

InterwiseConnect™

Working with Reverse Proxy

Version 7.x

Table of Contents

BACKGROUND.....	3
Single Sign On (SSO).....	3
Interwise Connect	3
INTERWISE CONNECT WORKING WITH REVERSE PROXY	4
Architecture	4
Interwise Web Applications	4
Interwise Communications Server Applications	4
Interwise Client Applications.....	4
Interwise Communication Scheme	6
Interwise Communication Workflow	7
Main User Scenarios in the Presence of a Reverse Proxy	8
User Access to the ICC	8
Redirecting user into online Event – authenticating and connecting to the ICS	8
Live Communications between External Clients and the ICS	9
HTTP Queries between the Interwise clients and the ICC.....	9
Scheduling an Event using Interwise Outlook AddIn	9
IMPLEMENTATION SCENARIOS	10
General	10
Internal Setup	10
Guidelines.....	10
Graphical Illustration.....	10
Public Setup – Option I.....	11
Guidelines.....	11
Graphical Illustration.....	11
Public Setup – Option II.....	12
Guidelines.....	12
Graphical Illustration.....	12

Background

Reverse Proxy (RP) is a web proxy. Similar to a standard web proxy, its main characteristics are caching and protection ('firewall') capabilities. Unlike a standard web proxy, the RP is installed to protect web servers and not web users.

Organizations typically use a RP to protect a realm of web servers by controlling the access to resources in the realm. Authenticated users are allowed to access specific protected web content: access by non-authorized users is rejected. There can be several different implementations and protocols in use for the authentication process (i.e. against Radius Server or Directory Server, using HTTPS or LDAP).

This document describes the required steps to set up an 'On Site' installation of Interwise Connect in an environment that uses RP.

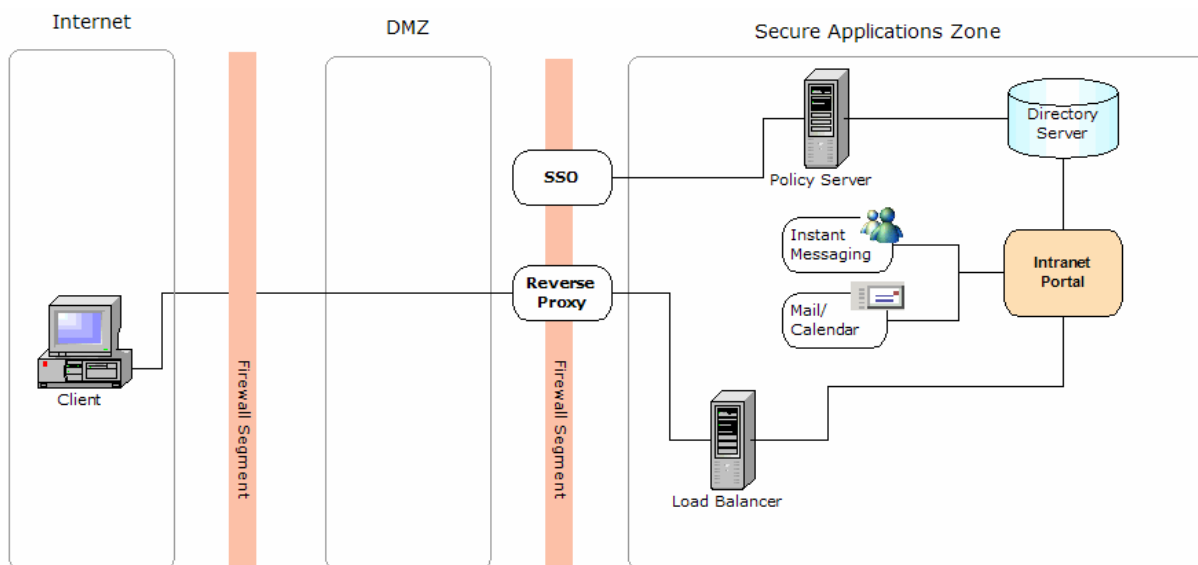


Figure 1: Typical Scenario

Single Sign On (SSO)

Single Sign On (SSO) eliminates the need to re-authenticate whenever accessing resources on the protected realm. An RP implementation that supports SSO allows end users to authenticate against the RP the first time only they access a web server in the protected realm. The RP passes the user identification to the protected web servers (typically in an HTTP header) allowing the different applications to avoid displaying their individual login screens.

