)

Purpose	Source	Destination	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
Logging	VCSe	Syslog server	192.0.2.2	40000 to 49999	UDP	10.0.0.13	514
Management	VCSe	TMS server	192.0.2.2	>=1024	TCP	10.0.0.14	80 / 443
LDAP (for login, if required)	VCSe	LDAP server	192.0.2.2	40000 to 49999	TCP		389 / 636
NTP (time sync)	VCSe	NTP server	192.0.2.2	>=1024	UDP		123

Access to services such as DNS (UDP port 53) and NTP (UDP port 123) for time synchronization should be permitted on the appropriate firewall.

- Traffic destined for the Logging and 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
RTCP Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	2777
RTP Assent	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	2776
H.323 endpoints registering with public IP addresses							
RAS	Endpoint	VCSe	Any	1719	UDP	192.0.2.2	1719
Q.931/H.225	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	15000 to 19999
H.245	Endpoint	VCSe	Any	>=1024	TCP	192.0.2.2	1720
RTP & RTCP	Endpoint	VCSe	Any	>=1024	UDP	192.0.2.2	50000 to 54999
SIP endpoints registering using UDP / TCP or TLS							

Purpose	Source	Dest.	Source IP	Source port	Transport protocol	Dest. IP	Dest. port
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	50000 to 54999
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	60000 to 61799

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	50000 to 54999	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	50000 to 54999	UDP	Any	>=1024
TURN server media	VCSe	Endpoint	192.0.2.2	60000 to 61799	UDP	Any	>=1024
Other services (as required)							
DNS	VCSe	DNS server	192.0.2.2	10000 to 10210	UDP	DNS servers	53

Note: 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 the *VCS Administrator Guide* for port usage information.

NAT device configuration requirement

For more information regarding port usage, see *VCS IP Port Usage for Firewall Traversal Deployment Guide*.

Appendix 4 – Static NAT and Dual Network Interface architectures

Prerequisites

Deploying a VCS Expressway behind a NAT **mandates** the use of the **Dual Network Interfaces** 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-E 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.62] section later in this appendix.

When deploying a VCS-E behind a NAT with static NAT configuration in place on the VCS-E, 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-E (experience shows that these tend to be unable to handle video traffic properly).

Although the **Dual Network Interfaces** option is available for both the VCS Expressway and VCS Control, only the 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 Expressway in a NATed DMZ rather than having the 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-E 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-E LAN2 IP address 10.0.10.2:

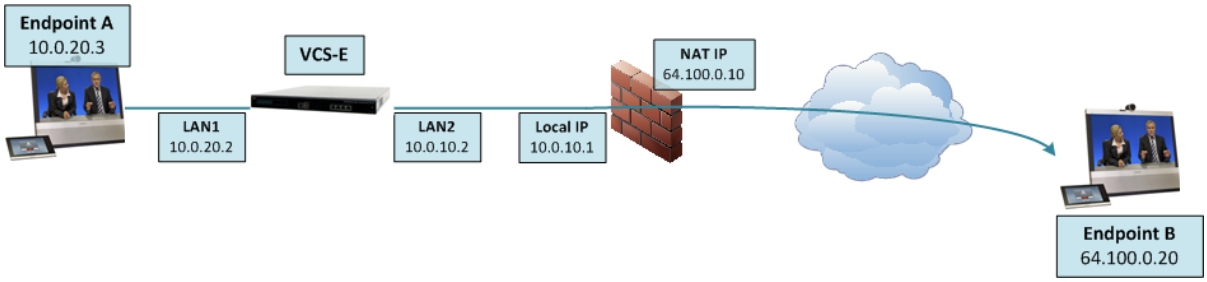


Figure 2: Example NAT deployment

- 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-E LAN1 (internally-facing interface) with IP address 10.0.20.2

- VCS-E LAN2 (externally-facing interface) with IP address 10.0.10.2 (and with static NAT disabled)
- VCS-E 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-E
- Endpoint B with IP address 64.100.0.20, located on the Internet, not registered to the Expressway

Assume that endpoint A places a SIP call towards endpoint B. The call will arrive at the VCS-E, which will proxy the SIP INVITE towards endpoint B. The VCS-E to Endpoint B will then be a traversal call, which means that the VCS-E 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-E 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-E 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 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).

