



# Pexip Reverse Proxy and TURN Server Deployment Guide

## Introduction

In Pexip Infinity deployments, all Pexip Infinity Connect clients use HTTPS for the call signaling connections towards Conferencing Nodes.

However, with some Pexip deployments, these clients are not able to communicate directly with Pexip Conferencing Nodes, for example in on-prem deployments where the Pexip platform is located on an internal, enterprise LAN network while the clients are located in public networks on the Internet. In these cases it is common to deploy a reverse proxy application in the environment. This is an application which can proxy HTTP and HTTPS traffic from an externally-located client to a web service application located on the internal network — in our case a Pexip Conferencing Node. A reverse proxy can also be referred to as a load balancer.

In addition to providing HTTP/HTTPS connectivity between external Pexip clients and internal Conferencing Nodes, a reverse proxy can also be used for hosting customized Infinity Connect Web App content.

In deployments such as the ones described above, the reverse proxy provides for HTTPS call signaling connectivity between Infinity Connect WebRTC clients (Chrome, Firefox and Opera browsers and the desktop client) and Conferencing Nodes. However, to ensure audio/video/presentation connectivity between the two, a TURN server is also required.

A TURN server is a media relay/proxy which allows peers to exchange UDP or TCP media traffic whenever one or both parties are behind NAT. When Conferencing Nodes are deployed behind NAT, these nodes will instruct the WebRTC client to send its media packets to the TURN server, which will forward (relay) the packets to the Conferencing Nodes. Since this TURN server is normally located outside of the enterprise firewall, the Conferencing Node will constantly send media packets to this TURN server to "punch holes" in the firewall, allowing this TURN server to relay media packets back to the Conferencing Node, as the firewall will classify this as return traffic.

Pexip's Infinity Connect WebRTC clients (the desktop client; Web App for Chrome, Firefox and Opera; and mobile clients for iOS and Android) use ICE (Interactive Connectivity Establishment) to negotiate optimal media paths with Conferencing Nodes. Microsoft Lync and Skype for Business clients use a similar ICE mechanism, which means that Pexip can use TURN for all of these client types.

Note that Infinity Connect clients on Internet Explorer, Edge, and Safari browsers use the RTMP protocol, rather than WebRTC. While RTMP clients can connect to Conferencing Nodes via the reverse proxy, they cannot establish audio/video paths to Pexip Infinity via a TURN server. To establish audio/video media connectivity, RTMP clients need a direct TCP connection to a Conferencing Node.

## What's new in this release ?

**Version 3** of the OVA template was released in July 2014 and includes a number of new features including a TURN/STUN server and enhancements to the delivery of the participant list to the Infinity Connect client (formerly referred to as the WebRTC client).

**Version 2** of the OVA template was released in November 2013 and was extended to support proxying of WebRTC traffic from the Pexip Web App.

**Version 1** of the reverse proxy OVA template and Reverse Proxy Deployment Guide was released in October 2013 and provided support for proxying of Infinity Connect Mobile client traffic.

## About this guide

This guide provides design and configuration guidelines for using a reverse proxy and a TURN server with Pexip Infinity. When implementing a reverse proxy, any type of HTTPS reverse proxy/load balancer or TURN server may be used. However, this guide describes how to deploy these applications using the Reverse Proxy and TURN Server VMware appliance provided by Pexip.

This virtual VMware appliance is available as an OVA template which can be deployed on VMware ESXi 4/5. The virtual appliance contains both reverse proxy and TURN applications.

## Pexip Infinity version 9 or later

The examples and configuration described here apply to deployments that are using Pexip Infinity version 9 or later.

## Pexip Infinity version 8

If you are using Pexip Infinity version 8, some network topologies may require you to deploy two appliances, where one is used as a reverse proxy and the other is used for TURN – this is because Pexip Infinity version 8 does not allow separate, external STUN servers to be configured. If you are using Pexip Infinity version 8, refer to version 3.a of this guide.

## Deployment options

Depending on the network topology, the reverse proxy can be deployed with one or two network interfaces in various configurations:

- Single NIC, public address – see [Example deployment: single NIC on public address](#)
- Dual NIC, private and public addresses – see [Appendix 2: Alternative dual NIC reverse proxy/TURN server deployment](#)

In deployments with more than one Conferencing Node, the reverse proxy can load-balance HTTPS traffic between all Conferencing Nodes using a round-robin algorithm. A reverse proxy can also provide an authentication layer between Infinity Connect clients and Conferencing Nodes, for instance through an Active Directory or similar LDAP backend.

We recommend that the reverse proxy is configured with at least 3 Conferencing Nodes for resiliency as backend/upstream servers.

## Prerequisites

Ensure that the following prerequisites are in place:

- The Pexip Infinity deployment (i.e. a Management Node and at least one Conferencing Node) must be configured and in a working state.
- Appropriate DNS SRV records must have been created in accordance with [Using the reverse proxy with the Infinity Connect desktop client and Infinity Connect Mobile client](#).

## Security considerations

The Infinity Connect Mobile client and Infinity Connect can only use encrypted HTTPS when communicating with Conferencing Nodes. The reverse proxy must therefore provide HTTPS interfaces through which the Infinity Connect Mobile client and Infinity Connect clients can communicate.

When configured correctly, the reverse proxy will allow HTTPS traffic to flow between the Infinity Connect Mobile client / Infinity Connect clients and the internal Conferencing Nodes only. Externally located clients will not be able to access other internal resources through the reverse proxy.

We recommend that you install your own SSL/TLS certificates on the reverse proxy and TURN server for maximum security.

## Design principles and guidelines

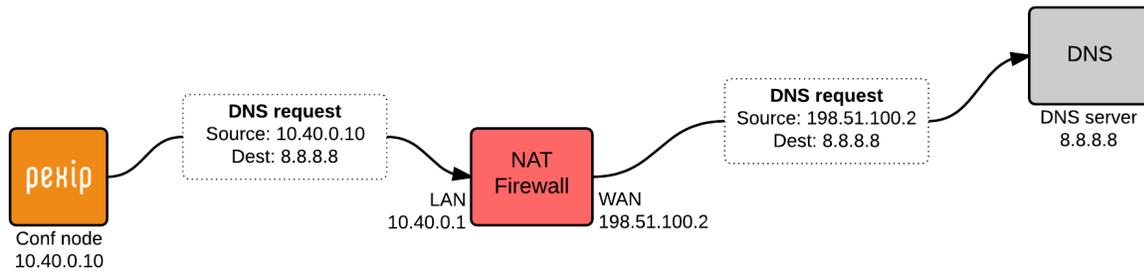
This section describes the network requirements for a reverse proxy and for a TURN server when deployed with Pexip Infinity.

