Proposed Design Change to Product:
CPE based VPN

Jack Crowder, SE

Abstract:

A review of the current router [product] configurations for the NewEdge CPE based VPN product ("CPE-VPN") for the purpose of enhancing the security of this product offering.

Summary:

The virtues of the CPE-VPN, as a product offering, must be balanced against the needs of securing the Customers' internal systems and information segmented from the Internet connectivity. The NewEdge product, as currently configured on the Cisco hardware, leaves open the possibility of intrusion/spoofing by untrusted sources operating on the public Internet. The router technology configuration exists to enhance our product offering without adversely affecting the ROI for either the Customer or NewEdge Networks.

Before these suggested changes can be implemented, a series of tests – of the routing functionality – will need to be conducted by Engineering/TNT.

Audience:

This document is meant for Product Marketing. Additionally, this document can be used for further discussion/expansion by the Engineering, TNT, and Sales Engineering teams.

Section 1. Overview of the CPE based VPN product.

The original idea behind this product offering was for it to act as a "fill-in" for the MPLS-DSL (formerly "Net-VPN") product for those remote locations that could not be included in an MPLS-DSL network; either because DSL couldn't be offered at a particular location or "frame fill-in" was too expensive. Tunneling traffic across the public Internet opened the option of differing access methods (e.g. wireless and cable).

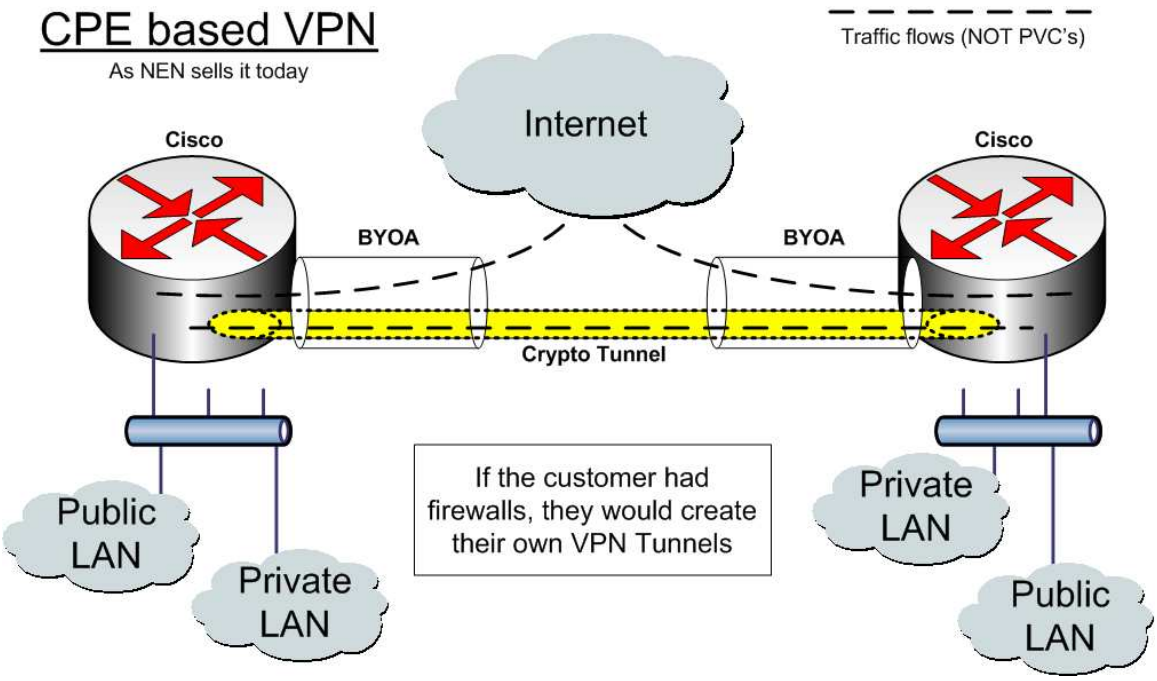
One of the gains possible with these differing access methods is the addition of last mile redundancy. Last mile redundancy means redundancy over a service that does not follow in the same cable run between the customer premise and the Central Office ("CO"). That means either cable and/or wireless (IR, EVDO, Cellular, microwave, and satellite) service. NewEdge doesn't provide any redundant network solutions – over cable and wireless connectivity – other than our CPE-VPN product.

There are several possible configurations of this CPE-VPN product. The configuration that is engineered for a potential customer depends upon what type of access exists at each location and whether "split-tunnels" (i.e. direct outbound access to both the Internet and the Private network) are required. For the purposes of this white paper, I will proceed with the configuration that

assumes the customer desires to have traffic route directly from a remote site to a destination in the public Internet (i.e. “spilt-tunnel”).

Section 2. What is the current configuration of the CPE-VPN?

Figure 1.