Interwise Connect

This document assumes the reader has some prior knowledge of Interwise Connect. For additional information, see *Interwise Connect Technical Overview* or contact an Interwise technical expert.

Interwise Connect working with Reverse Proxy

Architecture

Interwise Web Applications

Interwise Connect is comprised of several sub components; three of these are installed on a web server (**which can share one machine**):

- **Communications Center (ICC):** Mandatory component for On Site installations.
- **Server Manager (ISM):** Mandatory component for On Site installations.
- **Phone Portal (IPP):** Optional component for On Site installations. The IPP is installed when the organization wants to enable the use of telephones in Interwise Events.

When working with RP, the above three applications are installed in the secured realm protected by the RP. Users accessing any of these applications should be able to cross the RP. The different users that need to have access to at least one of the three applications are listed in the following sections (client/server applications).

Interwise Communications Server Applications

Server applications are backend applications that run as daemons (there is no end-user interaction required to operate the applications and therefore no user can submit authentication details). Interwise communications servers manage the live streaming of Audio, Video and Data during live Events. Server applications can be cascaded to provide load balancing, efficient bandwidth utilization and for security considerations (for more details see the *Interwise Connect Technical Overview*).

Interwise Participant applications connect to the live communication servers to receive the live audio, video and data during the Events. One communications server may also connect to a parent communications server to receive the live stream of audio, video and data.

HTTP queries performed by the Interwise communications servers:

- Communications Server (Px/Push). The application sends HTTP queries to the ICC and ISM in order to pull Server and Event configuration information.
- Communications Server (IVR). The application is sending HTTP queries to the IPP.
- Communications Server (ITS). The application sends HTTP queries to the ISM in order to retrieve configuration information

Interwise Client Applications

Client applications are applications used by an end-user. The user selects to run these applications and can submit authentication details when required. The list below describes the scenarios where an Interwise client application sends HTTP queries that need to go via the RP.

- Web browser: The web browser is used to access the ICC, browse the ICC catalog, create Events through the web UI, and access live Events.

- Participant and Moderator applications: The Participant and Moderator applications are launched by the web browser when accessing a live Event. The application connects to the ICS for the live data stream (see below). These applications also use HTTP queries to retrieve information from the ICC (for example, the Event Info page that is displayed to every user that enters an Event).
- Outlook AddIn: The application uses internal API calls over HTTP for communicating with the ICC.
- Communications Gateway: An application available from the Interwise icon in the Windows system tray. The application allows the user to register to new ICCs and access registered ICCs. The installation of the Participant application can be configured not to place the icon in the system tray.