A TURN server can also act as a STUN server, however, in some Pexip Infinity deployment scenarios you may need to configure a separate, external STUN server.

The **reverse proxy application** is responsible for proxying HTTP requests (via HTTPS) from clients (Infinity Connect Mobile client, and Infinity Connect WebRTC and desktop clients) to one or more Conferencing Nodes. To do this, the reverse proxy application must be able to communicate with both these externally-located clients as well as the Conferencing Nodes. This means that the reverse proxy must be able to reach the Conferencing Nodes either via a routed network or through NAT/port forwarding. The reverse proxy only needs to communicate with the Conferencing Nodes via HTTPS over TCP port 443 (when NAT/port forwarding is used to reach the Conferencing Nodes, the NATted port does not have to be 443, but the NAT/port forward must redirect to TCP/443 on the Conferencing Node).

The **TURN server application** is responsible for acting as a media relay between external clients and the Conferencing Nodes, so that these external clients can exchange RTP/RTCP media with the Conferencing Nodes. Conferencing Nodes communicate with the TURN server over a single UDP port (default UDP/3478).

Another key responsibility of the TURN server is to act as a STUN server for the Conferencing Nodes – when a Conferencing Node is deployed behind a NAT (from the perspective of clients located on the Internet), the Conferencing Node uses STUN towards the TURN server to discover its public NAT address. The Conferencing Node sends a STUN request to the TURN server, which responds back to the Conferencing Node and tells it from which IP address it received the STUN request. Using this method, the Conferencing Node can discover its public NAT address, which is important in order for ICE to work between the Conferencing Node and clients using ICE (such as Lync / Skype for Business clients and Infinity Connect WebRTC clients). In relation to TURN and ICE, this public NAT address is also known as the server reflexive address or simply reflexive address, and will be referred to as such throughout this section.



Using the above diagram as an example, the Conferencing Node has an IP address of 10.40.0.10 – this is a private/internal IP address which is not routable across public networks. When this Conferencing Node communicates with a host located on a public network (Internet), for instance a DNS server, traffic from this Conferencing Node passes through a NAT device (firewall/router), which will translate the source IP address for this traffic (10.40.0.10) to a public NAT address, in this case 198.51.100.2, before passing the traffic on to its destination. This means that when the DNS server receives the DNS request, the request will appear as coming from 198.51.100.2, which means that 198.51.100.2 is the **reflexive address** of the Conferencing Node.

For certain Lync / Skype for Business call scenarios to work correctly (notably RDP content sharing with external Lync / Skype for Business clients), it is essential that a Conferencing Node informs the remote Lync / Skype for Business client of this reflexive address. The Lync / Skype for Business client will in turn inform its Lync / Skype for Business Edge of this reflexive address so that the Edge server will relay media packets from the Conferencing Node to the Lync / Skype for Business client.

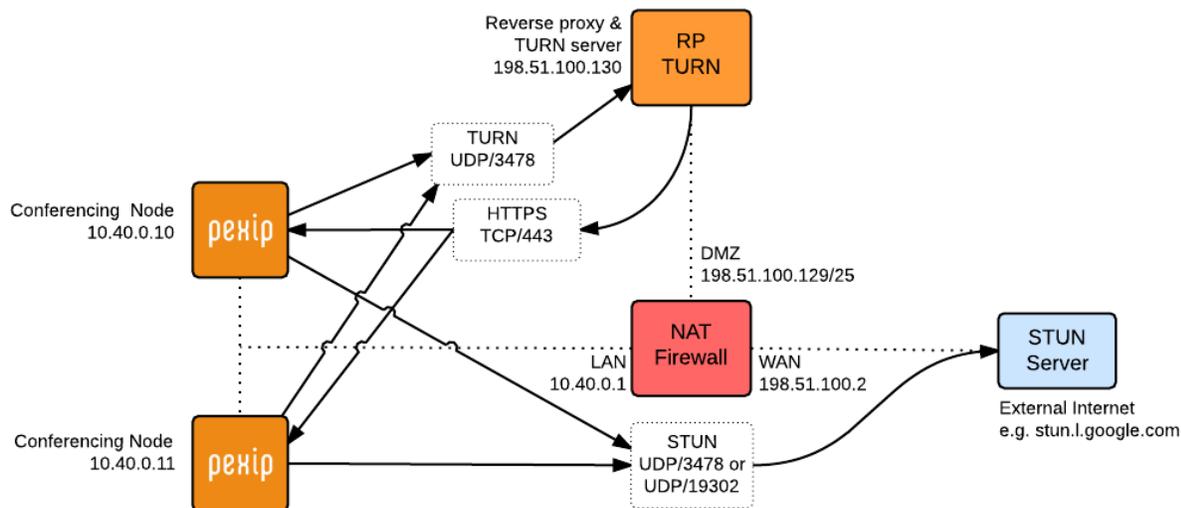
In some deployment scenarios where the TURN server is not located outside of the enterprise firewall — and thus sees traffic from the Conferencing Nodes as coming from its private address e.g. 10.40.0.10 — a Conferencing Node will not be able to discover its reflexive address (its public NAT address, e.g. 198.51.100.2) by sending its STUN requests to the TURN server. In this case you may need to configure Pexip Infinity with the address of a separate STUN server, such as [stun.l.google.com](https://stun.l.google.com), so that each Conferencing Node can discover its reflexive address.

## Example deployment: single NIC on public address

The diagram below depicts an example deployment where the reverse proxy and the TURN server application have been deployed with a single NIC on a public address.

The environment is split into two parts — an internal, private network segment and a DMZ network. The private network has two Pexip Infinity Conferencing Nodes, while the DMZ perimeter network contains the reverse proxy and TURN server.

**i** Note that all IP addresses in this guide are examples only — actual IP addressing will be deployment specific.



*Example deployment used in this guide: single NIC on public address*

This example forms the basis of this guide.

