Forcepoint

VPN Client

2.5.0 or higher

for Linux

User Guide

Revision A

Contents

Introduction

This guide provides end-user instructions for installing and using Forcepoint VPN Client for Linux.

The Forcepoint VPN Client is a software application that runs on your Linux computer. The client allows you to securely connect to your organization's network remotely when Forcepoint Next Generation Firewall (Forcepoint NGFW) is used as a virtual private network (VPN) gateway. Forcepoint NGFW protects internal networks against attacks from the Internet by inspecting incoming connections and IP packets. Using a VPN establishes a secure, encrypted connection that protects the information you transfer.

Install or upgrade the Forcepoint VPN Client

You can add the Forcepoint VPN Client as a new installation or as an upgrade.

> ## Before you begin
>
> If you are upgrading, disconnect from all VPNs by stopping the VPN Client process.

Your administrator provides the installation package.

Steps

1) Depending on your Linux distribution, copy the rpm or deb package to your client computer.

2) (Upgrade only) Depending on your Linux distribution, enter one of the following commands to remove the previous version of the Forcepoint VPN Client.

   - Debian or Ubuntu

   ```
   sudo dpkg -r forcepoint-client
   ```

- CentOS

  ```
  sudo rpm -e forcepoint-client
  ```

3) (New installation on CentOS only) Enter the following command to install the dependencies for the VPN Client:

   ```
   sudo yum install libevent
   ```

   Note

   In CentOS, installation might fail if there are missing dependencies. The following error message is shown:

   ```
   sudo rpm -i forcepoint-client-<version>-<build>.rpm
   error: Failed dependencies:
   libevent-2.0.so.5()(64bit) is needed by forcepoint-client-<version>-<build>.rpm
   libevent_openssl-2.0.so.5()(64bit) is needed by forcepoint-client-<version>-<build>.rpm
   libevent_pthreads-2.0.so.5()(64bit) is needed by forcepoint-client-<version>-<build>.rpm
   ```

4) Depending on your Linux distribution, enter one of the following commands to install the Forcepoint VPN Client.

   - Debian or Ubuntu

     ```
     sudo dpkg -i forcepoint-client-<version>+<distribution>.deb
     sudo apt-get -f install
     ```

   - CentOS

     ```
     sudo rpm -i forcepoint-client-<version>.<distribution>.rpm
     ```

Connect to VPNs

When you must use a secure connection to access resources in your organization, connect to the VPN.

Forcepoint VPN Client is the SSL VPN client for Forcepoint NGFW firewalls. It connects to an NGFW endpoint, authenticates, and configures a TUN/TAP device for routing traffic from the client machine to the NGFW Engine. Root privileges are needed to add routing entries for the VPN tunnel and to add any DNS servers and search domains.

When the VPN Client connects to a new endpoint for the first time, the VPN Client shows the hash of the certificate of the endpoint and prompts you to verify the certificate.

After the first successful connection to the endpoint, a configuration file is saved on the client computer in the `~/.config/forcepoint/sslvpn/` directory.

Steps

1) Establish a VPN connection in one of the following ways:

   - To establish a VPN connection to a Forcepoint NGFW firewall for the first time, enter the following command:

     ```
     sudo forcepoint-client <host name> | <IP address of the endpoint>
     ```

The VPN Client prompts you to verify the certificate of the endpoint.

- To establish a VPN connection to a Forcepoint NGFW firewall to which the VPN Client has previously connected, enter the following command:

```
sudo forcepoint-client <path to configuration file>
```

> **Note**
>
> If you connect without using a configuration file, you must specify the fully qualified domain name (FQDN) or IP address of the endpoint.

For a complete list of all configuration options, enter the following command to show the forcepoint-client man page:

```
man 1 forcepoint-client
```

Result

You are connected to the VPN.

DNS resolvers for the VPN

The Forcepoint VPN Client can receive DNS configurations over the VPN using DHCP.

To configure DNS for an interface that is connected to an SSL VPN tunnel, the VPN Client must use a DNS resolver that the client operating system is configured to use.

You can use the `-R` option on the command line to force the VPN Client to use a specific DNS resolver. You can use the following DNS resolvers:

- resolvectl
- systemd-resolve
- resolvconf
- nmcli

If the VPN Client does not use a specific DNS resolver, the VPN Client proposes the most likely option for the DNS resolver.

If you use the `-R none` option on the command line, the VPN Client does not use any DNS server configurations sent by the gateway.

Disconnect from VPNs

If you no longer need a secure connection to your organization's network, disconnect from the VPN.

> **Note**
>
> A VPN connection is established as long as the forcepoint-client process is running.

Steps

1) Terminate the VPN connection in one of the following ways:
   - Press Ctrl-C in the terminal where the forcepoint-client process is running.
   - If you started the forcepoint-client process with the `–daemonize` or `-z` command line arguments, send a kill signal to the forcepoint-client process.

Uninstall the Forcepoint VPN Client

If you no longer need to connect to VPNs, uninstall the Forcepoint VPN Client.

Steps

1) Disconnect from all VPNs.

2) Depending on your Linux distribution, enter one of the following commands to remove the previous version of the Forcepoint VPN Client.
   - Debian or Ubuntu

     ```
     sudo dpkg -r forcepoint-client
     ```

   - CentOS

     ```
     sudo rpm -e forcepoint-client
     ```

Result

Forcepoint VPN Client is uninstalled.

Published 19 March 2021