SSL VPN

https://campus.barracuda.com/doc/48660712/

The Barracuda NextGen X-Series SSL VPN is ideal for giving remote users secure access to their organization's network and files from virtually any device. With its web portal, the SSL VPN provides seamless service without the need to install and configure a full VPN client. The number of simultaneous users using the SSL VPN is limited only by the hardware limitations of the firewall.

Licensing

Most modern browsers have removed support for browser Java plugins. For SSL tunnels and applications, this functionality previously handled by browser-based applets is now covered by CudaLaunch. A Remote Access Premium subscription is required.

The following subscriptions are required to use SSL VPN in the X-Series Firewall:

- **Energize Updates** – Needed for the following SSL VPN features:
  - SSL VPN Web Portal
  - Web Forwards
  - User Attributes
  - VPN Group Policy (manual)
  - NAC
- **Remote Access Premium** – Needed for the following SSL VPN features:
  - CudaLaunch
  - Multiple client-to-site connections for the same user
  - VPN Group Policy (mananged)
  - Applications
  - SSL Tunnels

SSL VPN Web Portal

You can access the Barracuda SSL VPN web portal with any modern browser. Depending on the resource type you want to use, the client must meet the following requirements:

- **Web Forwards** – Any client operating system with a modern browser.
- **Applications / Tunnels** – Any client operating system with a Java Runtime environment installed in the browser.
- **WebDAV/SharePoint** – Any client operating system with a Java Runtime environment installed in the browser.

- **VPN Templates** – Windows or macOS with a Barracuda VPN client.
- **NextGen X-Series SSL VPN Client / Access Monitor** – Windows with a full Barracuda NAC VPN client and Java Runtime version 1.6 or higher.

For more information on authentication and basic setup, see How to Enable SSL VPN and CudaLaunch.

Web Forwards

Web forwards make internal web applications accessible through the SSL VPN web portal. This means that web servers do not have to be outside of your corporate firewall. Since all communication is secured with SSL, additional encryption or authentication routines are not required for the site. For web applications requiring the user to authenticate, you can configure the necessary single sign-on authentication information. Configuration templates for frequently used services such as Outlook Web Access or SharePoint are kept up-to-date through the Energize Updates subscription.

For more information, see:

- How to Configure a Generic Web Forward
- How to Configure Single Sign-On for Web Forwards
- How to Configure an Outlook Web Access Web Forward
- How to Configure a SharePoint Web Forward

Attributes

Attributes are placeholder variables used in web forwards. Session attributes are automatically filled in by the Barracuda NextGen Firewall X-Series. User attributes are created by the admin and filled in by the end users themselves in the web portal. Attributes are used to personalize web forwards or to configure single sign-on authentication. Session attributes are used if the user credentials are the same for the web forward and the SSL VPN. If the user credentials do not match, user attributes are used.

For more information, see How to Use and Create Attributes.

SSL Tunnels

SSL tunnels are used to tunnel TCP connections for client/server applications protected by your X-Series Firewall. The tunnel is created by CudaLaunch and terminated at the SSL VPN service. The user connects to a port on the 127.0.0.1 interface, instead of directly to the remote resource as in a VPN.

CudaLaunch accepts the local connection and forwards the traffic through the SSL tunnel. The SSL VPN service forwards the traffic to the destination IP address and port defined in the tunnel configuration. Traffic from the firewall to the destination IP address in the network does not have to be encrypted. Active tunnels are automatically terminated when the session is closed or timed out. SSL tunnels are available for CudaLaunch only.

For more information, see How to Configure SSL Tunnels.

Network Places

Network places provide remote users with a secure web interface to access corporate SMB network file shares. With appropriate permissions, users can browse network shares, rename, delete, retrieve, and upload files just as if they were connected in the office. Clients can connect to SMB1 and SMB2 shares, but must be able to negotiate a CIFS session. To use a network place resource, a Java browser plugin is required on the client.

For more information, see How to Configure Network Places

Applications

For resources requiring local applications on the client, you can configure application resources on the NextGen X-Series SSL VPN. Client application tunneling provides predefined and custom client/server protocols with an SSL-encrypted tunnel to the internal resource. Similar to web forwards, tunneling is employed when you need protocols on your desktop or mobile device to access your organization's network.

For more information, see How to Configure SSL VPN Applications for RDP.

CudaLaunch for mobile access

CudaLaunch provides mobile users secure remote access to your organization's applications and data. CudaLaunch is available for iOS and Android devices via the Apple App Store or Google Play Store. Desktop portal access is not supported for the Barracuda NextGen X-Series SSL VPN. To use CudaLaunch, you must have a remote access subscription. For testing purposes, one concurrent SSL VPN and CudaLaunch connection is included in the base license.

For more information, see CudaLaunch.

Full Device VPN for Android and iOS

Barracuda NextGen X-Series SSL VPN provides full device VPN for CudaLaunch clients. Create a client-to-site configuration and a VPN template resource in the SSL VPN in order to push the configuration to the mobile devices. By default, the first VPN template is used to connect to the VPN service. Due to differences in the mobile operating systems, the Android version of CudaLaunch uses the Barracuda VPN client, whereas CudaLaunch on iOS manages the built-in iOS IPsec client.

For more information, see How to Configure VPN Templates in the SSL VPN.