For this example deployment:

- Two Conferencing Nodes have been deployed in the LAN segment with IP addresses 10.40.0.10 and 10.40.0.11.
- The firewall in this scenario has three network interfaces:
  - LAN: 10.40.0.1/24
  - DMZ: 198.51.100.129/25
  - WAN: 198.51.100.2
- The DMZ network (198.51.100.129/25) can route network traffic to the LAN network (no NAT between LAN and DMZ).
- The reverse proxy and TURN server have been deployed in the DMZ subnet with IP address 198.51.100.130.
- As there is no NAT between the Conferencing Nodes in the LAN and the TURN server in the DMZ, the Conferencing Nodes have been configured to send their STUN requests to a STUN server in the public internet.
- The firewall has been configured to:
  - allow the reverse proxy to initiate HTTPS connections towards the Conferencing Node IP addresses
  - allow the Conferencing Nodes to send TURN packets to the TURN server on UDP port 3478
  - allow the Conferencing Nodes to send STUN packets to the STUN server, typically on UDP port 3478, although stun.l.google.com uses port 19302.

# Deploying the reverse proxy and TURN server using an OVA template

Pexip provides a preconfigured Reverse Proxy and TURN Server appliance via an OVA template suitable for deployment on VMware ESXi. This OVA template is provided "as-is" and provides a reference installation which will be suitable for typical Pexip deployments where:

- Conferencing Nodes are deployed in internal, private networks.
- The reverse proxy and TURN server is deployed in a DMZ environment using one or two network interfaces.

## Deployment steps

These steps involve:

- [Downloading the OVA template](#)
- [Deploying the OVA template](#)
- [Setting the password for SSH/console access](#)
- [Running the installation wizard](#)

## Downloading the OVA template

Download the Pexip RP/TURN OVA template from <http://download.pexip.com/rp-turn/v3/> to the PC running the vSphere client. Either the vSphere desktop client or web client can be used.

Note that there are two versions of the OVA file, one for ESXi 5.x and one for ESXi 4.x.

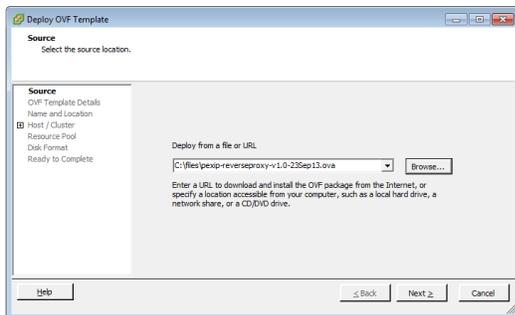
We recommend that you verify the OVA file integrity after downloading the OVA file by calculating the MD5 sum of the downloaded file (for instance using WinMD5 Free from [www.winmd5.com](http://www.winmd5.com)) and comparing that with the respective MD5 sum found in file `md5sums.txt` (located in the same download location as the OVA images).

## Deploying the OVA template

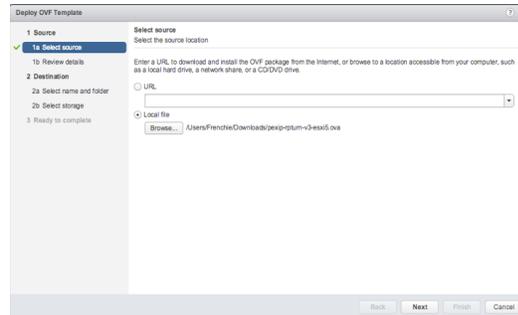
To deploy the OVA template:

- **vSphere Web Client:** go to **Hosts and clusters**, right-click on a host server and choose **Deploy OVF Template...**
- **vSphere Client for Windows:** go to **Hosts and clusters**, click **File** and **Deploy OVF Template.**

During the OVA deployment, we recommend that you use the default options. Also make sure to assign the correct VMware network/port group for the network interface of the virtual machine.



vSphere desktop client



vSphere web client

After the OVA template has been deployed, power on the newly-created virtual machine.

## Setting the password for SSH/console access

After the virtual machine has powered on, open the VMware console for the Reverse Proxy and TURN Server virtual machine, right-click on the virtual machine in the vSphere client and choose **Open Console**.

```

Ubuntu 12.04.4 LTS rp tty1
rp login: pexip
You are required to change your password immediately (root enforced)
Enter new UNIX password:
Retype new UNIX password:

#####
#
#      Pexip Reverse Proxy/TURN v3      #
#
#####

[sudo] password for pexip: _
    
```

### Initial login prompt and install wizard prompt

Before you can start the install wizard, you must change the password. To do this:

1. Log in as user **pexip** (this is case sensitive).
2. You are prompted to set a new account password. To do this you must enter the new password twice.
3. After setting the new password, the **Pexip Reverse Proxy/TURN** banner is shown, and you are prompted to enter the new password again.  
After this password has been entered, the install wizard will start.

## Running the installation wizard

The installation wizard is divided into several steps, which are explained below. Some steps require a single line of input, while others allow multiple lines of input to be entered, one line at a time. Some steps also allow multiple entries on the same line.

The configuration example described here is based on the [Example deployment: single NIC on public address](#), with the following additional assumptions:

- The reverse proxy and TURN server interface (198.51.100.130) resides in the same subnet as its default gateway (198.51.100.129).
- Router 10.40.0.1 is the next hop when accessing all internal hosts. The internal networks are defined by CIDR 10.0.0.0/8 (10.0.0.0-10.255.255.255).
- Hosts residing in the internal network 10.0.50.0/24 will access the reverse proxy and the TURN server over SSH.

**i** Note that all IP addresses in this guide are examples only — actual IP addressing will be deployment specific.

The following table shows, for each step, the prompt text that is shown, the example text you should input, and an explanation of the step.

Step	Prompt text	Example input	Explanation for this example deployment
1	IP address	198.51.100.130 [ENTER]	198.51.100.130 is the IP address of the reverse proxy/TURN server interface.  If the intention is to have dual NICs, specify the address of the internally-facing NIC (see <a href="#">Configuring a second NIC</a> ).
2	Subnet mask	255.255.255.0 [ENTER]	The reverse proxy/TURN server has a network mask of 255.255.255.0.
3	Default Gateway	198.51.100.129 [ENTER]	The reverse proxy/TURN server has a default gateway of 198.51.100.129.

