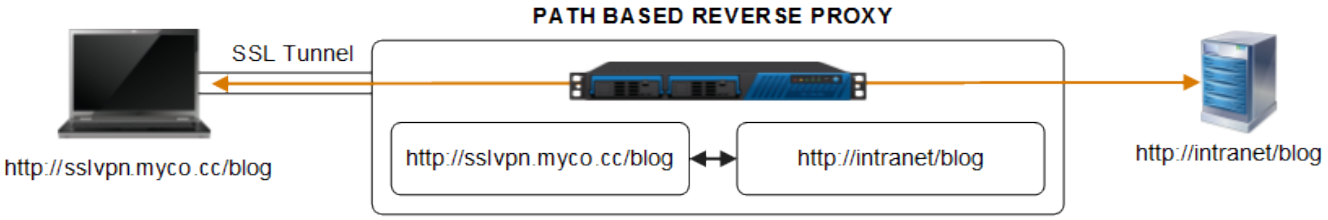
Custom Web Forwards

https://campus.barracuda.com/doc/39813748/

To create a Web Forward for a intranet site or web-based application, for which there is no predefined template, you have to create a Custom Web Forward. The Barracuda SSL VPN can differentiate between these types of Web Forwards:

Path-based reverse proxy



The Path-Based Reverse Proxy (most commonly used) acts as the front end to your web servers on the Internet or intranet. The Barracuda SSL VPN receives all the incoming web traffic from an external location and forwards it to the appropriate website host. For this proxy type to work, all possible destinations on the specified website or application for a particular Web Forward Resource must be within a directory on the web server - example: for Microsoft Outlook Web Access (OWA), */exchange* and */exchweb*.

This type of forward does not modify the data stream. The proxy works by matching unique paths in the request URI with the configured Web Forwards. For example, if you have a website that is accessible from the URL *http://intranet/blog* in your network you can configure the reverse proxy Web Forward with a path of */blog* so that all requests to the SSL VPN server URL *https://sslvpn.myco.cc/blog* are proxied to the destination site.

With a Path-Based Reverse Proxy, the Barracuda SSL VPN attempts to automatically detect all the paths that the target website uses, and add them to the Web Forward configuration when the Resource is launched. For example, when you create a Web Forward for *http://sslvpn.myco.cc/blog* and this blog page also contains images from a path called */images* from the root of the server, the Barracuda SSL VPN adds */blog* and */images* to the Web Forward configuration. This allows anything in the */blog* or */images* directory or subdirectories to work with this Web Forward. The following example shows the paths that the Barracuda SSL VPN added to the Web Forward *http://sslvpn.myco.cc/blog* which the user can access:

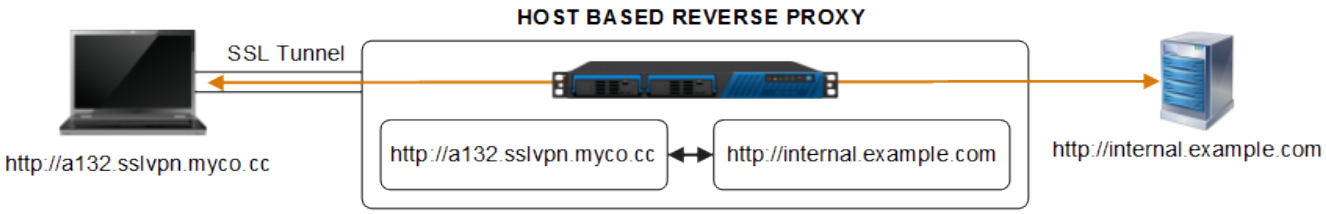
- *https://sslvpn.example.com/blog/images/picture.jpg* - The subdirectory of */images* below */blog* is added to this Web Forward.

- *https://sslvpn.example.com/blog/page2.htm - page.2.htm*, a child of */blog*, is added to this Web Forward.

When you try to access this Web Forward and the web content attempts to bring up an HTTP request that is not at one of those locations, such as: *http://sslvpn.example.local/news/index.html,* the Barracuda SSL VPN automatically adds the path specified by that request; in this case: */news.* Adding paths automatically does not work when they conflict with a path that the Barracuda SSL VPN uses to display HTTP content, such as */default /theme /js /fs.* If parts of the web page are missing, the Barracuda SSL VPN might not have detected some of the paths . To resolve this issue, edit the Web Forward, and manually add these extra paths.

To use the Path-Based Reverse Proxy, make sure that you set the **Always Launch Agent** option to *Yes*.

