Pexip Reverse Proxy and TURN Server Deployment Guide

Introduction

In Pexip Infinity deployments, Pexip clients use HTTPS to communicate with Conferencing Nodes. The Pexip Mobile App for Apple iOS and Android devices uses HTTPS towards Conferencing Nodes to fetch conference information and to issue dial, mute and disconnect commands. The 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 web content in relation with branded Infinity Connect web portals.

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 use ICE (Interactive Connectivity Establishment) to negotiate optimal media paths with Conferencing Nodes. Microsoft Lync clients use a similar ICE mechanism, which means that Pexip can use TURN for both of these client types.

Note that Infinity Connect on Internet Explorer and Safari browsers uses the RTMP protocol, rather than WebRTC. RTMP clients cannot currently connect via the reverse proxy or TURN server and thus 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 server and enhancements to the delivery of the roster 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 Pexip Mobile App 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, and in some network topologies it will be ideal to deploy a single appliance and use it both for reverse proxy and TURN purposes, while in other scenarios it may be required to deploy two appliances, where one is used as a reverse proxy and the other is used for TURN – this is described in further detail in Design principles and guidelines .

About the Pexip Mobile App, Infinity Connect and reverse proxies

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: separate reverse proxy and TURN server instances
- Dual NIC, private and public addresses – see Appendix 2: Alternative dual NIC reverse proxy deployment

In deployments with more than one Conferencing Node, the reverse proxy can load-balance HTTPS traffic between all Conferencing Nodes in a deployment using a round-robin algorithm. A reverse proxy can also provide an authentication layer between the Pexip Mobile App / Infinity Connect 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. For more information, see the **Pexip Infinity Administrator Guide**.
- Appropriate DNS SRV records must have been created in accordance with Using the reverse proxy and TURN server with Infinity Connect.

Security considerations

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

When configured correctly, the reverse proxy will allow HTTPS traffic to flow between the Pexip Mobile App / 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.

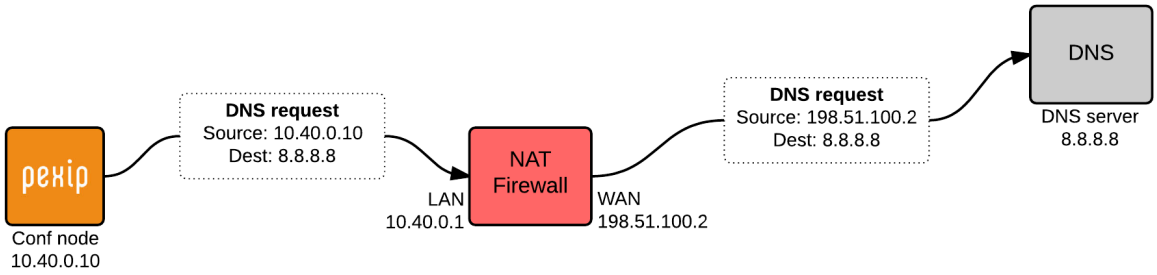
Design principles and guidelines

This section describes the network requirements for a reverse proxy and TURN server. Study this section carefully to determine whether the reverse proxy and TURN applications can be co-located on a single virtual machine in your deployment, or if these two roles should be split out as separate virtual machines.

The **reverse proxy application** is responsible for proxying HTTP requests (via HTTPS) from clients (Pexip Mobile App 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 (for example, WebRTC and Lync 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 call scenarios to work correctly (notably RDP content sharing with external Lync clients), it is essential that a Conferencing Node informs the remote Lync client of this reflexive address. The Lync client will in turn inform its Lync Edge of this reflexive address so that the Lync Edge server will relay media packets from the Conferencing Node to the Lync client.

This means that for a Pexip deployment where Lync will be used, it is essential that the TURN server must be deployed in such a way that traffic from the Conferencing Node towards the TURN server appears as coming from this reflexive address (198.51.100.2) when it arrives on the TURN server. This allows the Conferencing Node to discover its reflexive address from the TURN server through STUN. For comparison, if the TURN server sees this traffic as coming from 10.40.0.10 instead, the Conferencing Node will be unable to discover its reflexive address from the TURN server, and Lync RDP sharing will in those cases fail.