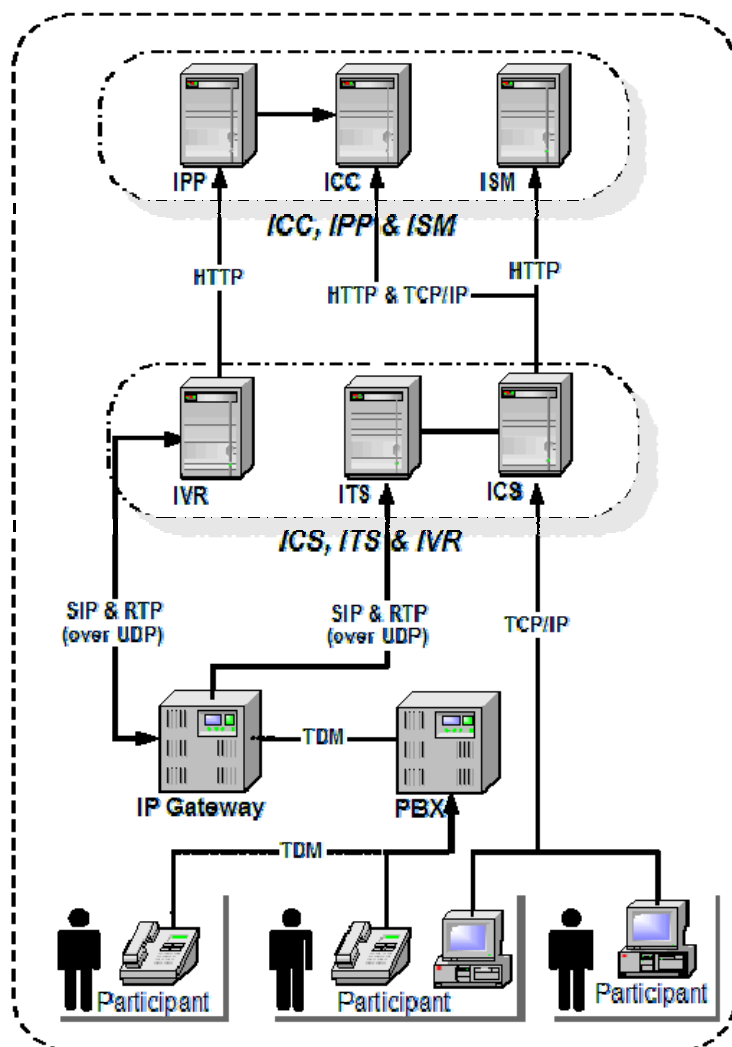


Figure 2: Typical Scenario

Interwise Communication Scheme

	Application	Component	Ports and protocols to be opened	Direction	From	Usage / purpose
1.	ICC (3 IP addresses)	IIS (IP #1)	HTTP: 80, HTTPS: 443	Inbound	Any	System Administration Users Login to live Event Queries from other system components API calls
2.		ISM (IP #1)	HTTP: 80	Inbound	ICC ICS(s) System Admin	System Administration Queries from other system components
3.		IPP (IP #1)	HTTP: 80	Inbound	ICS(s) System Admin	System Administration Queries from other system components
4.		Servers Remote Controller (RC) (IP#2)	TCP: 443 (SSL Tunnel)	Inbound	ICS(s)	Queries from other system components (ICS)
5.		Mux (IP#3)	TCP: 443 (SSL Tunnel)	Inbound	Any	Queries from other system components (ICS) Queries to retrieve on-demand content (users)
6.	ICS(s) (1-2 IPs)	Mux	TCP: 443 (SSL Tunnel)	Inbound and Outbound to parent ICS	Any	Live Event Connection Queries to retrieve on-demand content (Users)
7.		IWSes	SIP: 5060	Inbound from the IP Gateway		Users connecting with a telephone
8.		IWVoip	TCP: 443	Outbound to parent ICS		Live Event connection
9.		IWIVR	HTTP: 80	Outbound to the IPP		Live Event information

Interwise Communication Workflow

	Order	Action and workflow	From	To	Protocol and port
Event scheduling					
1.	A	User creates new Event on ICC	User IE browser	ICC	https: 443/ http: 80
	B	Email invitations are sent to invitees	ICC – SMTP Service	Users email clients	SMTP
2.	A	User creates new Event (Outlook AddIn)	Outlook AddIn on user desktop	ICC	http: 80
	B	Email invitations are sent to invitees	Outlook	Users email clients	Exchange mails
Event Entry (user side)					
3.	A	User logs in to Event	User IE browser or via email invitation link	ICC	https: 443
	B	User credentials sent to ICC	User IE browser	ICC	https: 443
	C	User authenticated	ICC	SQL DB	SQL Protocol: 1443
	D	User receives list of available servers and encrypted credentials for ICS login	ICC	User browser	https: 443
	E	Participant application is launched	User OS	Participant application	N/A
	F	Participant application selects best available server by running the ISS process (Intelligent Server Selection)	Participant application	ALL ICS servers for this Event	TCP: 443 (SSL Tunnel)
4.	A	Participant application connects to best available server – online communication starts (voice, data, video)	Participant application	Selected ICS	TCP: 443 (SSL Tunnel)
ICC and ICSs form the server tree for the Event (15 minutes before Event start time)					
5.	A	ICC to receive details of the Server Tree assignment to the specific Event	RC (Remote controller) on the ICC	ISM	http: 80
	B	RC notifies Main server to get ready for Event (and also sends it the list of registered Participants for this Event)	ICS – Main	RC (Remote controller) on the ICC machine	TCP: 443 (SSL Tunnel)