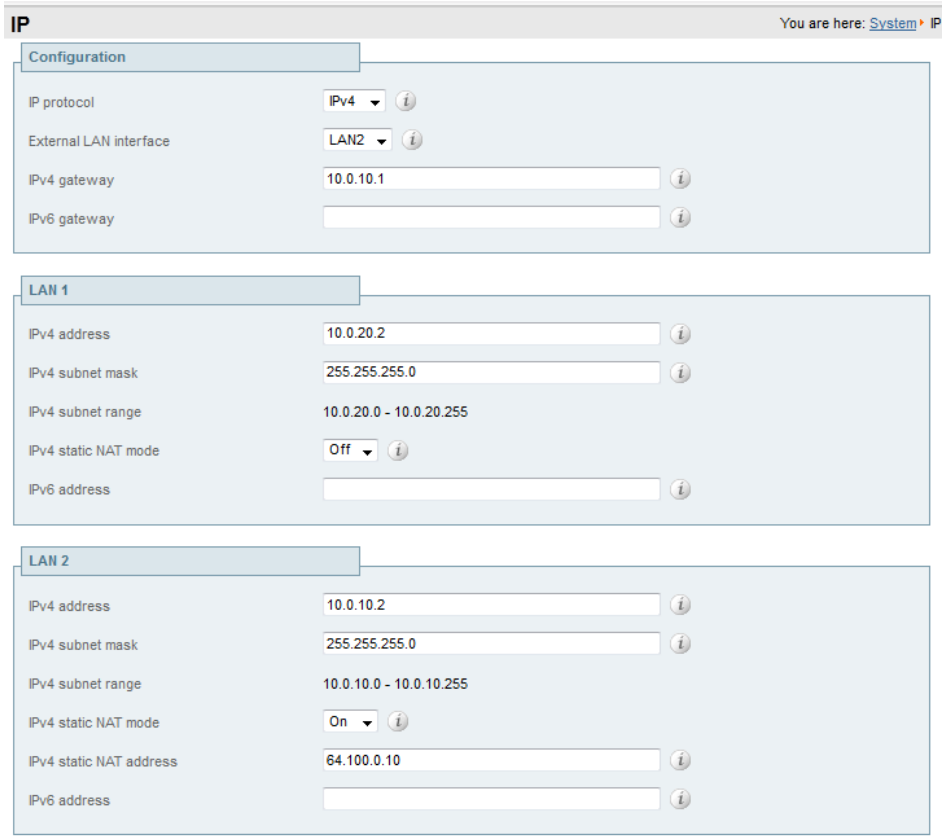
This can be achieved by enabling **Static NAT mode** on selected network interfaces on the Expressway. The Static NAT mode feature on the Expressway is made available with the **Dual Network Interfaces** option key.

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, even though they have been enabled; 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 **Dual Network Interfaces** key is installed on the VCS Expressway, the **IP** configuration page (**System > IP**) has additional options, allowing the user 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:



- 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 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 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 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 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 Expressway itself. This is also mentioned in Appendix 3 – Firewall and NAT configuration [p.54].

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 **Dual Network Interfaces** 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-E configuration, this should normally be set to the externally-facing LAN interface on the VCS-E.

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).

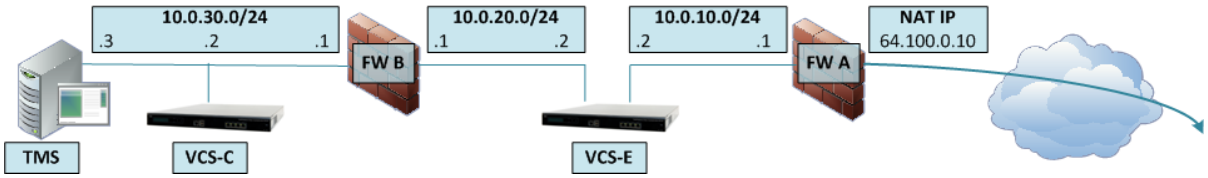


Figure 6: Dual network interfaces deployment

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-E – 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-E – 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-C – 10.0.30.2
  - the network interface of the 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-E)
- Firewall B is the internally-facing firewall
- VCS-E LAN1 has static NAT mode disabled
- VCS-E LAN2 has static NAT mode enabled with Static NAT address 64.100.0.10
- VCS-C has a traversal client zone pointing to 10.0.20.2 (LAN1 of the VCS-E)
- TMS has VCS-E 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-E 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-E 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-E (for example traversal client traffic from VCS-C 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-E. The VCS-E 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-C to LAN1 of the VCS-E 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-E 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-E 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-E LAN interface

