Pass Through Proxy
How-to Guide
Contents

Overview: 3
Why PTP? 3
  • Via an SA port 3
  • Via external DNS resolution 3
Examples of Using Passthrough Proxy 4
  Example configuration using virtual host name: 5
  Example configuration using SA port mode: 8
Configuring PTP using resource profile: 9
Troubleshooting PTP issues: 10

Note: This document applies to IVE OS 6.0 and above.
Overview:

The pass-through proxy feature enables you to specify Web applications for which the SA (Secure Access) 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 SA receives client requests to those application servers. Either of the following 2 options can be deployed:

Why PTP?

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 SA allows the client to send only layer-7 traffic directed to fixed application ports to the enterprise network. Use this option to enable the SA 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. Either of the following 2 options can be deployed to access a backend application via SA PTP method:

- **Via an SA port**
  
  When specifying an application for the pass-through proxy to intermediate, you specify a port on which the SA listens for client requests to the application server. When the SA receives a client request for the application server on this designated port, it forwards the request to the specified backend application server port. When you choose this option, you must open traffic to the specified SA port on your corporate firewall. SA uses TCP port 11000-11099 for PTP purposes.

- **Via external DNS resolution**
  
  When specifying an application for the pass-through proxy to intermediate, you can 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 SA IP address. When the SA receives a client request for the alias, it forwards the request to the port you specify for the backend application server.

  This option is useful if your company has restrictive policies about opening firewall ports to access the SA. When using this option, we recommend that each hostname alias contains the same domain substring as your SA hostname and that you upload a wild card server certificate to the SA in the format: *.domain.com.

  If obtaining a wildcard certificate is not possible then you can use SA’s virtual ports and avoid the certificate warning for ‘host name mismatch’.

---

**Note:** You will need a certificate that is exclusively issued to the DNS name (virtual hostname) that you plan to use for PTP.
For this you can following the procedure below:

1. Login to SA as admin. Goto network -> internal port -> Virtual ports.
2. Add a virtual port by giving a name and a valid IP address in the same subnet as the internal port address.
4. Assign the virtual port with a device certificate, one that is exclusively obtained for the PTP DNS name that you are using.

**Example**, if your SA is SAserver.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. However this behavior does not prevent a user from accessing the application server.

**Examples of Using Passthrough Proxy**

If your SA is SAserver.yourcompany.com and you have an Oracle server at oracle.companynetwork.net:8000, you could specify the following application parameters when specifying an SA port:

**Server:** oracle.companynetwork.net  
**Port:** 8000  
**IVE port:** 11000  

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

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

**Server:** oracle.companynetwork.net  
**Port:** 8000  
**IVE alias:** oracle.yourcompany.com  

When the SA 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 SA based on a hostname alias, you must also add the SA 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.

**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 create a passthrough proxy resource policy, you need to specify two things:

a. Which Web application to intermediate with the passthrough proxy

b. How the SA listens for client requests to the application server

**Example configuration using virtual host name:**

1. Administrator would like SA clients to access backend web server resource http://mail.internal.com through PTP host name mode (Via external DNS resolution).

2. Users login to SA using URL http://remote.mycompany.com

3. Create a bookmark under user role which users will click to access their web mails.

4. The bookmark should contain the backend application name.

5. In this example we will use the host name as http://mail.internal.com


7. Add web ACL on SA to allow mail.internal.com

8. Goto resource policies->web->web acl. Click on new policy.
9. Assign this to the role and action: allow access.
10. Goto resource policy->web->passthrough proxy. Click on new application.

11. Add a policy name, URL of the backend application and the virtual host name (mail.mycompany.com).

12. In the Action section, specify the method for the SA to use to intermediate traffic:
   
a. Rewrite XML—If you select this option, the SA rewrites URLs contained within XML content. If you disable this option, the SA passes the XML content “as is” to the server.

b. Rewrite external links—If you select this option, the SA rewrites all URLs. If you disable this option, the SA rewrites only those URLs that contain a hostname specified in the passthrough proxy policy.

c. Block cookies from being sent to the browser—If you select this option, the SA blocks cookies destined for the client’s browser. The SA stores the cookies locally and sends them to applications whenever they are requested.

d. Host-Header forwarding—If you select this option, the SA passes the hostname as part of the host header instead of the actual host identifier.

13. Save changes.

---

**Note:** Client should be able to resolve mail.mycompany.com address to SA's IP address.
Example configuration using SA port mode:

Use same options as above from 1) to 10)

11. Add a policy name, URL of the backend application and use SA port.

Use option 12) as above.

13. Save changes.

Note:

a. Open traffic to the SA port you specified (11000) for the application server in your corporate firewall.

b. If your application listens on multiple ports, configure each application port as a separate pass-through proxy entry with a separate SA 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 SA port.
Configuring PTP using resource profile:

2. Select Type as custom.
3. Give a name for the profile.
4. Configure the URL of the backend application.
5. Click on Show ALL autopolicy types>>

- **Autopolicy: Web Access Control**
  Use this autopolicy to control access to web servers and URLs.

- **Autopolicy: Single Sign-on**
  Use this autopolicy to automatically pass user credentials to the Web application.

- **Autopolicy: Caching**
  Use this autopolicy to control which Web content is cached on a user's machine.

- **Autopolicy: Java Access Control**
  Use this autopolicy to specify the servers and ports to which Java applets connect. You may signing certificates.

- **Autopolicy: Rewriting Options**
  Use this autopolicy to bypass rewriting content through the Content Intermediation Engine.

7. Select Rewriting options.

8. Select the radio button to Passthrough Proxy.

9. Use either virtual hostname mode or SA port mode as per requirement.

10. Select the rewrite options that you need as the case may be.

11. Save and continue.

12. Select the role to which this profile needs to be available.

13. Bookmark will be automatically created.

Troubleshooting PTP issues:

1. Use HTTP watch utility (www.httpwatch.com) when accessing a PTP resource.

2. In case virtual host name is used from client computer try to ping or nslookup for the virtual host name.

3. It should resolve to SA IP address.

4. In case SA port mode is used ensure that you are able to reach to SA using this port.

5. Capture Policy trace on SA for the user session that is facing problems.

6. Users access log can help if there is an acl issue with the resource that you are trying to access.

7. SA TCP dump will help to confirm if PTP traffic reached SA or not whether in virtual host name mode or SA port mode.
Common Issues:

1. **Unable to access the PTP resource from internet works, fine when accessed from local network.** Troubleshooting approach:
   
   a. If the PTP resource is configured to be accessed via PTP virtual port mode, ensure that ports are allowed on the internet gateway in your network.
   
   b. If the PTP resource is configured to be accessed via PTP host name mode, ensure that the host name resolves to either the SA's address or an internet gateway which then translates address and forwards the request to SA.
   
   c. If there are links within a PTP accessed resource page and if these links are on a different destination server then necessary steps need to be taken inorder to handle such links. You can configure a separate PTP policy for such links.