Configuring WAN Connectivity for 802.1X Authentication Bridging and VLAN0 PCP Tagging

With some fiber-based Internet Service Providers, the ISP requires customers to use their modem in conjunction with an ONT (whether integrated into the modem or separate) to be granted access to their fiber network. However, it is often possible to bypass this equipment and connect a firewall directly. This guide walks through this process and primarily applies to the AT&T Residential Fiber Network in North America, but can be adapted to any ISP utilizing a similar configuration.

The purpose of this configuration is to provide authentication for access to the fiber network. Some ISPs offer a mode for their modems called “IP-Passthrough” which allows end users to have their public IPv4 and IPv6 addresses/blocks to be assigned directly to the equipment behind it. However, this comes with a few drawbacks:

1. Modem Memory Limitations - The fiber modem may still track states even when in IP-Passthrough mode. Some modems have a hard limit on the number of states that they can handle at a time, becoming unstable under significant load.
2. Limitations in IPv6 Implementation - When in IP-Passthrough, the modem is usually provisioned with a IPv6 subnet (/60 for ATT, for example), but will only hand out a single /64 out of this subnet via DHCP-PD to the firewall. This means that only a single LAN can be provisioned with IPv6 by default. It’s possible to request multiple /64 networks out of the IPv6 subnet block, but this is an ugly workaround.
3. Multiple Points of Failure - Having an ONT, a modem, and a firewall all needing to be powered at all times and available at all times introduces unnecessary additional points of hardware failure potential that can bring down connectivity even if the physical fiber link is in working order.

Bypassing the ISP equipment and attaching directly to the ONT with a pfSense Plus firewall eliminates or reduces the above limitations, allowing for greater control and flexibility.

Important Note: The best practice when bypassing the ISP modem that you have the WiFi Access Point disabled in the ISP equipment. This scenario requires an alternate means of WiFi and switch connectivity behind the firewall to ensure connectivity parity with the ISP-provided all-in-one solution for WiFi connectivity.

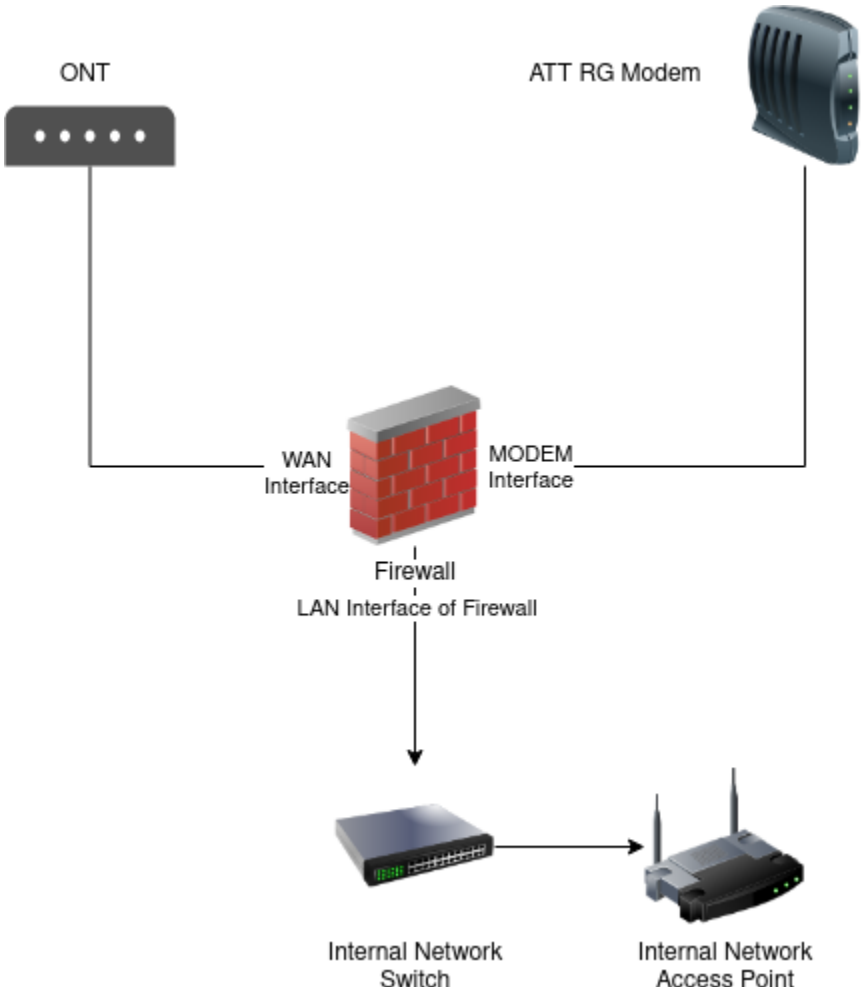
Overview of Network Requirements and Layout of Bypass

Authenticating the firewall and allowing it to connect to the provider, requires the following:

1. A firewall with at least 3 unique, discrete interfaces (one for the modem, one for the WAN connection, and one for the inside network or networks).