Step	Prompt text	Example input	Explanation for this example deployment
4	Network address and subnet mask of network/host allowed to access this host over SSH	10.0.50.0 [SPACE] 255.255.255.0 [ENTER]	10.0.50.0 is the network address and 255.255.255.0 is the subnet mask of the enterprise's management network that is allowed to access this host over SSH.
5	Hostname	proxy [ENTER]	The reverse proxy has a hostname of <b>proxy</b> . The hostname and domain (configured in the next step) must match the actual DNS name by which the reverse proxy will be addressed ( <b>proxy.example.com</b> ).
6	Domain suffix	example.com [ENTER]	The reverse proxy has a domain name/suffix of <b>example.com</b> . This means, since the host name in the previous step was configured as <b>proxy</b> , that the full FQDN of this reverse proxy is <b>proxy.example.com</b> .  If a custom SSL certificate is created for this reverse proxy, this FQDN needs to match the Subject Name and Subject Alternate Name of the SSL certificate. For more information, see <a href="#">Replacing the default SSL certificate</a> .
7	DNS server(s), space separated	8.8.8.8 [SPACE] 8.8.4.4 [ENTER]	The reverse proxy is configured to use DNS servers <b>8.8.8.8</b> and <b>8.8.4.4</b> . DNS is in this case mainly used to resolve the hostnames of NTP servers.
8	NTP server(s), space separated	0.no.pool.ntp.org [SPACE] 1.no.pool.ntp.org [SPACE] 2.no.pool.ntp.org [ENTER]	The reverse proxy is configured to use three different pools of NTP servers, to ensure proper NTP time synchronization.  We recommend that at least three NTP servers are used.
9	Enter the IP address of each conference node separately, followed by [ENTER].  Press [ENTER] on an empty line to finish entering conference nodes: Enter IP of next conference node or press [ENTER] if finished	10.40.0.10 [ENTER] 10.40.0.11 [ENTER] [ENTER]	Here, the IP addresses of both Pexip Conferencing Nodes are input, one at a time – <b>10.40.0.10</b> is the first Conferencing Node and <b>10.40.0.11</b> is the second Conferencing Node.  (If you are deploying a TURN server only, input '169.254.0.1' followed by <ENTER>. 169.254.0.1 is a link-local IP address which is not used in production networks.)
10	Choose a space-separated username and password to enable the built in TURN server  Enter 'disable' to disable the built in TURN Server  Example: someusername [SPACE] somepassword [ENTER]	pexip [SPACE] admin123 [ENTER]	When deploying the TURN server application, you must enter some credentials, for example, entering:  pexip [SPACE] admin123 [ENTER]  would set the username to 'pexip' with a password of 'admin123'.  These are the credentials you would use when configuring Pexip Infinity with the access details for this TURN server.  (If you are deploying the reverse proxy only, input 'disable'.)

When all of the installation wizard steps have been completed, the appliance will automatically reboot.

After the appliance has started up again it will be ready for use — Infinity Connect Mobile client and Infinity Connect users will now be able to access Virtual Meeting Rooms from outside your network.

## Restoring the Reverse Proxy and TURN Server to its default state

If you need to re-run the install wizard (for instance if additional Conferencing Nodes have been added to the environment and therefore should be included in the reverse proxy configuration), you must first reset the appliance to its original default state. To do this:

1. Open the console of the virtual machine (or otherwise log in via SSH).
2. Log in as user `pexip`.
3. Run the following command:  

```
sudo reset_to_default_settings.sh
```
4. You are presented with a warning asking if you wish to continue. Enter `y`.
5. You are asked whether you want to delete or keep the log files which exist on the Reverse Proxy and TURN Server. Enter `y` or `n` as appropriate.
6. You are asked whether you want to reboot the virtual machine. Enter `y`.

After the appliance has rebooted and restarted, you can re-run the install wizard by logging in as user `pexip`, setting a new password and following the steps in [Running the installation wizard](#).

## Replacing the default SSL certificate

If you want to replace the built-in X.509 SSL certificate on the reverse proxy with a custom-created certificate, the following procedure should be performed:

1. Create a text file called `pexip.pem` which contains the following items in this specific order:
  - server certificate
  - server private key (which must be unencrypted)
  - one or more intermediate CA certificates (a server certificate will normally, but not always, have one or more intermediate CA certificates)

Note that the contents MUST be in this specific order for the certificate to work properly.

The first section with the server certificate should contain a single entry starting and ending with the following:

```
----- BEGIN CERTIFICATE ----- / ----- END CERTIFICATE -----
```

The second section with the server private key should contain a single entry starting and ending with the following (although it may instead show 'BEGIN RSA PRIVATE KEY'):

```
----- BEGIN PRIVATE KEY ----- / ----- END PRIVATE KEY -----
```

Finally, there will normally be one or more intermediate CA certificates, where each intermediate has a section starting and ending with:

```
----- BEGIN CERTIFICATE ----- / ----- END CERTIFICATE -----
```

2. Using the SCP file transfer protocol, upload the `pexip.pem` file to the `/tmp` folder of the Reverse Proxy and TURN Server. This can be done using for instance WinSCP ([www.winscp.net](http://www.winscp.net)) or the 'scp' command-line utility for Linux/Mac OS X, using a command such as:

```
scp pexip.pem pexip@198.51.100.130:/tmp
```

3. After the `pexip.pem` file has been transferred into the `/tmp` folder of the reverse proxy, connect over SSH to the reverse proxy, log in as user `pexip` and run the following commands, one at a time:

```
sudo cp /etc/nginx/ssl/pexip.pem /etc/nginx/ssl/pexip.pem.backup
```

```
sudo mv /tmp/pexip.pem /etc/nginx/ssl/pexip.pem
```

```
sudo service nginx restart
```

Note that `sudo service nginx restart` will restart the reverse proxy application and therefore interrupt the service briefly.

After these commands have been run, the reverse proxy should now be operational and using the new certificate.

If any problem occurs with the replaced certificate, the previous certificate can be restored using the following commands:

```
sudo cp /etc/nginx/ssl/pexip.pem.backup /etc/nginx/ssl/pexip.pem
```

```
sudo service nginx restart
```

## Using the reverse proxy and TURN server with Infinity Connect and Lync / Skype for Business clients

Infinity Connect clients can connect directly to a Conferencing Node, but this will not provide a mechanism for balancing load between multiple Conferencing Nodes, or failing over in the event of a node failure. In addition, many customers may deploy Conferencing Nodes in a private network but would like to also provide access to external users using the Infinity Connect Web App.

