BAILY'S

Technical VPN Guide
v0.1.1

Contents

Introduction 3
Why PfSense?

VPN Client Installation 4
Installing OpenVPN GUI.

VPN Configuration 5
Setup configuration files for Local and Remote.

VPN Quick Start 6
For those who already have OpenVPN GUI setup.

User Account Management 7
Making an account to access Baily's VPN connections.

NTP Time Server Issues 8
Ensuring that time synchronization does not interfere.

Introduction

As recently as August 2016 and January 2018, MICROS POS systems were hacked utilizing security flaws within the POS systems. It is important to realize that everything created by man, including software, contains flaws, and nothing is completely impervious to tampering. With these flaws, software can be manipulated to perform other actions outside of the original design of the programmer. Baily's has taken security seriously in order to prevent the exposure of sensitive customer data, by implementing PCI requirements, as well as sensible security practices. These changes will allow Baily's to become far more resilient against malicious attacks, keeping customers data secure.

In order to meet new PCI requirements, Baily's utilizes a homebrew PfSense router to host OpenVPN. It was required for the network to be segmented into three general departments: Public, Private, and Micros POS. The public network is hosted on the Aruba router in the North, under the Access Point name “Bailys Guest.” The private network is hosted by multiple devices, and are utilized by managers, and employees under the Access Points, FSBG, OTD, and OTD-EXT. Finally, the Micros POS network is hosted mainly by a switch in the closet, with the DHCP server hosted by the PfSense router. All networks utilize their own IP subnet, and are blocked from communicating with each other, unless explicit firewall rules are set in place. This is why, in order to communicate with another network, it is required to join that network through a specific VPN connection. With this setup, a manager connected to any network can access the Micros Server, run the Micros Applications (if installed), and access company hardware, such as printers, without compromising security by exposing these devices to the Guest network.

VPN Client Installation

Not anyone can simply connect to the VPN's hosted at Baily's, it requires a specific setup with managed account credentials. An individual with access to the PfSense router will need to perform this process. To gain this access, the OpenVPN GUI must be installed, along with a config generated from the PfSense router. PfSense luckily contains a Client Export Utility, which allows new clients to be setup with an installer. It is best to install the OpenVPN GUI from the installer provided by PfSense.

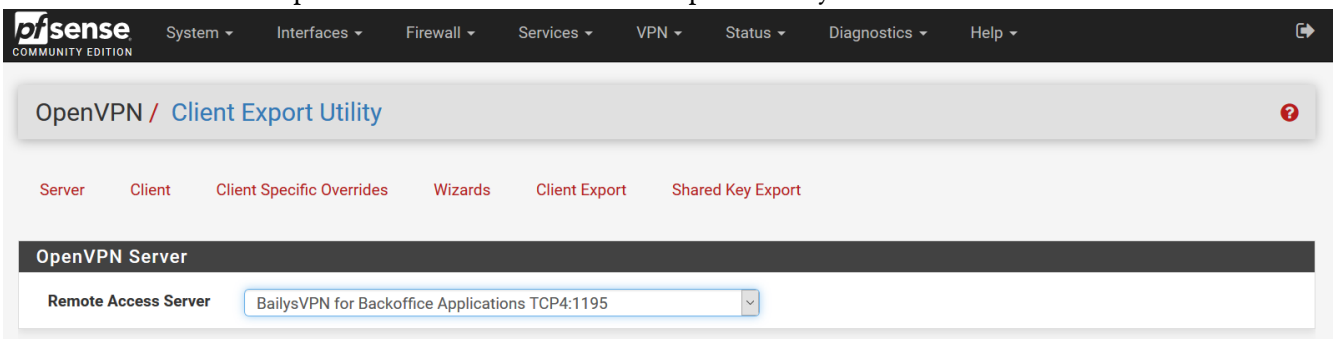


Illustration A: Make sure to select the proper Remote Access Server.

Scrolling down the page further, the Client Export options will become visible. This selection provides the ability to install the OpenVPN GUI with their respective config files for Android, Windows, Mac, and Linux. Currently, the installers are only for Windows, and Mac, although the config file can be used on any platform which supports an OpenVPN client.