The benefits of the current configuration:

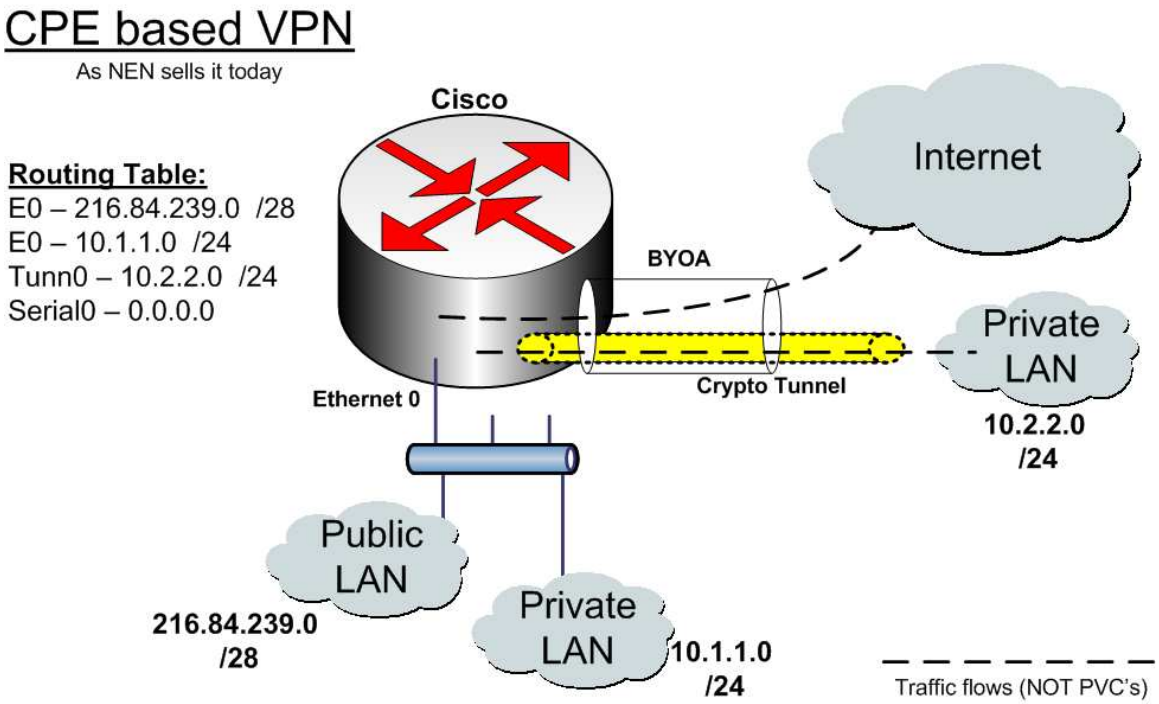
This configuration provides a great deal of flexibility to the customer. With a single circuit, a circuit that doesn’t have to support PVC’s, the End User (“EU”) can connect to both the Internet and their private network outbound from each location. Alternately, all traffic can be routed to the Host location for routing to the Public Internet from there.

This configuration assumes that the customer either does not have their own firewall or their firewall does not support encrypted tunnels (“VPN”).

The drawbacks to the current configuration:

The current configuration allows for the possibility of intrusion/spoofing into the customer’s private network. Consider **Figure 2**. A hacker who successfully spoofs a packet from the 10.2.2.0 subnet will have access to the 10.1.1.0 private LAN. If a hacker successfully spoofs a packet from the 10.1.1.0 subnet, they would be able to traverse the crypto tunnel to the remote 10.2.2.0 LAN. Either way, there is no separation between Public and Private traffic on any of the Cisco routers in the current configuration. The possibility exists for a hacker to analyze/view the Private traffic mixing on the Cisco router as well as spoofing the Private routes.

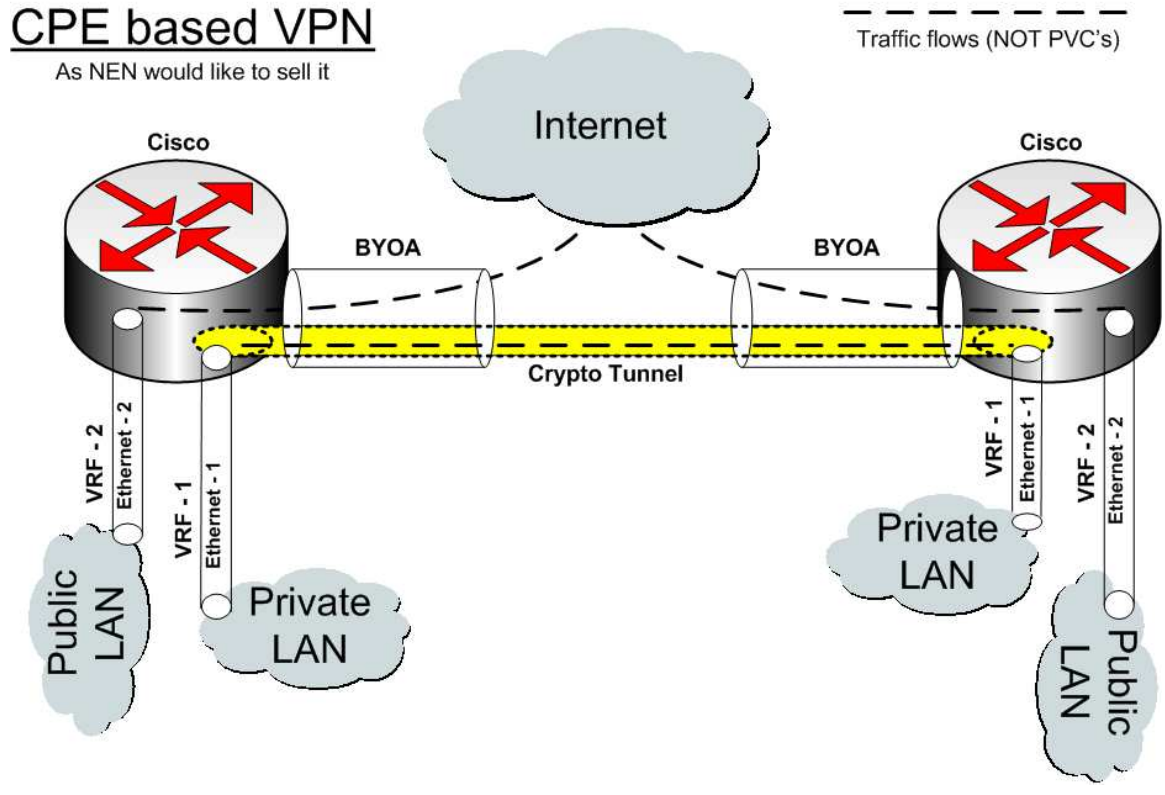
Figure 2.