To resolve these issues, a reverse proxy in the DMZ can be used to forward the HTTPS traffic from the browser to the Conferencing Nodes, and a TURN server can be used to forward media from a private network to the public Internet.

Microsoft Lync and Skype for Business clients can also use the TURN server to relay media to the Conferencing Node. It may also be necessary to configure Pexip Infinity with the address of a separate STUN server, such as [stun.l.google.com](https://stun.l.google.com), so that each Conferencing Node can discover its reflexive address, which is essential for certain Lync / Skype for Business call scenarios to work correctly.

This section describes how to:

- connect to the reverse proxy from Infinity Connect clients and the Infinity Connect Mobile client
- configure the Pexip Infinity platform with details of the TURN server
- configure the Pexip Infinity platform with details of a STUN server.

### Using the reverse proxy and TURN server with Infinity Connect Web App

When the reverse proxy has been deployed, Infinity Connect users with WebRTC-compatible browsers can access conferences via <https://<reverse-proxy>/webapp/>, where **<reverse-proxy>** is the FQDN of the reverse proxy. This mechanism uses HTTPS for accessing the web pages and conference controls, and RTP/RTCP for the media streams (via a TURN server if necessary).

Note that if the reverse proxy is not available, Infinity Connect Web App users can connect via <https://<node>/webapp/>, where **<node>** is the IP address or URL of the Conferencing Node.

### Using the reverse proxy with the Infinity Connect desktop client and Infinity Connect Mobile client

The Infinity Connect desktop client and Infinity Connect Mobile client work by sending HTTP GET and POST requests to a specific destination address to fetch information about a meeting (such as the participant list) and to send various commands (such as to mute or remove conference participants).

Clients discover the destination address for those HTTP requests through a custom DNS SRV lookup for **\_pexapp.\_tcp.<domain>**. For instance, if the Infinity Connect desktop client or Infinity Connect Mobile client has been configured with a meeting URI of **meet.alice@example.com**, it will perform a DNS SRV lookup for **\_pexapp.\_tcp.example.com**.

Assume that the following **\_pexapp.\_tcp.example.com** DNS SRV records have been created:

```
_pexapp._tcp.example.com. 86400 IN SRV 10 100 443 proxy1.example.com.  
_pexapp._tcp.example.com. 86400 IN SRV 20 100 443 proxy2.example.com.
```

These point to the DNS A-records **proxy1.example.com**, port 443 (HTTPS), with a priority of 10 and a weight of 100, and **proxy2.example.com**, port 443, with a relatively lower priority of 20 and a weight of 100.

- This tells the Infinity Connect desktop client to initially send its HTTP requests to host **proxy1.example.com** (our primary reverse proxy server) on TCP port 443. The desktop client will also try to use host **proxy2.example.com** (our fallback server) if it cannot contact proxy1.
- The Infinity Connect Mobile client will send its HTTP requests either to **proxy1.example.com** or to **proxy2.example.com**, depending on the order of the returned SRV records. If it fails to contact the first host, it will not attempt to contact the second host address.

The connection logic in this example is explained in more detail below for each client. (Note that this section describes the operation of version 2.1 of the Infinity Connect desktop client; earlier versions of the desktop client operate in the same way as the Infinity Connect Mobile client.)

## Infinity Connect desktop client

In this example, when a user attempts to access `meet.alice@example.com`, the Infinity Connect desktop client will attempt an SRV lookup on `_pexapp._tcp.example.com`:

- If the SRV lookup succeeds, it will return the records shown above, and the Infinity Connect desktop client will attempt to contact **proxy1.example.com** (the record with the highest priority) on TCP port 443.  
If it cannot contact **proxy1.example.com** it will next try to contact **proxy2.example.com**.
- If it fails to contact either host, or the SRV lookup fails, and neither a **serverAddress**, **Connection server address** nor a **Registration server address** have been specified, the desktop client will report that it has failed to contact a server.
- If any of the **serverAddress**, **Connection server address** or a **Registration server address** have been specified, and are for a different domain to that of the dialed alias (`example.com` in this case) the Infinity Connect desktop client will perform SRV lookups on those other domains, and attempt to contact the hosts returned in those lookups. For example, if the **Connection server address** is `localserver.example.com` then it will perform an SRV lookup on `_pexapp._tcp.localserver.example.com`.
- If each subsequent SRV lookup fails, or the returned hosts in those lookups cannot be contacted, the Infinity Connect desktop client will also attempt to connect directly to that domain, for example to `http://localserver.example.com:443` (via DNS A-records for `localserver.example.com`).

## Infinity Connect Mobile client

In this example, when a user attempts to access `meet.alice@example.com`, the Infinity Connect Mobile client will attempt an SRV lookup on `_pexapp._tcp.example.com`:

- If the SRV lookup succeeds, it will return the records shown above, and the Infinity Connect Mobile client will attempt to contact the first host in the returned list on TCP port 443. Note that the addresses are returned in an arbitrary order and thus the first host may be either **proxy1.example.com** or **proxy2.example.com**.
- If the SRV lookup fails, or it fails to contact the first host on the returned list, the Infinity Connect Mobile client will attempt to connect to `http://example.com:443` (via DNS A-records for `example.com`).

(Note that for the Android client, this example assumes that a **Connection server address** is not configured on the client. If a connection server address is specified, it would be used instead of the domain portion of the dialed conference address i.e. `example.com` in this case.)

Note that the Infinity Connect Mobile client will keep polling the reverse proxy periodically to update the participant list for a given virtual meeting room for as long as the application is active.

## Configuring Pexip Infinity to use a TURN server

To relay media between the internal and external networks, a TURN server must be used. In addition to Pexip's TURN Server appliance, many other commercial TURN servers exist, including those on products such as a VCS Expressway, or those deployed using commercial or free software such as `restund` or `rfc5766-turn-server`.

To use the Pexip TURN server, you must be running Pexip Infinity version 6 or later software.