Host-based reverse proxy



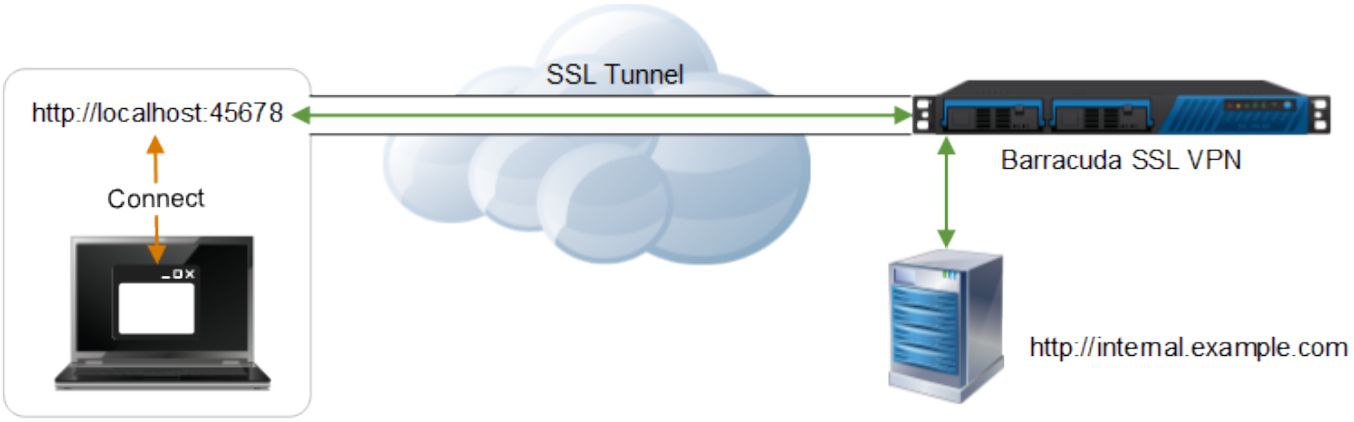
A host-based reverse proxy works in a similar way to a path-based reverse proxy, but is not restricted to subdirectories. However, the host must resolve properly via DNS. The proxy allows the web content to be located anywhere on the destination web server, including its root. This is useful for websites and applications that specify a host header or use relative paths in the content.

The Host-Based Reverse Proxy creates a unique hostname and appends it to the subdomain of the Barracuda SSL VPN.

For example: If the Barracuda SSL VPN hostname is *sslvpn.myco.cc,* the URL for the host-based reverse proxy Web Forward would be *https://<random string>*.sslvpn.myco.cc. Because a unique subdomain is created for each Web Forward configured as a Host-Based Reverse Proxy, you must configure a DNS entry on your DNS server for each subdomain that is used to resolve to the Barracuda SSL VPN. You can identify every generated hostname and create an explicit entry for it on your DNS server, or create a wildcard entry so that all lookups resolve to the same IP address as the Barracuda SSL VPN. As with the Path-Based Reverse Proxy, accessing links to a location that was not specified in the configuration fails unless you configure the destination hostname as an allowed host (with the *Allowed Host* option).

You must create configure your DNS server to resolve all generated subdomains to the IP address of the Barracuda SSL VPN.

Tunneled proxy



A tunneled proxy uses the Barracuda SSL VPN Agent on the client to open up a SSL tunnel to the Barracuda SSL VPN. The clients browser connects to a localhost address (e.g., `http://localhost:45678`). A direct connection to the resource located behind the SSL VPN is then established through the SSL tunnel. This type of Custom Web Forward does not modify the data stream, but will only work as long as all links stay on the same destination host. If the destination site uses multiple domains, or sub-domains, a host file or a proxy auto-configuration file (PAC) with routing information can tell the client which additional target sites have to be routed through the SSL tunnel. If needed, the PAC file is downloaded to the remote system when the session is initiated.

The tunnel proxy the following basic configurations, based on your web resource:

- **None** - (Recommended at first use) Creates a simple SSL tunnel. The browser connects to a local address (e.g., `http://127.0.0.1:45678`). The SSL VPN Agent forwards all traffic from the localhost address through the SSL tunnel, where the connection with the configured destination host is made. Use the None proxy type for simple, static websites, that are not virtually hosted and do not check the headers for the hostname.
- **Host File Redirect** - Adds temporary entries to the remote system's host file to enable direct routing to the destination site. Upon launch of a Web Forward of this type, the Barracuda SSL VPN automatically uploads the additional configuration information to the remote system. Because of this, the user must have write permissions to the system's *hosts* file. This proxy type is typically used with Microsoft Silverlight applications, because they do not operate in a reverse proxy environment. The Host File Redirect proxy type only works with Windows applications and does not support single sign-on.
- **Proxy** - For complex environments, you can use the Proxy type to create a SSL Tunnel to a proxy

server located in the destination network. This proxy type injects a proxy auto configuration (PAC) file into the browser with instructions about how to connect to different sites. These instructions redirect the target web requests through the tunnel. Use the Proxy proxy type when:

- Laptop users do not need to disable their proxy settings when they are outside their corporate network.
- Internal applications are hosted across WAN links. For example, if your users are in Austria but the Citrix server is hosted in the United States. You can use a PAC file to direct specific URLs to proxy servers that handles Citrix traffic exclusively. The rest of the traffic goes through your default Internet proxy in Austria.

With Tunneled proxy, all the links must be relative on the host that you have defined. For example: */folder/file.html* instead of *http://server/folder/file.html*

Replacement proxy

A replacement proxy is generally used if all the other Custom Web Forward types cannot be used. This proxy type attempts to find all links in the website code and replace them with links pointing back to the Barracuda SSL VPN. The content of the web page is modified as it passes through the SSL VPN, making it possible to create custom replacement values for different remote users.

If you have absolute URL addressing, use the Replacement Proxy when the other Custom Web Forward types do not work. The Replacement Proxy works most of the time, provided that the web page is not using a lot of JavaScript. However, using a Replacement Proxy is more resource intensive than the other proxies. Due to the number of ways it is possible to create links (in many different languages), this proxy type is not always successful. However, it is possible to create custom replacement values to get a website working through a replacement proxy Web Forward.

Direct URL

The Direct URL type is a direct link to an external website. Traffic does not pass through the Barracuda SSL VPN. This should be used for linking to external resources, like for example search engines, Wikipedia, etc...

Figures

1. PathBasedReverseProxy.png
2. ReverseProxy.png
3. TunneledProxy.png