SSL VPN

The Barracuda NextGen F-Series SSL VPN is ideal for giving remote users secure access to their organization's network and files from virtually any device. With its mobile and desktop portals, the Barracuda SSL VPN provides seamless service without having to install and configure a fully blown VPN client. The number of simultaneous users using the SSL VPN is limited only by the hardware limitations of the NextGen Firewall F-Series. Remote Access Premium subscriptions are available for NextGen Firewall F80 and larger, as well as all NextGen Firewall F-Series Vx and public cloud models.

In this article

Video Demo

Desktop Portal

Mobile Portal

Web Forwards

Video Demo

Watch the video below to see a short demo of all the remote access features:

Desktop Portal

The Barracuda SSL VPN provides both mobile and desktop portals. You can access the desktop 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.
- **Dynamic Firewall Rules** – 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 F-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 Configure the SSL VPN Service.

Mobile Portal

To use the mobile portal, you must connect to the NextGen F-Series SSL VPN via the mobile browser on your smartphone or tablet. The NextGen F-Series SSL VPN automatically detects your device and redirects you to the mobile portal. The mobile portal can dynamically adapt its layout to account for various screens resolutions and for landscape or portrait orientation. The mobile portal is enabled by default. The following resource types are available:

- **Web Forwards** – For all supported mobile devices.
- **Dynamic Firewall Rules** – For all supported mobile devices.
- **VPN Templates** – Only for iOS devices.

For more information, see Mobile Portal.

Web Forwards

Web forwards make internal web applications accessible through the SSL VPN desktop or mobile 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

Dynamic Firewall Rules

Dynamic firewall rules allow administrators to temporarily enable access rules. This can be useful for direct access to servers during maintenance. In the desktop portal, you can enter the number of minutes the access rule should be active. The mobile portal has an additional option to enable or disable the dynamic rule without setting a time limit. When the time limit is reached, all existing sessions are terminated.

For more information, see How to Activate Dynamic Firewall Rules for Remote Connections via SSL VPN.

Attributes

Attributes are placeholder variables used in web forwards. Session attributes are automatically filled in by the Barracuda NextGen Firewall F-Series. User attributes are created by the admin and filled in by the end users themselves in the desktop or mobile 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.

VPN Templates

VPN Templates allow end users to self-provision the VPN clients on their Windows, macOS, or iOS devices. VPN Templates can currently be created for all group policy-based Client-to-Site VPN configurations. To automatically configure the VPN clients, end users simply log into the desktop or mobile portal and click the provisioning link. Administrators do not need to configure each desktop or mobile device individually.

For more information, see:

- How to Configure VPN Templates in the SSL VPN
- Self-Service VPN Provisioning on Microsoft Windows
- Self-Service VPN Provisioning on macOS
- Self-Service VPN Provisioning for iOS Devices

Applications / Tunnels

For resources requiring local applications on the client, you can configure Application resources on the NextGen F-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. Application tunnels are available for the following protocols:

- RDP
- VNC
- SSH
- Telnet

- SMTP
- POP3
- IMAP4
- SMB

For more information, see How to Configure an SSH Resource for SSL VPN or How to Configure a Remote Desktop Resource for SSL VPN.

WebDAV/SharePoint

WebDAV forwards are used to offer access to internal file servers. These resources can be mapped to network drives in Windows, or directly accessed through the Windows Explorer. SharePoint servers with WebDAV file shares enabled can also be configured to offer a SSL VPN WebDAV Forward.

For more information, see Example SSL VPN Resource Configurations.

NextGen F-Series SSL VPN Client / Access Monitor

The Barracuda NextGen F-Series SSL VPN Client (Transparent Agent) for Windows is a VPN client to establish transparent network access (Layer 3) to your company network. The client is fully integrated into the SSL VPN Portal and is executed by starting the **my Network** applet on the desktop portal. You can enable the automatic health check by enabling **Must be healthy** for a Resource. This will limit the resource to Windows clients.

For more information, see How to Install the Transparent VPN Client.

Microsoft Exchange Active Sync

If you are using Microsoft Exchange Server, your users can securely access their email, calendar, contacts and tasks from their mobile devices using Microsoft Exchange ActiveSync via the Barracuda NextGen Firewall F-Series HTTP Proxy service. ActiveSync allows mobile users to securely connect to an Exchange server. As an added layer of security, you can use the Barracuda SSL VPN to authenticate ActiveSync requests and proxy all the traffic. The advantage of this deployment is that the Barracuda NextGen Firewall F-Series handles the HTTPS traffic from the Internet.

For more information, see Example - Reverse Proxy for Exchange Services.