The TURN server's details must be configured on the Pexip Infinity platform, and each location must nominate the TURN server that will be used automatically to forward media when required. To do this:

1. Go to **Call control > TURN servers**, and add details of the TURN server(s) to be used.

### Add TURN server

<b>Name</b>	<input type="text" value="Pexip TURN"/> *	<small>The name used to refer to this TURN server. Maximum length: 250 characters.</small>
<b>Description</b>	<input type="text"/>	<small>A description of the TURN server. Maximum length: 250 characters.</small>
<b>IP address</b>	<input type="text" value="198.51.100.130"/> *	<small>The IP address of the TURN server.</small>
<b>Port</b>	<input type="text" value="3478"/> *	<small>The IP port on the TURN server to which the Conferencing Node will connect. Range: 1 to 65535. Default: 3478.</small>
<b>Username</b>	<input type="text" value="pexip"/>	<small>The username of a valid account on the TURN server. Maximum length: 100 characters.</small>
<b>Password</b>	<input type="password" value="••••••"/>	<small>The password of a valid account on the TURN server. Maximum length: 100 characters.</small>

2. Go to **Platform configuration > Locations**, and for each location, select the TURN server to be used for that location.

<b>SIP proxy</b>	<input type="text" value="-----"/> +	<small>The SIP proxy to be used for outbound calls from this location. For more information, see <a href="#">About H.323 gatekeepers and SIP proxies</a>.</small>
<b>Lync server</b>	<input type="text" value="-----"/> +	<small>The Lync server to be used for outbound calls from this location. For more information, see <a href="#">About Lync servers</a>.</small>
<b>TURN server</b>	<input type="text" value="Pexip TURN"/> +	<small>The TURN server to be used when ICE clients (including Lync clients and Infinity Connect WebRTC clients) located outside the firewall connect to a Conferencing Node in this location. For more information, see <a href="#">About TURN servers</a>.</small>
<b>STUN server</b>	<input type="text" value="-----"/> +	<small>The STUN server to be used by Conferencing Nodes in this location to determine the public IP address to signal to ICE clients (including Lync clients and Infinity Connect WebRTC clients) located outside the firewall.</small>

## Configuring Pexip Infinity to use a STUN server

A STUN server allows clients, such as Conferencing Nodes, to find out their public NAT address. In Microsoft Lync and Skype for Business deployments it is essential that a Conferencing Node can discover its public NAT address.

By default, Conferencing Nodes will send their STUN requests to the TURN server, but if the TURN server is not located outside of the enterprise firewall — the Conferencing Node will not be able to discover its public NAT address. If this is the case in your deployment scenario, you must configure a separate STUN server. The Conferencing Node's STUN requests will then be sent to the STUN server, instead of the TURN server.

You do not need to configure STUN servers if the STUN requests sent from the Conferencing Nodes to the TURN server will return the public NAT address of the Conferencing Node.

To configure STUN servers, you must be running Pexip Infinity version 9 or later software.

## How Conferencing Nodes decide which STUN server to use

The STUN server used by a Pexip Infinity Conferencing Node handling a call is determined as follows:

- **Conferences:** uses the STUN server associated with the location of the Conferencing Node that is handling the call signaling.
- **Point-to-point calls via the Pexip Distributed Gateway:** uses the STUN server associated with the Gateway Routing Rule that matched the call request. If there is no STUN server associated with the rule, then the STUN server associated with the location

of the Conferencing Node that is handling the call signaling is used instead. Note that rules can optionally be configured on a per-location basis.

If a STUN server is not configured for a location or rule, but a TURN server is configured, the Conferencing Node will send STUN requests to that TURN server.

## Nominating the STUN servers used by Pexip Infinity

Within Pexip Infinity you can configure the addresses of one or more STUN servers. You then associate those STUN servers with each System location and with each Gateway Routing Rule.

### Configuring STUN server addresses

To add, edit or delete STUN server connection details, go to **Call control > STUN servers**. The options are:

Option	Description
Name	The name used to refer to this STUN server in the Pexip Infinity Administrator interface.
Description	An optional description of the STUN server.
Address	The IP address or hostname of the STUN server. This should not be the same address as any of your configured TURN servers.
Port	The IP port on the STUN server to which the Conferencing Node will connect. Default: 3478.

Note that Pexip Infinity ships with one STUN server address already configured by default: **stun.l.google.com**. This STUN server is typically used by Infinity Connect WebRTC clients and uses port 19302 (rather than the common 3478).

You can use this STUN server or configure a different one.

#### Select STUN server to change

Action:   0 of 1 selected

	Name	Address	Description
<input type="checkbox"/>	stun.l.google.com	stun.l.google.com	

1 STUN server

## Associating STUN server addresses with Conferencing Nodes

To associate a STUN server address with a Conferencing Node, you must configure the node's system location:

1. Go to **Platform configuration > Locations**.
2. Select the Conferencing Node's location.
3. Select a **STUN server** and select **Save**.

All Conferencing Nodes in that location will use the nominated STUN server for conference calls.

SIP proxy    
The SIP proxy to be used for outbound calls from this location. For more information, see [About H.323 gatekeepers and SIP proxies](#).

Lync server    
The Lync server to be used for outbound calls from this location. For more information, see [About Lync servers](#).

TURN server    
The TURN server to be used when ICE clients (including Lync clients and Infinity Connect WebRTC clients) located outside the firewall connect to a Conferencing Node in this location. For more information, see [About TURN servers](#).

STUN server    
The STUN server to be used by Conferencing Nodes in this location to determine the public IP address to signal to ICE clients (including Lync clients and Infinity Connect WebRTC clients) located outside the firewall.

### Client STUN servers

Note that the per-location **Client STUN servers** option is used to configure the specific STUN server addresses that are provisioned to Infinity Connect WebRTC clients. These STUN servers are used by the WebRTC client to discover its public NAT address.

### Associating STUN server addresses with gateway calls

If a gateway call is being placed to an ICE-enabled client (such as Lync / Skype for Business clients and Infinity Connect WebRTC clients), the Conferencing Node placing the call will use the STUN server associated with the matching rule. (For gateway calls, the Conferencing Node does not use the STUN sever associated with its system location.)

To associate a STUN server address with a Gateway Routing Rule:

1. Go to **Service configuration > Distributed Gateway**.
2. Select the relevant rule.
3. Select a **STUN server** and select **Save**.

SIP proxy	Use DNS ▾ +	The SIP proxy to be used for outbound SIP calls. For more information, see <a href="#">About H.323 gatekeepers and SIP proxies</a> . To try to use normal SIP resolution procedures to route the call, select <b>Use DNS</b> .
Lync server	Use DNS ▾ +	The Lync server to be used for outbound Lync (MS-SIP) calls. For more information, see <a href="#">About Lync servers</a> . To try to use normal Lync (MS-SIP) resolution procedures to route the call, select <b>Use DNS</b> .
TURN server	Pexip TURN ▾ +	The TURN server to be used for outbound Lync (MS-SIP) calls (where applicable). For more information, see <a href="#">About TURN servers</a> .
STUN server	stun.l.google.com ▾ +	The STUN server to be used for outbound Lync (MS-SIP) calls (where applicable).