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

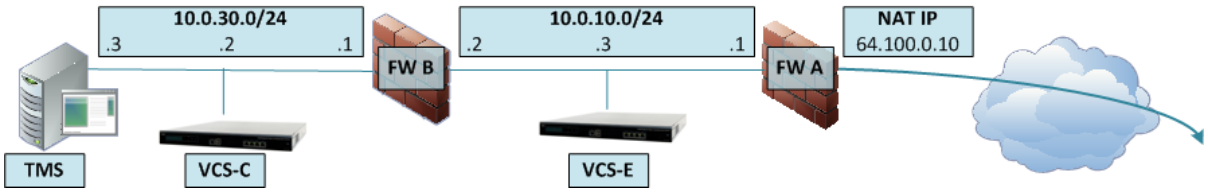


Figure 7: Single subnet DMZ using single LAN interface

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-E – 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-C – 10.0.30.2
  - the network interface of 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-E. **Static NAT mode** has been enabled for LAN1 on the VCS-E, with a static NAT address of 64.100.0.10.

The traversal client zone on the VCS-C needs to be configured with a peer address which matches the static NAT address of the VCS-E, in this case 64.100.0.10. This is because, since the VCS-E has static NAT mode enabled, it will request that incoming signaling and media traffic should be sent to its static NAT address, which means that the traversal client zone has to be configured accordingly.

This means that firewall A must allow traffic from the VCS-C 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-E 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-C to VCS-E communications will be to the 64.100.0.10 address of the VCS-E; the return traffic from the VCS-E to VCS-C might have to go via the default gateway. If a static route is added to the VCS-E so that reply traffic goes from the VCS-E 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-E can be added to TMS with the IP address 10.0.10.3 (or with IP address 64.100.0.10 if FW A allows this), since TMS management communications are not affected by static NAT mode settings on the VCS-E.

3-port firewall DMZ using single VCS-E LAN interface

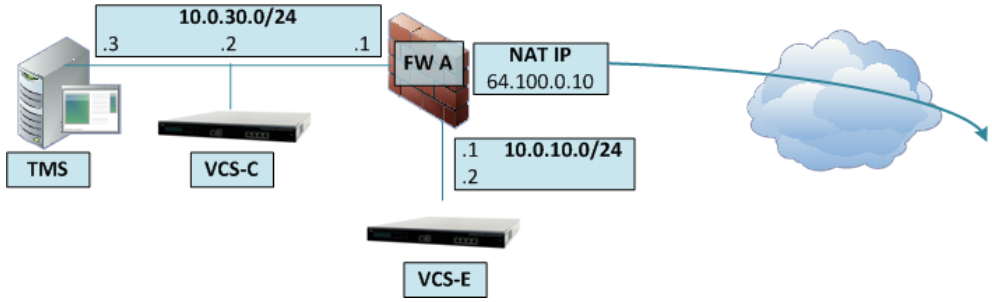


Figure 8: 3-port firewall DMZ using single VCS-E LAN interface

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-E - 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-C – 10.0.30.2
  - the network interface of 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-E. Static NAT mode has been enabled for LAN1 on the VCS-E, with a static NAT address of 64.100.0.10.

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

The traversal client zone on the VCS-C needs to be configured with a peer address which matches the static NAT address of the VCS-E, 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-E LAN interface".

This means that firewall A must allow traffic from the VCS-C 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-E can be added to TMS with the IP address 10.0.10.2 (or with IP address 64.100.0.10 if FW A allows this), since TMS management communications are not affected by static NAT mode settings on the VCS-E.

Checking for updates and getting help

If you experience any problems when configuring or using the product, consult the online help available from the user interface. The online help explains how the individual features and settings work.

If you cannot find the answer you need, check the web site at http://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,
- find further relevant documentation, for example product user guides, printable versions of the online help, reference guides, and articles that cover many frequently asked questions,
- get help from the Cisco Technical Support team. Click on Technical Support Overview for information on Accessing Cisco Technical Services. Make sure you have the following information ready before raising a case:
  - the serial number and product model number of the unit (if applicable)
  - the software build number which can be found on the product user interface (if applicable)
  - your contact email address or telephone number
  - a full description of the problem

Document revision history

Date	Description
November 2010	Initial release.
September 2011	Updated for X7.0.
March 2012	Updated for X7.1. Added Appendix 4 Static NAT and Dual Network Interface architectures.
August 2012	Updated for X7.2.
October 2012	Revised page layout.
January 2015	Corrected outbound source in Appendix 3.