VPN Configuration

By default the OpenVPN GUI installer provided by the PfSense router will only connect locally while still on one of Baily's network connections. In order to connect from the outside, it is necessary to create a second configuration which will point OpenVPN to Baily's external IP address. On all Windows systems except for XP, the OpenVPN configuration files are located in *C:\Program Files\OpenVPN\config.* Before an edit can be made to the configuration, the system must be using an account with administrator access, as Windows deems these files to be protected. In order to create a new configuration for remote access the existing configuration file must be copied within the same directory. It is important to rename the new configuration file in this structure:

router brand + port number + - + Local // Remote.

Renaming the new configuration file in this structure will help to determine what VPN connection is actually being utilized. OpenVPN will use the name of the configuration file, and display it in the list of connections. If the configuration files are not named in this format, it would be wise to rename them for consistency across all systems operated by Baily's managers and employees.

After renaming the file to the correct structure, the configuration file must be modified in order to properly make the connection. In order to modify the configuration, Notepad will have to be opened with Administrator access. To do this, Go to *Start,* type: "notepad," and before selecting, *right click,* and select *"run as administrator."* This will grant Notepad the required privileges in order to modify the configuration file. While Notepad is open, go to *File, Open,* and ensure in the lower right hand selection to specify *"All Files"* in the drop-down. Then browse to the location of the configuration files as stated earlier, and click *open* after selecting the new configuration file. In the open configuration, there will be a line which specifies the IP address which OpenVPN will attempt to make a connection to:

remote 192.168.2.53 1194 tcp-client

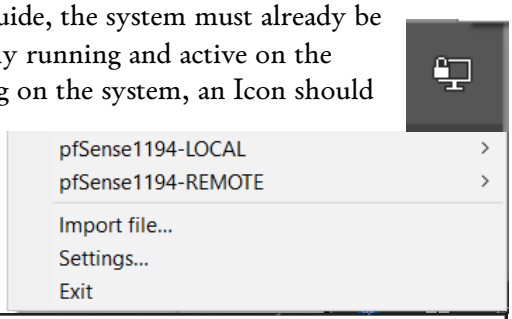
This line will need to be modified to point to Baily's external IP address which is currently, 71.177.27.202. Modify this line in the configuration file to show:

remote 71.177.27.202 1194 tcp-client

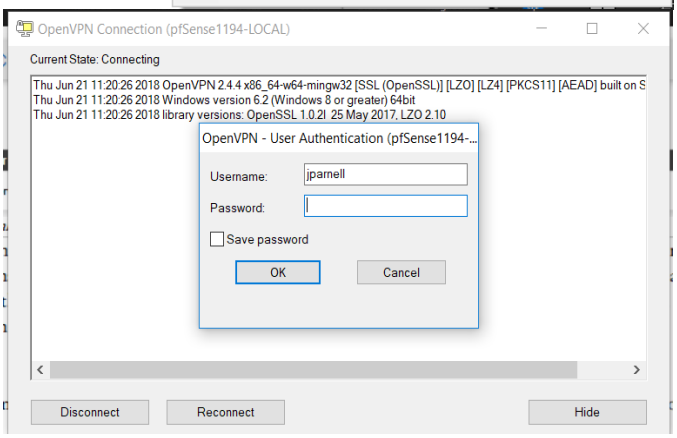
After this has been done, the *pfSense1194-Remote* connection (if using the same naming convention) should appear in the list of possible connections. If the configuration file was created properly, while utilizing this connection, all of Baily's resources will become accessible as if the system were sitting on site.

VPN Quick Start

If the system has already been setup by an IT member within Baily's, getting connected to the VPN should prove to be quite simple. Before moving forward with this guide, the system must already be connected to the internet, and the OpenVPN GUI must be currently running and active on the system. In order to ensure that OpenVPN GUI is currently running on the system, an Icon should be shown in the lower right hand corner of the screen, with an image which looks like a lock. If this icon is not showing, then the OpenVPN GUI needs to be started by locating it within the start menu.



In order to connect to Baily's VPN, it must first be determined whether you are working “Local,” or “Remote.” If the connection is to be made “Local,” it will only run if the user is located within the Baily's restaurant building, and connected to at least one of the many network connections offered. If the connection is to be made “Remote,” the system must be located outside of the Baily's restaurant, and connected to a network outside of the building. The two different connections are used based upon whether the system wishing to connect is inside, or outside of Baily's restaurant. After selecting which connection to use, a Username and Password prompt will appear before a successful connection can be made. If the setup was properly implemented, the user should have obtained the credentials already from an IT member. When those credentials are entered correctly, and the connection is successful, all OpenVPN GUI windows will close, and the lock icon will turn green. If there is an error, all OpenVPN GUI windows may still close, and yet there will be a yellow lock icon in the lower right hand corner of the desktop screen.