## Appendix 1: Firewall ports

### Traffic between the reverse proxy and TURN server and clients in the Internet

The following ports have to be allowed through any firewalls which carry traffic between the reverse proxy and TURN server in the DMZ and the Infinity Connect Mobile client and Infinity Connect clients in the public Internet:

Purpose	Direction	Source IP	Protocol	Port	Destination IP
HTTP/HTTPS	Inbound	<any>	TCP	80 / 443	Reverse proxy
UDP TURN/STUN	Inbound	<any>	UDP	3478	TURN server
TURN relay media	Inbound	<any>	UDP	49152–65535	TURN server
RTP media	Outbound	TURN server	UDP	<any>	<any>
DNS	Outbound	Reverse proxy and TURN server	TCP/UDP	53	DNS server
NTP	Outbound	Reverse proxy and TURN server	TCP	123	NTP server

### Traffic between the local network and the DMZ / Internet

The following ports have to be allowed through any firewalls which carry traffic between Conferencing Nodes and management stations in the local network and the reverse proxy and TURN server in the DMZ/internet:

Purpose	Direction	Source IP	Protocol	Port	Destination IP
HTTPS	Inbound	Reverse proxy	TCP	443	Conferencing Nodes
UDP TURN/STUN	Outbound	Conferencing Nodes	UDP	3478	TURN server
UDP TURN/STUN	Outbound	Conferencing Nodes	UDP	3478 / 19302	STUN server (if configured). Note that stun.l.google.com uses port 19302.
SSH	Outbound	Management PC	TCP	22	Reverse proxy and TURN server

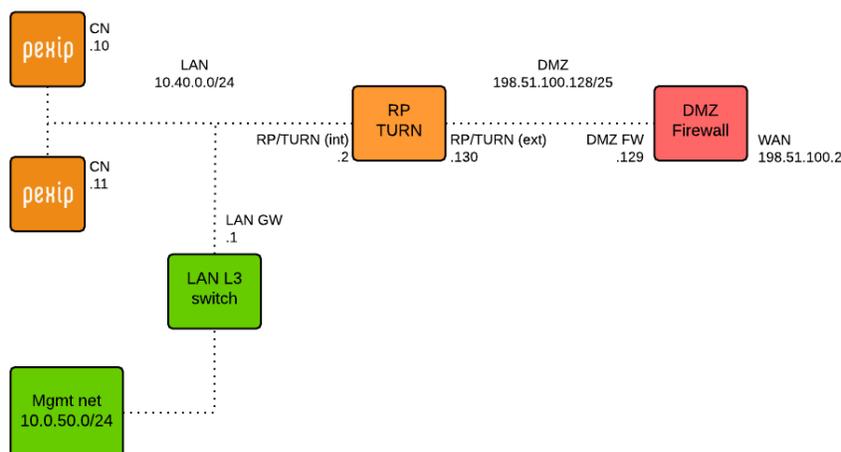
## Appendix 2: Alternative dual NIC reverse proxy/TURN server deployment

This section shows an alternative dual NIC network configuration for the reverse proxy and TURN server.

### Dual NIC public/private address with routing to alternative VLAN for management

In this example, the environment is split into two parts: an internal, private network segment and a DMZ network. The private network has two Pexip Infinity Conferencing Nodes and the reverse proxy/TURN server internal interface, while the DMZ perimeter network contains the reverse proxy/TURN server external interface.

**i** Note that all IP addresses in this guide are examples only — actual IP addressing will be deployment specific.



The reverse proxy/TURN server in this case has two network interfaces:

- An internal facing interface (IP address 10.40.0.2) which is connected to the internal LAN network.
- An external facing interface (IP address 198.51.100.130) which is connected to the DMZ network.

The internal interface of the reverse proxy/TURN server is configured on the same subnet as the Conferencing Nodes, while the external interface of the reverse proxy/TURN server is configured on the DMZ subnet. The Conferencing Nodes use 10.40.0.1 as their default gateway. This is also the gateway to the 10.0.50.0/24 management network, from where SSH connections to the internal interface of the reverse proxy/TURN server will originate.

There is no NAT between the outside and the DMZ network segment. The reverse proxy/TURN server uses the DMZ firewall 198.51.100.129 as its default gateway, and is also configured with a static route to the 10.0.50.0/24 management network via the LAN gateway at 10.40.0.1 so that SSH management traffic from this management network can function.

To deploy the reverse proxy/TURN server in this configuration:

1. Deploy the Reverse Proxy and TURN Server appliance OVA file and power on the VM instance.
2. In the install wizard, define the network configuration (steps 1 and 2 in the install wizard) for what will be the internal interface of the reverse proxy/TURN server (10.40.0.2 in this example).
3. For the default gateway (step 3), configure the LAN gateway (10.40.0.1).
4. For the trusted hosts/networks (step 4), configure 10.0.50.0 255.255.255.0.
5. After the install wizard completes, the reverse proxy/TURN server will reboot with the new configuration. When it is back up, connect over SSH to the reverse proxy from a host in the management network (or log in via the VMware console) as user 'pexip' and shut down the virtual machine using the following command:

```
sudo shutdown -h now
```

Input the password for user 'pexip' when prompted by sudo.

6. After the VM has been shut down, add one additional network interface to this VM instance and power it on again.
7. Log in to the reverse proxy/TURN server through SSH or VMware console and add the network configuration for the external network interface (198.51.100.130 in this example) and the static route configuration to `/etc/network/interfaces`, as described in [Configuring a second NIC](#).

In this example, the resulting `/etc/network/interfaces` file should contain the following (note that the existing gateway entry for interface `eth0` is removed as the reverse proxy/TURN server should only have one default gateway defined):

```
auto lo eth0 eth1
iface lo inet loopback

iface eth0 inet static
    address 10.40.0.2
    netmask 255.255.255.0

iface eth1 inet static
    address 198.51.100.130
    netmask 255.255.255.128
    gateway 198.51.100.129
    dns-nameservers 8.8.8.8 8.8.4.4

post-up route add -net 10.0.50.0 netmask 255.255.255.0 gw 10.40.0.1
```

To ensure that the `eth0` and `eth1` interfaces correspond with the correct port group in VMware, running the `ifconfig` command on the reverse proxy/TURN server will show the hardware MAC addresses of each interface, so that these can be matched against the virtual interfaces in VMware.