Section 3. What is the product design recommendation?

It makes a certain sense to separate the Public and Private traffic using VRF. Consider **Figure 3**.

Figure 3.

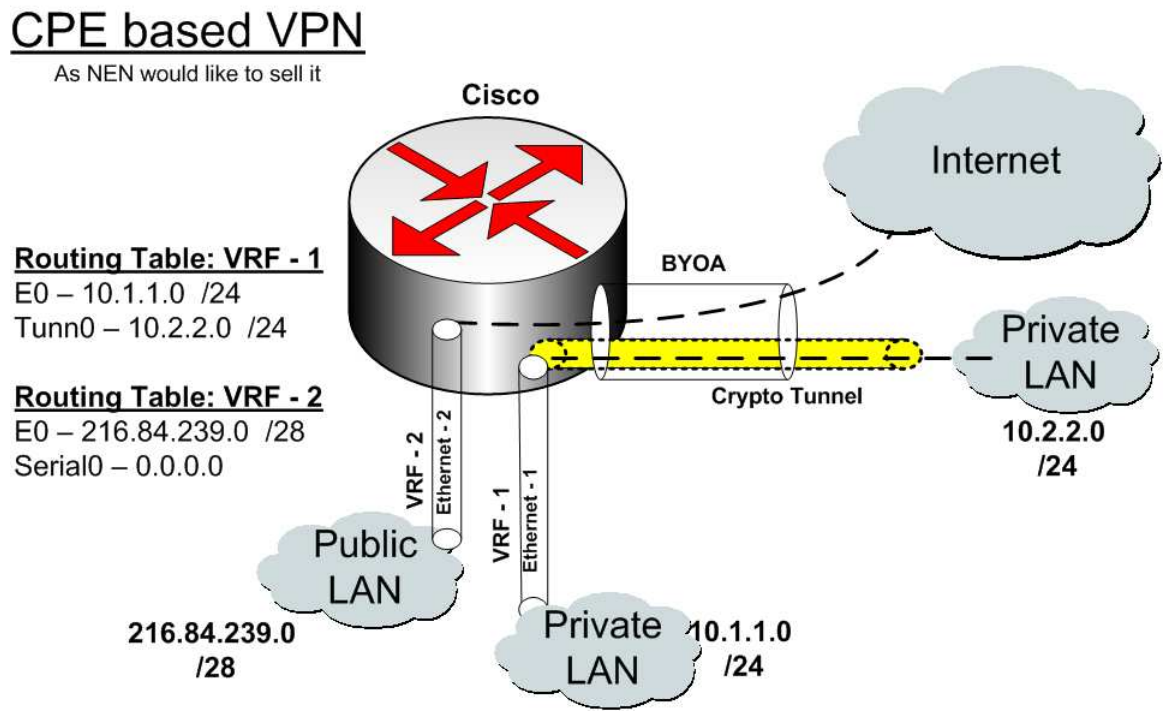


What are the advantages of the recommendation?

Increased security. Consider **Figure 4**. Any spoofing, from sources on the Internet, will only touch the routing table on the "VRF – 2" instance. Even a successful spoof would not reveal information concerning the Private network and/or routing table.

What are the disadvantages of the recommendation? In certain cases, when the customer brings their own Internet access (BYOA), they hand off that access to us with an Ethernet cable, NewEdge would need to provision a Cisco router with 3 Ethernet interfaces. This can be the 1841 with HWIC-4ESW or a 2811 with an NM-2FE or a 1721 with 2 WIC-1ENET. This will increase the cost model.

Figure 4.



Section 4. What are the next steps required to adopt this proposal?

This configuration will need to be tested, on the Cisco 2811, 1841, and 1721 routers, by Engineering and TNT.