	Order	Action and workflow	From	To	Protocol and port
	C	RC notifies child servers to get ready for Event and notifies them of the main server details	ICS - Child	RC (Remote controller) on the ICC	TCP: 443 (SSL Tunnel)
	D	Child servers connect to main server to form the server tree	ICS - Child	ICS - Main	TCP: 443 (SSL Tunnel)
	E	Server tree is ready, Participants can start to connect to the Event			
Live Event communications					
6.	A	Participant communicates with selected ICS	Participant application	ICS	TCP: 443 (SSL Tunnel)
	B	Child ICS communicates with its parent server	ICS Child	ICS – upper level	TCP: 443 (SSL Tunnel)

Main User Scenarios in the Presence of a Reverse Proxy

User Access to the ICC

Upon access to any ICC page, the Reverse Proxy (RP) intercepts the user request. At this stage, the user is requested to submit their credentials to the RP. (The authentication request comes from the RP before the HTTP request arrived to the ICC. This process is completely external to Interwise Connect.)

After being successfully authenticated by the RP, the original HTTP request is forwarded to the ICC along with an additional HTTP header identifying the authenticated user. The ICC has a hook that can be configured to retrieve the user identification from this header and avoid displaying a second login page to these users.

The RP also returns a cookie to the user’s browser. The browser sends this cookie in subsequent requests to the same ICC, ensuring that the RP will not prompt the user to re-authenticate.

Redirecting user into online Event – authenticating and connecting to the ICS

There are numerous ways to enter a live Event, such as via an email link or by accessing the ICC from the browser. Regardless of the selected method, the user’s browser is used to access ICC pages that direct them into the Event. When accessing this ICC page, the user is authenticated by the RP, as described above.

Once the ICC authenticates the user, the Participant application begins the process of logging in into the live Event. This automatic process is initiated by sending the user (via the browser encrypted session) a small encrypted file, which includes the available servers for this specific Event (the servers forming the Event server tree) and his/her temporary credentials for the Event. When the user connects to the ICS, they pass these credentials and the ICS checks them against the temporary credentials list that was transferred to it from the ICC. If the user credentials match the credentials on the ICS, the user will be logged into the Event.

Note: The encrypted file activates the Participant application installed on the user desktop. The Participant application is then launched, interprets the file and uses it for the server selection process (selecting the best available server) and for sending the encrypted credentials that are stored in that file. **This guarantees that the user connects to the ICS only after successfully authenticating via the RP!**

Live Communications between External Clients and the ICS

Due to the real time nature of live audio, video and data communication, it cannot be transferred using the HTTP protocol. The solution is to use a real time protocol (Interwise proprietary) and to encrypt this protocol (if needed) with SSL. The SSL protocol is exactly the same protocol a browser would use when communicating with a secured web site.

Since the live communications protocol is not HTTP, the RP does not monitor the communication.

The solution is to place an additional ICS outside of the secured realm that will tunnel the live data between external users and the main ICS. A direct connection from this ICS machine to the ICS and ICC in the secured realm must be permitted (the port on which this connection occurs can be configured accordingly). In a configuration designed to support external users, this ICS would be placed in the DMZ. External users would connect only to this ICS in the DMZ. This ICS will accept their connection only after they have been authenticated by the RP and have the temporary credentials for the specific Event that they are attempting to connect to (as described above). Once connected, live audio, video and data to/from these Participants are transmitted via the ICS in the DMZ.

HTTP Queries between the Interwise clients and the ICC

In addition to live communications with the ICS, the Interwise clients perform some HTTP access to the ICC (e.g. to display the Dial-in Info page).