8. Reboot the reverse proxy/TURN server VM to apply the new network settings.

## STUN server configuration

If the reverse proxy/TURN server is deployed with a dual NIC public/private address, then Conferencing Nodes will typically not be able to discover their public NAT addresses as they will be sending their STUN requests to the internal interface of the TURN server.

Therefore, you will need to configure Pexip Infinity with a separate STUN server (see [Configuring Pexip Infinity to use a STUN server](#)).

## Appendix 3: Advanced configuration

This section describes some advanced configuration scenarios for the reverse proxy and TURN server:

### Adding or removing Conferencing Nodes from an existing reverse proxy configuration

To add an additional Conferencing Node, or to remove a Conferencing Node from an existing reverse proxy configuration:

1. Run the following command to edit the Reverse Proxy and TURN Server config file:

```
sudo nano /etc/nginx/sites-enabled/pexapp
```

2. To add a Conferencing Node:

In sections `upstream pexip` and `upstream pexip-webrtc` at the top of the config file, add additional `server` statements. In these additional entries, specify the IP address of each additional Conferencing Node; other parameters should be similar to the existing entries.

3. To remove a Conferencing Node:

In sections `upstream pexip` and `upstream pexip-webrtc` at the top of the config file, remove the `server` statements that specify the IP address of each Conferencing Node to be removed.

4. After editing the file, run the following command to reload the nginx configuration gracefully (not interrupting any existing sessions):

```
sudo service nginx reload
```

### Configuring NAT for the TURN server

To configure NAT, run the following command to edit the TURN server configuration:

```
sudo nano /etc/turnserver.conf
```

Anywhere in the config file, add the parameter `external-ip=1.2.3.4`, where `1.2.3.4` is the public NAT address of the TURN server.

After editing the file, run the following command to make the configuration change take effect:

```
sudo service rfc5766-turn-server restart
```

Note that this will interrupt any existing TURN sessions (e.g. any WebRTC or Lync / Skype for Business calls going via the TURN server), therefore these changes should be performed during a maintenance window that is outside of normal operating hours.

### Configuring a second NIC

- i** The first, existing NIC must be the internally-facing NIC. When a reverse proxy is deployed and the intention is to have dual NICs, the network configuration provided during the install wizard must be the internally-facing NIC, as SSH access will only be enabled for this initial NIC.

To configure a second NIC, run the following command to edit the network configuration file:

```
sudo nano /etc/network/interfaces
```

The existing interfaces file will be similar to this:

```
# >/etc/network/interfaces
# Written at 2014-04-23 10:30:34 UTC by InterfacesFileWriter
auto lo eth0
iface lo inet loopback

iface eth0 inet static
    address 10.40.0.2
    netmask 255.255.255.0
    gateway 198.51.100.129
    dns-nameservers 8.8.8.8 8.8.4.4
```

To add a second NIC:

1. Change the line `auto lo eth0` to `auto lo eth0 eth1`.
2. Create a new section called `iface eth1 inet static`, and create entries for `address`, `netmask`, `gateway` and `dns-nameservers`.
3. Remove the existing `gateway` parameter for `eth0` (as `eth0` will now be the internally-facing interface and thus should not have a default gateway; the default gateway should belong to the externally-facing `eth1`).

### Important: static routes

If any static routes are needed in this scenario (which is usually the case unless the reverse proxy does not need to access any hosts outside of the internal `eth0` subnet), these have to be defined at the bottom of the interfaces file, using syntax as follows:

```
post-up route add -net 10.0.50.0 netmask 255.255.255.0 gw 10.40.0.1
```

The above entry will create a static route for `10.0.50.0/24` via `10.40.0.1`.

The resulting interfaces file will then look like this:

```
# >/etc/network/interfaces
# Written at 2014-04-23 10:30:34 UTC by InterfacesFileWriter
auto lo eth0 eth1
iface lo inet loopback

iface eth0 inet static
    address 10.40.0.2
    netmask 255.255.255.0
    dns-nameservers 8.8.8.8 8.8.4.4

iface eth1 inet static
    address 198.51.100.130
    netmask 255.255.255.128
    gateway 198.51.100.129
    dns-nameservers 8.8.8.8 8.8.4.4

post-up route add -net 10.0.50.0 netmask 255.255.255.0 gw 10.40.0.1
```

After the configuration has been changed and saved, the following command will make the changes take effect:

```
sudo service networking restart
```

Alternatively, you can reboot the Reverse Proxy and TURN Server appliance with the command `sudo reboot`.

### TURN server

If the reverse proxy and TURN applications co-exist on the same virtual machine, you must also edit the TURN server configuration file to specify the external IP address.

Run the following command to edit the TURN server configuration file:

```
sudo nano /etc/turnserver.conf
```

Change the line that begins `relay-ip=` to specify the external IP address, e.g. `relay-ip=198.51.100.130`

After editing the file, run the following command to make the configuration change take effect:

```
sudo service rfc5766-turn-server restart
```

Note that this will interrupt any existing TURN sessions (e.g. any WebRTC or Lync / Skype for Business calls going via the TURN server), therefore these changes should be performed during a maintenance window that is outside of normal operating hours.

## Changing the TURN server's access credentials

To set new access credentials for the TURN server, run the following command:

```
sudo turnadmin -k -a -b /etc/turnuserdb.conf -u <username> -r <realm> -p <password>
```

where `<username>` and `<password>` are the credentials to be applied, and `<realm>` is the domain of your deployment.

You can check the realm in use in your deployment by looking at your TURN server configuration file (by running `cat /etc/turnserver.conf`) and checking the `realm=` line.

If you change the credentials, remember to update the TURN server configuration on Pexip Infinity (**Call control > TURN servers**).

## Enabling LDAP/AD authentication on the reverse proxy

The reverse proxy supports remote LDAP/AD authentication, meaning that the Infinity Connect Mobile client will have to be configured with a username and password (in **Connection Settings**) to allow it to communicate with the reverse proxy.

If you intend to use this feature, please contact your authorized Pexip representative for assistance.