To summarize, for the reverse proxy and TURN applications to function properly, it is important that the following key requirements are satisfied:

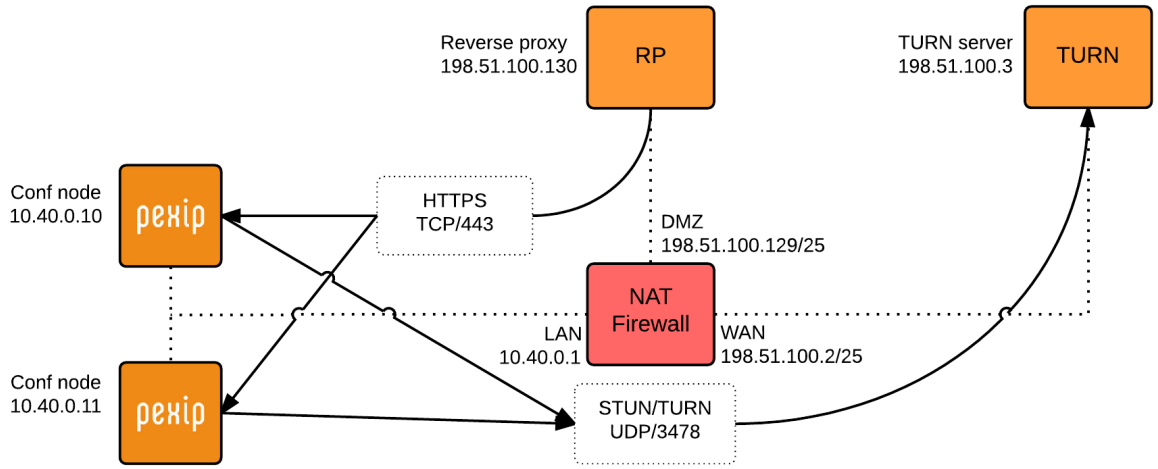
- For Lync RDP to work correctly, traffic from Conferencing Nodes towards the TURN server MUST arrive from the reflexive address of the Conferencing Nodes upon reaching the TURN server.

- For the reverse proxy to work correctly, the reverse proxy application must be able to communicate both with external clients and the internal Conferencing Nodes. This means that external clients are able to establish HTTPS connections towards the reverse proxy, and that the reverse proxy is able to establish HTTPS connections towards the Conferencing Nodes.
- The reverse proxy has to communicate with Conferencing Nodes either via a routed network or via NAT/port forwarding of HTTPS (TCP port 443).
- Where the reverse proxy reaches Conferencing Nodes via a routed (non-NATted) network, and where the TURN server and reverse proxy are co-located on the same virtual machine, the firewall/router located in between this virtual machine and the Conferencing Nodes has to be configured so that traffic from Conferencing Nodes towards the TURN server (traffic to UDP port 3478) is NATted to the reflexive address of the Conferencing Nodes, while HTTPS traffic between the reverse proxy and Conferencing Nodes is not NATted (also known as policy NAT).

As it may not be feasible to satisfy these requirements if the reverse proxy and TURN applications co-exist on the same virtual machine, it may be better to instead deploy these two application roles on separate virtual machines, so that firewall/routing/NAT rules can be setup appropriately for each application.

Example deployment: separate reverse proxy and TURN server instances

The following diagram depicts an example deployment where the reverse proxy application and the TURN server application have been deployed in different instances. This example forms the basis of this guide.



Example deployment used in this guide: separate reverse proxy and TURN instances

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

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

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: 198.51.100.2/25
- 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 has been deployed in the DMZ subnet with IP address 198.51.100.130.
- The TURN server has been deployed outside the WAN interface of the firewall with IP address 198.51.100.3.
- The firewall has been configured to allow the reverse proxy to initiate HTTPS connections towards the Conferencing Node IP addresses.
- The firewall has been configured to allow the Conferencing Nodes to send STUN/TURN to the TURN server on UDP port 3478.

Deploying the Reverse Proxy and TURN Server using an OVA template

Pexip provides a pre-configured 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

or

- Conferencing Nodes are deployed in internal, private networks
- the reverse proxy application is deployed in a DMZ environment using one or two network interfaces
- the TURN server application is deployed outside the WAN interface.

