ZYNSTRA TECHNICAL BRIEFING NOTE

End User VPN Installation

Introduction

Cloud Managed Servers can be accessed by end user clients through a VPN connection. This note explains how to install the End User VPN that is available with each Cloud Managed Server based on the OpenVPN software platform which is a widely-used, open source VPN client which is actively maintained and developed by its developer community. OpenVPN is available on a wide range of platforms including Windows 7 and 8, Linux, Apple iOS, MacOS and Android.

Installation Process

The Gateway Control Console is the tool that enables individual VPN profiles to be created for users requiring remote access. This tool provides the capability to download and distribute VPN settings and unique certificate for a user. When you create a new VPN user in the Gateway Control Console, the process of setting up a user with VPN access involves the following steps:

1) Download the installer for the relevant operating system (see the section at the end of this document for more information)
2) Install the client on the device that requires remote access
3) Go to the Gateway Control Console and create a new user
4) Export the user profile
5) Import the profile into the client.

It is possible to download either a Windows specific binary from the Gateway Control Console that includes Windows OpenVPN software as well as the user's unique configuration file and certificate or just the user's unique configuration file and certificate. The latter is OS independent. This allows the software itself to be downloaded and installed on client devices in advance or separately (or indeed, it may already be installed) and then the configuration file and certificate can be distributed to each user. This also allows the latest official version of the OpenVPN to be downloaded from official sources for each OS.

Security Best Practice

There are a number of best practice security measures that should be followed when using any VPN technology, including OpenVPN:

- Only users that require remote VPN access should have VPN profiles created.
- Access to the VPN should be granted by possessing a valid certificate which is unique to each user. These should be kept securely, and treated in the same way as passwords. If a certificate is believed to be compromised then it should be revoked and a new one issued.

For example, if a device with an End User VPN is stolen, then that certificate should be immediately revoked and a new one issued. Certificate revocation is a standard feature of the Gateway Control Console.

- Certificates should be unique to each user and should not be shared. The VPN Server will not allow two simultaneous connections with the same certificate.

If two users accidentally obtain the same certificate then, when the second user connects with the first connected, the first will be disconnected by the VPN server. When the first user re-connects, they will in turn disconnect the second user. This can cause frustration as users will incorrectly believe that either the VPN Client or the server is unreliable. If a user needs to connect from more than one client device concurrently, for example, via a laptop and a mobile phone, then multiple VPN profiles are required, one for each concurrent connection.

Technical Considerations

By default, the configuration of OpenVPN uses split tunnelling:

- Internet access for client devices will use their local network and not travel over the VPN connection.
- Access to local network resources (such as network printers) is permitted. The VPN server will allow connectivity and access to all resources in the remote network, both those on the Cloud Managed Server, as well as an organisation's LAN.

In a multi-site deployment of Cloud Managed Servers, all resources on all remote networks and servers are reachable.

The OpenVPN server is configured to supports client DNS override. For Operating Systems that support DNS override such as Windows, DNS resolution will automatically update so that both local and remote DNS records will resolve.

Whenever a new VPN profile is added, the OpenVPN service restarts. This only takes a few seconds, but all currently connected OpenVPN connections will be momentarily dropped.

If a Cloud Managed Server is configured with a public IP on its WAN interface, the OpenVPN Server will automatically listen on that IP for incoming connections. The client OpenVPN configuration file's internal IP address will point to the public IP address of the server.

In a 'double NAT' setup where there is a third party firewall between the Cloud Managed Server and the WAN, the Cloud Managed Server does not have a public IP. In this configuration it is necessary to update the client OpenVPN configuration file and enter the public IP of the upstream firewall. This is simply a case of changing the IP address in the OpenVPN configuration text file. The upstream firewall must be configured to port forward the IANA assigned OpenVPN port of UDP 1194 to the private WAN IP of the Cloud Managed Server.

Operational Considerations

OpenVPN modifies routes on the client OS when it connects. On Windows, it needs to be installed and run with an account that has local Administrator privileges. There are similar requirements for other Operating Systems.

Because adding or removing a user causes an OpenVPN service interruption, it is best practice to carry out user administration when there are no active VPN connections. It is advisable to bulk create VPN profiles for all users that need them, and/or pre-create profiles for new users in advance and assign them as needed. These should be retained securely until they are needed. Re-downloading certificates or configuration settings for existing profiles on OpenVPN does not cause service interruptions.

A restart of OpenVPN, whether adding or removing users, only affects client OpenVPN connections. No other aspects of the Cloud Managed Server are negatively impacted.

Latest Versions of OpenVPN

The OpenVPN site (openvpn.net) is the definitive site for OpenVPN information. The latest versions of the most common clients are available as follows:

Windows: openvpn.net/index.php/download/community-downloads.html

Apple iOS: itunes.apple.com/us/app/private-tunnel-vpn/id854725970

Mac OSX: code.google.com/p/tunnelblick

Android: play.google.com/store/apps/details?id=net.openvpn.privatetunnel.

Clients for other platforms (such as Linux, iOS, etc) are also available from the official package repositories and app stores for those platforms. Please contact the Customer Success Team if you need help with one of these versions.