

SSL VPN Web Forwards

<https://campus.barracuda.com/doc/50266299/>

Web forwards let the SSL VPN act as the front end to your web servers on the Internet or Intranet. The SSL VPN service on the X-Series Firewall receives the incoming web traffic through the SSL VPN web portal or CudaLaunch before forwarding it to the appropriate internal web-based service. The SSL VPN service handles authenticating users and secures all communication with SSL, allowing you to publish unsecured internal websites while still offering secure access to them.



Proxied web forwards using templates

Frequently used proxied web forwards, such as Outlook Web Access or SharePoint, are available as templates. Templates contain all the necessary configurations for the application and query the user for the required settings. By default, templates are configured to use the session username and password to log in.

For more information, see [How to Configure an Outlook Web Access Web Forward](#) and [How to Configure a SharePoint Web Forward](#).

Generic proxied web forwards

Generic proxied web forwards are used either when a manual rewrite configuration is required, or when a template does not exist for the service. A simple setup creates a reverse proxy for the service. The data stream is not modified. For advanced configurations, you can configure additional paths, custom replacements, and headers. For services requiring authentication, a single sign-on configuration is possible.

For more information, see [How to Configure a Generic Web Forward](#).

Tunneled web forwards

A tunneled web forward uses an SSL tunnel established by CudaLaunch to connect to a web server behind the firewall. The user's browser connects to a localhost address (e.g., <http://localhost:5678>). A direct connection to the resource located behind the SSL VPN is then established through the SSL tunnel. This type of web forward only works as long as all links stay on the same destination host; it does not modify the data stream. If the destination site uses multiple domains, or sub-domains, use a proxied generic Web forward instead.

For more information, see [How to Configure a Tunneled Web Forward](#).

Single sign-on for web forwards

Web services published through SSL VPN web forwards often require the user to sign in. You can use session or user attributes as placeholders to configure single sign-on. Session attributes contain the username and password used to log in to the SSL VPN service. If the credentials for the web forward differ, configure user attributes. When users access the web forward for the first time, they are prompted to fill in the username and password. Subsequent changes can be made in the SSL VPN web portal or via CudaLaunch.

For more information, see [How to Configure Single Sign-On for Web Forwards](#).

Figures

1. sslvpn_web_apps.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.