In order to avoid the need for the user to authenticate again to the RP when these queries are performed, the ICC can be configured to trap the session authentication token that is returned by the RP to the browser and pass it on to the Participant application. In this way, the Interwise client application, when acting as a web client, uses the token like the browser and maintains the SSO. The user experience therefore remains streamlined.

Scheduling an Event using Interwise Outlook AddIn

The Interwise Outlook AddIn enables users to schedule Interwise Events from Microsoft Outlook on their desktops. The AddIn uses internal API calls over HTTP to establish the functionality of creating a new Event, setting the Event attributes and registering users to the Event.

The Outlook AddIn can be configured to work in a RP environment. When configured as such, the AddIn takes the role of a web client and displays the user the authentication request (HTML) page that returns from the RP. After successfully authenticating to the RP, the AddIn continues using the same functionality of the browser by continuing to send the authentication token with every HTTP request.

Implementation Scenarios

General

The following scenarios describe implementation plans. The scenarios are referring to On Site installation, meaning that the entire Interwise Connect system is managed and maintained by the customer. All the applications are installed and supervised by the customer.

Internal Setup

All users will connect from within the network. Interwise Connect is not available for users connecting from outside the organizations.

Guidelines

1. The ICC, ISM and IPP are installed on the protected realm.
2. The ICSs are installed inside the organizational network (WAN).
3. The ICSs are granted with non-authorized access to the realm on the selected ports as defined above.