2. The modem needs to be able to authenticate access using 802.1X EAP-TLS authentication. Every ISP modem using 802.1X has a “burned in” certificate and will initiate authentication when it is attached to a physical network on the red “ONT” port. This is handled on boot-up of the modem normally when it is in-line between the ONT and the local equipment and it will periodically retry authentication.
3. All traffic after authentication must be 802.1Q tagged on VLAN0 with a Priority Code Point (PCP) of 1. Priority Code Point is a means of defining traffic priority. A PCP of 1 is “Best Effort” and is how most ISPs, including AT&T, expect traffic to be flagged. Setting a PCP under an interface in pfSense Plus will tag the traffic on VLAN0.
4. The WAN interface must have the MAC address spoofed to match the WAN interface on the fiber modem.
5. The interface attached to the modem must be in promiscuous mode.
6. The firewall must send all IPv6 DHCP requests with a defined and expected DUID. A DUID is a unique identifier that is used when requesting DHCPv6 leases. Normally pfSense will use a generated identifier, but if using AT&T they expect a DUID-EN (or DUID Enterprise Number) of 3561 and an identifier tied to the serial number of the modem. The Identifier for a modem can be generated using the open source script here. You can learn more about DUIDs here.
7. The firewall must send a prefix hint when requesting DHCPv6 Prefix Delegation. Typically this is a /60 for AT&T. A /60 subnet allows for 16 interfaces to each have their own /64 subnet.

Diagram of Wiring Layout



Modem Bypass Configuration Example

Create Interfaces

- Navigate to Interfaces → Assignments
- Select the physical interface attached to the Modem under “Available network ports:” and click “Add”
- Select the newly added OPT Interface
- Set the options as follows:
    - Enable: Check “Enable interface”
    - Description: MODEM
    - IPv4 Configuration Type: None
    - IPv6 Configuration Type: None
    - Promiscuous Mode: Check “Enable Promiscuous Mode”
    - Click Save and Apply Changes
- Navigate to Interfaces → WAN (or whatever interface name your ONT is attached to)
- Select the options as follows:
    - Enable: Check “Enable interface”, if not already
    - Description: WAN or another descriptive name
    - IPv4 Configuration Type: DHCP
    - IPv6 Configuration Type: DHCP6
    - MAC Address: The MAC address of the RG Modem
    - Priority Tag: 1
    - DHCPv6 Prefix Delegation size: 60 for AT&T or whatever is provisioned by the provider
    - Send IPv6 prefix hint: Checked
    - Do not wait for a RA: Checked
    - Click Save and Apply Changes
- Navigate to Interfaces → LAN (or whatever the inside interface is named)
- Select the options as follows:
    - Enable: Check “Enable interface”, if not already
    - Description: LAN or another descriptive name
    - IPv4 Configuration Type: Static IPv4
    - IPv6 Configuration Type: Track Interface
    - Track IPv6 Interface
        - IPv6 Interface: WAN (or whatever interface name your ONT is attached to)
        - IPv6 Prefix ID: 1
    - Save and Apply Changes
    - Repeat for any remaining inside interfaces, incrementing “IPv6 Prefix ID” by 1 for each network up to 15.

Configure IPv6 DUID

- Navigate to System → Advanced → Networking
- Set the option “DHCP6 DUID” to “DUID-EN: Assigned by Vendor based on Enterprise Number”

- Set the option DUID-EN to 3561
- Set the option “Identifier” to the DUID Identifier generated by the gen-duid.sh script linked earlier
- Click Save

Configure 802.1X Ethernet Rules for Authentication Passthrough

- Navigate to System → Advanced → Firewall & NAT →Advanced Options
- Ethernet Filtering: Check “Enable Ethernet Filtering”
- Click Save
- Navigate to Firewall → Rules → Ethernet
- Click Add
- Select the options as follows:
    - Action: Pass
    - Quick: Check “Apply the action immediately on match”
    - Interfaces → WAN (or whatever interface name the ONT is attached to)
    - Direction: in
    - Protocol: IEEE 802.1X
    - Source: any
    - Destination: any
    - Click “Show Advanced”
    - Bridge To: MODEM
    - Save and Apply Changes
- Click Add
- Select the options as follows:
    - Action: Pass
    - Quick: Check “Apply the action immediately on match”
    - Interfaces → MODEM
    - Direction: in
    - Protocol: any
    - Source: any
    - Destination: any
    - Click “Show Advanced”
    - Bridge To: WAN
    - Save and Apply Changes

The modem bypass configuration is now complete. Reboot your firewall. On boot, the modem should detect the link change and begin transmitting 802.1X authentication requests across the Layer 2 filter to the WAN interface and the WAN interface should be able to pull a DHCP and DHCPv6 lease.