

Pass-through Proxy overview

The pass-through proxy feature enables you to specify Web applications for which the IVE performs minimal intermediation. Unlike traditional reverse proxy functionality, which also rewrites only selective parts of a server response but requires network changes as well as complex configuration, this feature only requires that you specify application servers and the way in which the IVE receives client requests to those application servers:

- **Via an IVE port**

When specifying an application for the pass-through proxy to intermediate, you specify a port on which the IVE listens for client requests to the application server. When the IVE receives a client request for the application server, it forwards the request to the specified application server port. When you choose this option, you must open traffic to the specified IVE port on your corporate firewall.

- **Via external DNS resolution**

When specifying an application for the pass-through proxy to intermediate, you specify an alias for the application server hostname. You need to add an entry for this alias in your external DNS that resolves to the IVE. When the IVE receives a client request for the alias, it forwards the request to the port you specify for the application server. This option is useful if your company has restrictive policies about opening firewall ports to access the IVE. When using this option, we recommend that each hostname alias contains the same domain substring as your IVE hostname and that you upload a wild card server certificate to the IVE in the format: *.domain.com.

For example, if your IVE is `iveserver.yourcompany.com`, then a hostname alias should be in the format `appserver.yourcompany.com` and the wild card certificate format would be `*.yourcompany.com`. If you do not use a wild card certificate, then a client's browser issues a certificate name check warning when a user browses to an application server, because the application server hostname alias does not match the certificate domain name. This behavior does not prevent a user from accessing the application server, however.

Examples

If your IVE is `iveserver.yourcompany.com` and you have an Oracle server at `oracle.companynetwork.net:8000`, you could specify these application parameters when specifying an IVE port:

Server: `oracle.companynetwork.net`

Port: `8000`

IVE port: `11000`

When the IVE receives Oracle client traffic sent to `iveserver.yourcompany.com:11000`, it forwards the traffic to `oracle.companynetwork.net:8000`.

Or, if you want to specify a hostname alias, you could configure the application with these parameters:

Server: oracle.companynetwork.net

Port: 8000

IVE alias: oracle.yourcompany.com

When the IVE receives Oracle client traffic sent to oracle.yourcompany.com, it forwards the traffic to oracle.companynetwork.net:8000.

When you choose to route client requests to the IVE based on a hostname alias, you must also add the IVE to your external DNS server. This option is useful if your company has restrictive policies about opening firewall ports to either internal servers or servers in the DMZ.

Just as with the core intermediation engine, the pass-through proxy option offers increased security relative to the Secure Application Manager, because when enabled for an application, the IVE allows the client to send only layer-7 traffic directed to fixed application ports to the enterprise network. Use this option to enable the IVE to support applications with components that are incompatible with the content intermediation engine, such as Java applets in Oracle e-business suite applications or applets that run in an unsupported Java Virtual Machine.

Note: The pass-through proxy option works only for applications that listen on fixed ports and where the client does not make direct socket connections. To specify applications for which the IVE performs minimal intermediation, see “Write a pass-through proxy resource policy” on the IVE Administration Guide.

Rewriting > Pass-through Proxy tab

Use the **Rewriting > Pass-through Proxy** tab to write a Web resource policy that specifies Web applications for which the IVE performs minimal intermediation. To create a pass-through proxy resource policy, you need to specify two things:

- Which Web application to intermediate with the pass-through proxy
- How the IVE listens for client requests to the application server

Write a pass-through proxy resource policy

To write a pass-through proxy resource policy:

1. In the Web console, choose **Resource Policies > Web > Rewriting > Pass-through Proxy**.
2. On the **Pass-through Proxy Policies** page, click **New Policy**.
3. On the **New Policy** page, enter:
 - 1 A name to label this policy.

2 A description of the policy (optional).

4. In the **URL** field, specify the application server hostname and the port used to access the application internally. Note that you cannot enter a URL in this field.

5. Choose the way in which you want to enable the pass-through proxy feature:

- **Use virtual hostname**

If you choose this option, specify a hostname alias for the application server. When the IVE receives a client request for the application server hostname alias, it forwards the request to the specified application server port in the **URL** field.

Important: If you choose this option, you must also define the IVE name and hostname in the **Network Identity** section of the **System > Network > Internal Port** tab.

- **Use IVE port**

If you choose this option, specify a unique IVE port in the range 11000-11099. The IVE listens for client requests to the application server on the specified IVE port and forwards any requests to the application server port specified in the **URL** field.

6. In the **Action** section, specify the method for the IVE to use to intermediate traffic:

- **Rewrite XML**
- **Rewrite external links**

7. Click **Save Changes**.

8. On the **Pass-through Proxy Policies** page, order the policies according to how you want the IVE to evaluate them. Keep in mind that once the IVE matches the application requested by the user to an application specified in a policy's (or a detailed rule's) **Resource** list, it performs the specified action and stops processing policies.

9. If you select:

- **Use virtual hostname**, you must also:

1 Add an entry for each application server hostname alias in your external DNS that resolves to the IVE.

2 Upload a wildcard server certificate to the IVE (recommended).

- **Use IVE port**, open traffic to the IVE port you specified for the

application server in your corporate firewall.

Note: If your application listens on multiple ports, configure each application port as a separate pass-through proxy entry with a separate IVE port. If you intend to access the server using different hostnames or IP addresses, configure each of those options separately; in this case, you may use the same IVE port.

Write a Web resource policy

When you enable the Web access feature for a role, you need to create resource policies that specify which resources a user may access, whether or not the IVE needs to rewrite the content requested by the user, and caching, applet, and single sign-on requirements. For every Web request, the IVE first evaluates the rewriting policies you configure¹. If the user's request is to a resource specified as "don't rewrite" due to either a selective rewriting or pass-through proxy resource policy, then the IVE forwards the user's request to the appropriate backend resource. Otherwise, the IVE continues to evaluate those resource policies corresponding to the request, such as Java resource policies for a request to fetch a Java applet. After matching a user's request to a resource listed in a relevant policy, the IVE performs the action specified for the resource.

When writing a Web resource policy, you need to supply key information:

- **Resources:** A resource policy must specify one or more resources to which the policy applies. When writing a Web policy, you need to specify Web servers or specific URLs.
- **Roles:** A resource policy must specify the roles to which it applies. When a user makes a request, the IVE determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions:** Each type of resource policy performs a certain action, which is either to allow or deny a resource or to perform or not perform some function, such as rewrite content, re-sign an applet, or post Web data.