Graphical Illustration

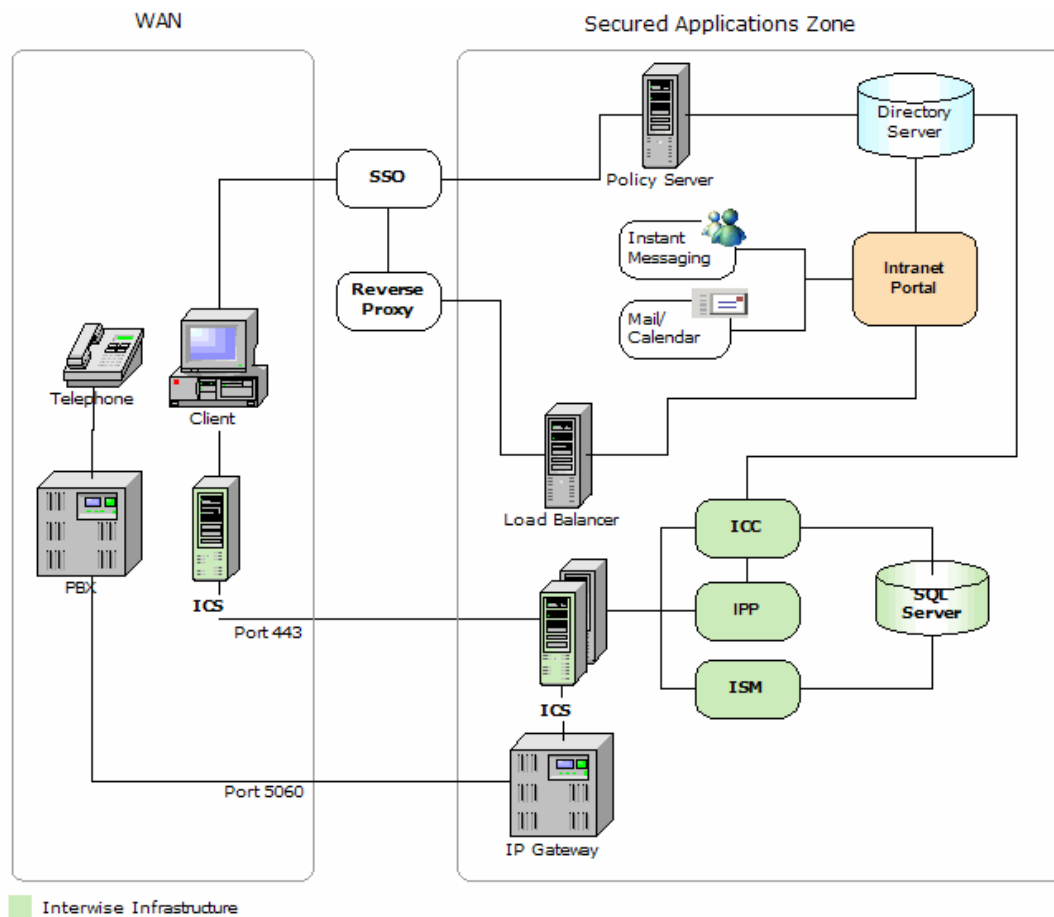


Figure 3: Private Setup

Public Setup – Option I

Interwise Connect is available both for users inside the network as well as users connecting from the Internet.

Guidelines

1. The ICC, ISM and IPP are installed on the protected realm.
2. One ICS machine is located in the DMZ. The machine has access to the Main ICS inside the network on a designated port that is pre-configured in the firewall so that the ICS is allowed to contact the main ICS machine.
3. ICSs are installed on the organizational network.
4. The ICSs are granted with non-authorized access to the realm on the selected ports as defined above.
5. The telephony support is hosted by the organization.

Graphical Illustration

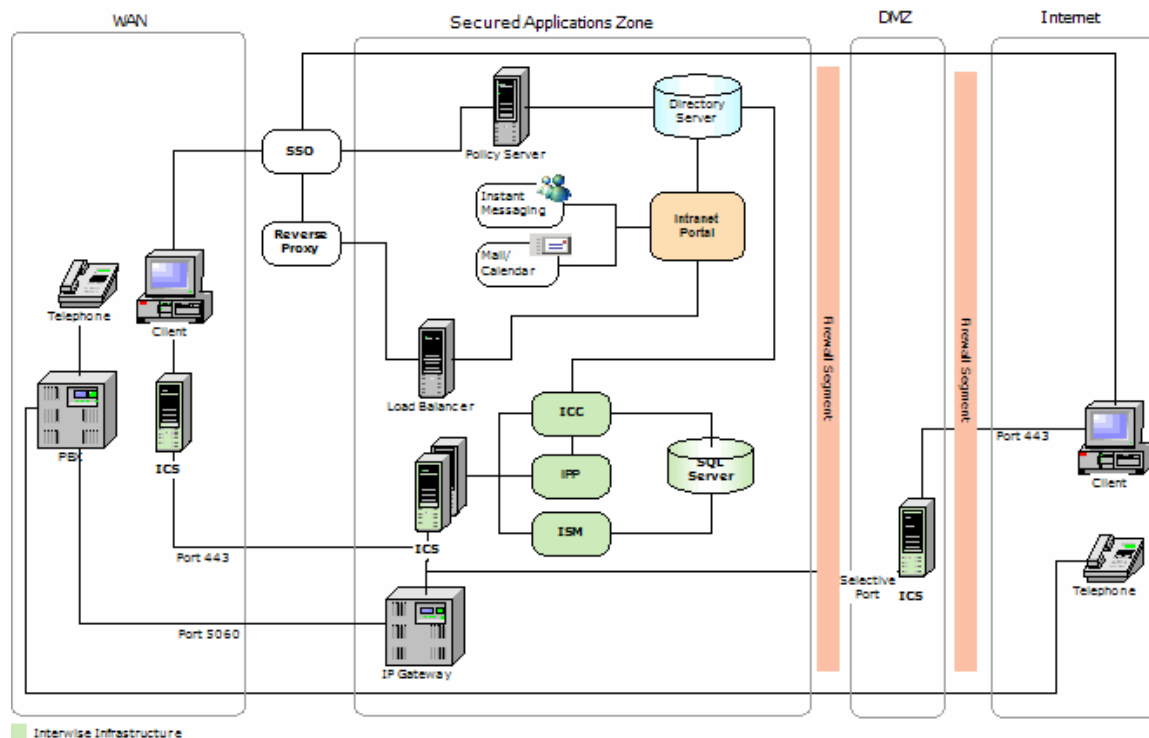


Figure 4: Public Setup – Option I

Public Setup – Option II

Interwise Connect is available both for users inside the network as well as users connecting from the Internet.