User Account Management

After installing the OpenVPN GUI provided by the PfSense router, attempting to connect to the VPN will produce a prompt for a user account. In order to connect, there must already be an account created by an administrator within PfSense. To create a user for the VPN, simply utilize the User Manager in System/User Manager. The user accounts to log into the VPN can also be modified in order to have specific privileges in order to operate, change, or manipulate the various different settings within PfSense. In the case of OpenVPN and it's connections, OpenVPN will operate with user accounts at the lowest privilege level, as it simply ensures that strangers will be unable to access Baily's network. It is important to have employee's set custom passwords to their accounts, as default or simple passwords can easily be hacked.

NTP Time Server Issues

In order to properly establish a secure connection with OpenVPN on the PfSense router, each machine must have their clocks properly synchronized. The generated certificates on each machine are time stamped before being sent, if the time isn't accurately set, this may cause either the client or the server to reject the connection entirely.

The PfSense router has been setup in order to provide an NTP time server service for use on machines who have difficulty connecting to a default time server. One example is the XP machine in Baily's office, this machine has been setup to link to the NTP server on PfSense through it's own Gateway (192.168.100.1). The NTP server on PfSense allows connections to it through any of the subnets that PfSense is supporting.

Currently, all security cameras, KIM-HP and the vintage XP Machine are the only ones syncing with PfSense's NTP time service. Further details about how PfSense provides it's service, refer to the PfSense user manual found online for free.

How It Works

Bailys systems may be difficult to understand at first, until the reason why it exists, and how it is setup is discovered first. The first aspect to understand is PCI compliance. Micros processes credit card information which must be as completely secure as possible, or credit card companies will charge higher fee's and may introduce a lawsuit if the system is hacked. In order to properly secure Micros, a firewall must be set in place in order to set the server within a secure environment where it cannot be accessed without authorization.

There are two important networks: The .2 network, and the .100 Micros network. The .2 network has a DHCP server hosted by the FiOS router directly, and provides a DMZ service to PfSense to port directly through it's firewall to the outside world. The .100 network is hosted by PfSense, and no devices inherently have access to the internet per PCI compliance standards. The .100 Network was originally intended to only be a connection for the Micros POS systems, although the same hardware has become the networking backbone, in order to prevent the laying of all new cabling throughout the entire building. Devices placed on the .100 network, which require internet access, are explicitly granted within the PfSense firewall rules.

It is important to realize that the PfSense router was not installed in order to completely replace the FiOS router. It was realized that in order for Fronteir to properly diagnose issues with the network from their end, the original FiOS router, and other equipment needed to be preserved without any serious modification. Thus, a DMZ was created for the PfSense router according to it's WAN IP, in order to allow pass-through access without any filtering to the outside world. This prevents the firewall in each router from conflicting with each other. Devices on the .2 network are protected by the FiOS router firewall, while all other networks are protected by the firewall in PfSense. Please refer to Bailys Network Map for a more broad understanding of how the network is structured.

Although the concept of isolating the Micros server in a subnet will maintain very high security, the server still needs some form of internet access in order to install updates, send a credit card batch, and generate reports for accounting. This is where it was decided to create a PfSense router/firewall in order to manage the network properly. With PfSense, BACKOFFICE-LOCAL was created in order to allow an accounting person to join the Micros .100 network, and generate reports, without compromising PCI compliance.

Bailys also requires a free WiFi connection, which needed to provide access to the internet to customers for free, without allowing access to any of Baily's hardware, such as Micros, POS systems, printers, and desktop workstations. PfSense allowed for the creation of a VLAN in order to produce a subnet only for the use of free public WiFi. With firewall rules, PfSense blocks any access to any of the other networks utilized by the management team, effectively isolating the guest network.

Not only are the VPN's utilized within the building to securely join alternate subnets, but it was required to allow remote access from the outside into the Micros network. For this, the BACKOFFICE-REMOTE connection was created. This connection will allow for a system to join the Micros .100 network, with a static IP if the device was configured to run the Micros Applications.

Most of the systems which management and accounting utilize reside on the .2 network off the FiOS router, outside of what is controlled by PfSense. All other devices except for what is directly accessible on the .2 network will function. In order to view the ZoneMinder Camera Server, or utilize any other functionality with Micros, the user must join BACKOFFICE-LOCAL.