Deployment steps

Downloading the OVA template

Download the Pexip RP/TURN OVA template from https://file.ac/oGUCBqZC3Z4/ 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.

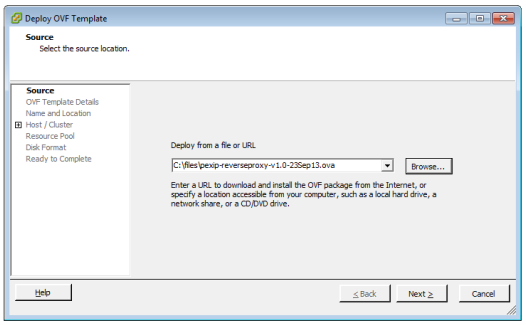
We recommend that you verify the OVA file integrity after downloading the OVA file by calculating the MD5 sum of the downloaded file (for instance using WinMD5 Free from www.winmd5.com) and comparing that with the respective MD5 sum found in file **md5sums.txt** (located in the same download location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

Deploying the OVA template

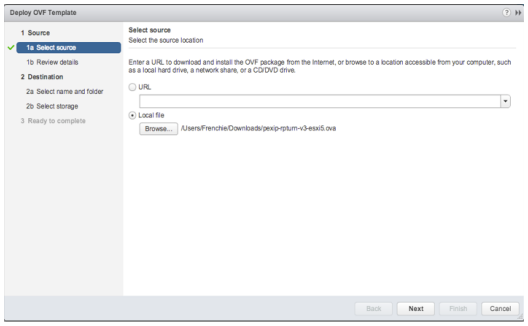
To deploy the OVA template:

- **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

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**.

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: separate reverse proxy and TURN server instances, with the following additional assumptions:

- The reverse proxy 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.

This example deployment uses two separate instances of the RP/TURN VM appliance, one instance for the Reverse Proxy application and another instance for the TURN application. Hence you will have to deploy the template and run the install wizard separately for each application. The install wizard steps explained below are primarily related to the deployment of the reverse proxy application, but they also contain specific guidance for the TURN application where required (steps 9 and 10 in particular).

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 will be 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 interface. If the intention is to have dual NICs, specify the address of the internally-facing NIC (see Appendix 3: Advanced configuration).
2	Subnet mask	255.255.255.0 [ENTER]	The reverse proxy has a network mask of 255.255.255.0.

Step	Prompt text	Example input	Explanation for this example deployment
3	Default Gateway	198.51.100.129 [ENTER]	The reverse proxy has a default gateway of 198.51.100.129.
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 **proxy**. The hostname and domain (configured in the next step) must match the actual DNS name by which the reverse proxy will be addressed (**proxy.example.com**).
6	Domain suffix	example.com [ENTER]	The reverse proxy has a domain name/suffix of **example.com**. This means, since the host name in the previous step was configured as **proxy**, that the full FQDN of this reverse proxy is **proxy.example.com**. 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 Replacing the default SSL certificate.
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 **8.8.8.8** and **8.8.4.4**. 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]	**Reverse proxy application** Here, the IP addresses of both Pexip Conferencing Nodes are input, one at a time – **10.40.0.10** is the first Conferencing Node and **10.40.0.11** is the second Conferencing Node. **TURN server application** 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]	disable [ENTER]	**Reverse proxy application** In this example reverse proxy deployment, we will deploy the TURN server as a separate VM instance, therefore you need to enter 'disable' here. **TURN server application** 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'.

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 — Pexip Mobile App 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 Reverse Proxy and TURN Server 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) 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
```

Enabling LDAP/AD authentication on the reverse proxy (for advanced users)

The reverse proxy supports remote LDAP/AD authentication, meaning that the Pexip Mobile App 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.

Using the reverse proxy and TURN server with Infinity Connect

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 users using Infinity Connect via a web browser.

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.

This section describes how to connect to the reverse proxy from Infinity Connect clients and the Pexip Mobile App, and how to configure the Pexip Infinity platform with details of the TURN server.

Note that the Pexip Mobile App does not use a TURN server to receive presentation content (it is delivered via the reverse proxy).

Using the reverse proxy and TURN server with Infinity Connect via a web browser

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 via a web browser 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 Pexip Mobile App

The Infinity Connect desktop client and Pexip Mobile App work by sending HTTP GET and POST requests to a specific destination address to fetch information about a meeting (such as the roster) 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 Pexip Mobile App) 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 record has been created:

```
_pexapp._tcp.example.com. 86400 IN SRV 1 100 443 proxy.example.com.
```

This points to the DNS A-record **proxy.example.com**, port 443 (HTTPS), with a priority of 1 and a weight of 100. In other words, it tells the Infinity Connect desktop client and Pexip Mobile App to send their HTTP requests to host **proxy.example.com** (our reverse proxy server) on TCP port 443.

If the client cannot locate the reverse proxy through DNS SRV discovery because either:

- the SRV lookup on **_pexapp._tcp.<domain>** does not return any records, or
- the client cannot contact the first host on the list that is returned in the SRV lookup,

it will fall back to performing a DNS A-record lookup for the domain in question. If successful, it will attempt to connect to port 443 on the IP address returned from this A-record lookup.

The DNS SRV lookup does not apply to participants using Infinity Connect via a web browser, because they connect to Conferencing Nodes or the reverse proxy directly, so no lookup is required.

This mechanism also uses RTP/RTCP for the media streams (via a TURN server if necessary).

Note that the Pexip Mobile App will keep polling the reverse proxy periodically to update the roster for a given virtual meeting room for as long as the application is active.

Configuring Pexip Infinity to use a TURN server

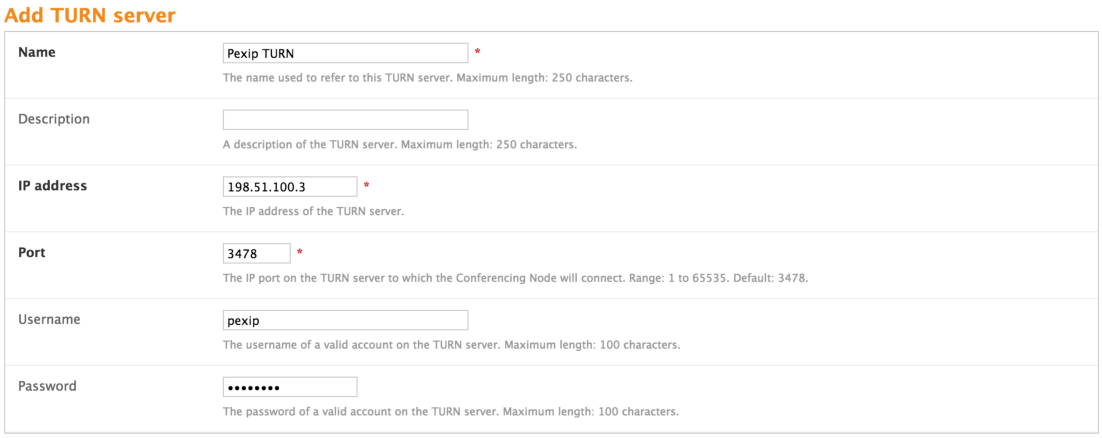
To relay media between the internal and external networks, a TURN server must be used. In addition to Pexip's TURN Server appliance, many other commercial TURN servers exist, including those on products such as a VCS Expressway, or those deployed using commercial or free software such as restund or rfc5766-turn-server.

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

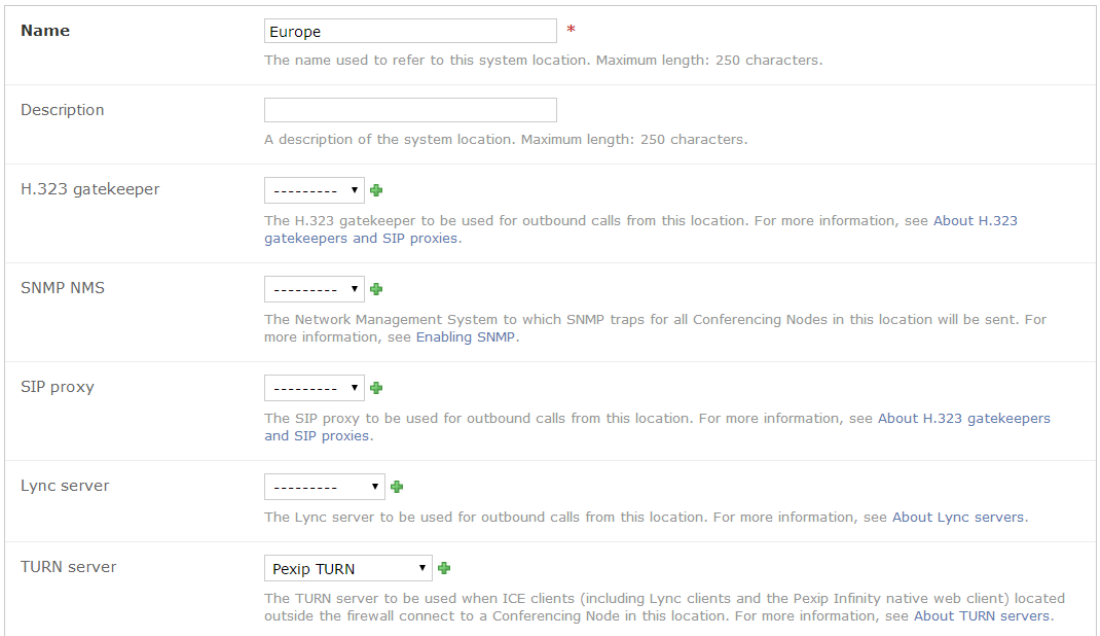
The TURN server's details must be configured on the Pexip Infinity platform, and each location must nominate the TURN server that will be used automatically to forward media when required.

To do this:

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



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



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 Pexip Mobile App 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:

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 Pexip Mobile App and Infinity Connect clients in the public 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
SSH	Outbound	Management PC	TCP	22	Reverse proxy and TURN server

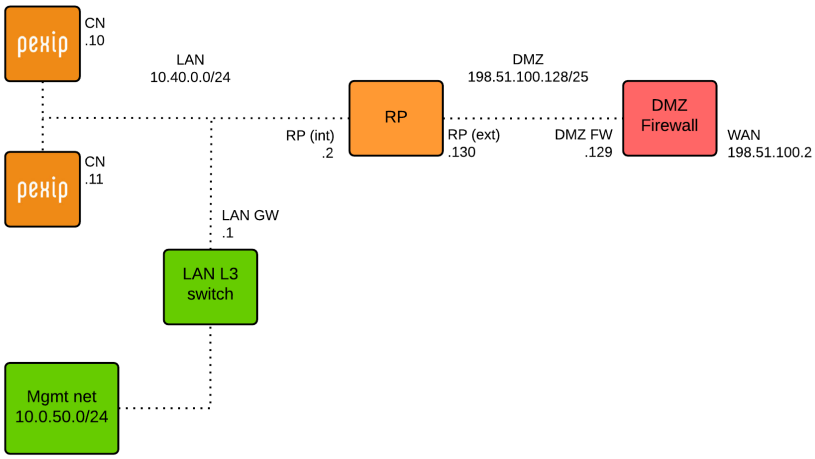
Appendix 2: Alternative dual NIC reverse proxy deployment

This section shows an alternative network configuration for the reverse proxy.

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 internal interface, while the DMZ perimeter network contains the reverse proxy external interface. The TURN server is not shown in this example and is deployed as a separate VM instance outside of the DMZ firewall.

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



The reverse proxy 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 is configured on the same subnet as the Conferencing Nodes, while the external interface of the reverse proxy 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 will originate.

There is no NAT between the outside and the DMZ network segment. The reverse proxy 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 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 (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 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 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 Appendix 3: Advanced configuration.

   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 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 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 VM to apply the new network settings.

Appendix 3: Advanced configuration

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

Adding additional Conferencing Nodes to an existing reverse proxy configuration

To add an additional Conferencing Node, run the following command to edit the Reverse Proxy and TURN Server config file:

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

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.

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 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

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
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 calls going via the TURN server), therefore these changes should be performed during a maintenance window that is outside of normal operating hours.