Guidelines

1. The ICC, ISM and IPP are installed on the protected realm.
2. One ICS machine is located in the DMZ. The machine has access to the Main ICS inside the network on a designated port that is pre-configured in the firewall so that the ICS is allowed to contact the main ICS machine.
3. ICSs are installed on the organizational network.
4. The ICSs are granted with non-authorized access to the realm on the selected ports as defined above.
5. The telephony support is hosted by Interwise

Graphical Illustration

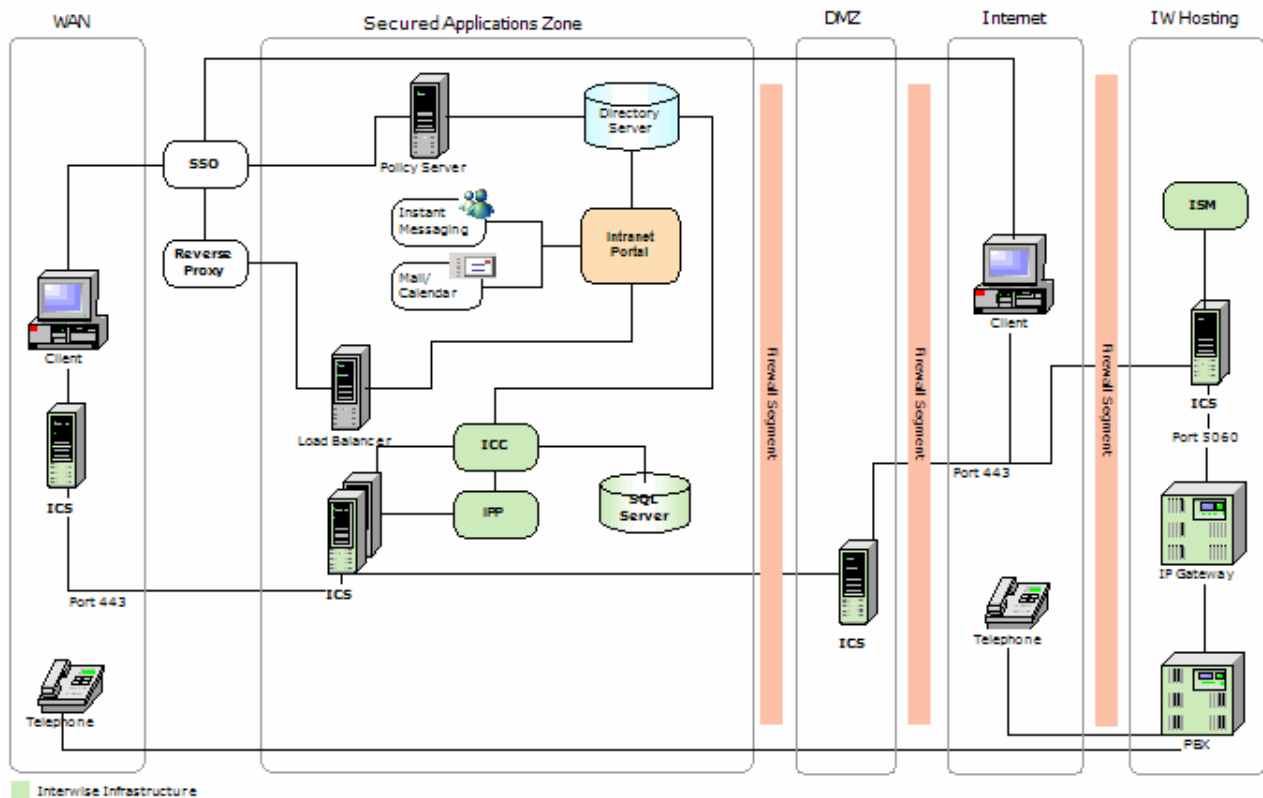


Figure 5: Public Setup – Option II