Applicability Statement for Provider Provisioned CE-based Virtual Private Networks using IPsec

Abstract

This document is an applicability statement for Provider Provisioned CE-based IPsec VPNs, as described in [CEVPN]. This document describes how provider provisioned CE-based approaches meet the key requirements that are outlined in the PPVPN Applicability Statements Guideline document [ASGUIDE] and the key security requirements according to the template in section 8 of the VPN security framework document [SEC-FW].
1. Introduction
This document provides an Applicability Statement for the VPN solution described in [CEVPN]. We refer to these VPNs as "provider provisioned CE-based IPsec VPNs".

A VPN service is provided by a Service Provider to a Customer. Provider provisioned CE-based IPsec VPNs are intended for the situation in which (one or more of the following apply):

- a SP wants to offer VPN services to its customers without implementing VPN specific functions in its edge (PE) or backbone (P) routers;

- the customer does not trust the access network and the backbone networks that are used to interconnect the customer’s sites;

- CE-to-CE VPN data might need to be forwarded through the Internet or across multiple SPs;

- the customer does not want to configure and manage the VPN-specific functions of its edge equipment;

- the customer trusts its SP to properly and securely configure and manage its CE devices, and trusts the SP to take care of the security of its VPN and of the VPN’s key management; the customer is not concerned with hiding the data from the SP;

There are different business scenarios wherein PP CE-based IPsec VPNs can be offered to a customer.

The first case is where the different sites of a customer attach to the network of a particular SP, and where this SP is offering VPN services to its customers. In that case the SP is both the managed VPN provider and the network provider.

This case can be extended to a multi-SP scenario, where the SP, offering the VPN service and the network service, has trust agreements with other SPs to enable customer sites that are not attached to the former SP to belong to the same VPN. In this last scenario, the ‘other SP’ will make sure that the CE device that is attached to its backbone will be reachable by the original (primary) VPN Service Provider. This means that the VPN Service Provider will end up managing CE devices that are attached to its backbone, and CE devices that are not directly attached to its backbone.

The second case is where the different sites of a customer have access to the Internet via the (I)SP of their choice and where a (VPN) SP (‘the SP’) manages the customer’s CE devices for VPN purposes.
The basic scenario is the following. Every CE device has IP connectivity with the other CE devices that will belong to the same VPN (this can be via a "SP's backbone network" that is owned by one SP and that may internally use private addressing, via a set of cooperating SPs' PE-based VPNs or via the Internet). The SP's management system provisions the site's CE devices with the necessary topology and security information. The CE devices establish IPsec protected tunnels to the appropriate peering CE devices (according to the VPN's topology). The VPN sites start exchanging reachability information by tunneling routing protocol messages through the IPsec protected tunnels. Alternatively, the SP may provision static routes or tunnel traffic policy to the CEs, for example for small-sized, 'static' VPNs. Under the latter scenario, dynamic routing protocol tunneling is not required.

In provider provisioned CE-based IPsec VPNs, VPN tunnels are initiated and terminated at the CE devices, and it is assumed that the PE devices receive IP packets from the CE-PE links. This limits the supported tunneling techniques to IP-in-IP, L2TP, GRE and IPsec (tunnel mode). [CEVPN] uses IPsec (transport mode) protected IP-in-IP or GRE tunnels, or IPsec tunnel mode tunnels.

Note that the tunnel termination points are always the CE devices.

In CE-based VPNs, there are different aspects that need to be provisioned on the customers' CE devices: the VPN tunnels, the (IPsec) security policies and parameters, the intra- and inter-site routing aspects. Now, depending on what aspects are provisioned by the SP and what aspects are provisioned by the customer, different scenarios can be considered, and these scenarios may have a different applicability.

In this document, that considers VPNs in the provider-provisioned scope, we consider the following scenarios:

(a) the SP provisions the VPN tunnels and the security aspects. The intra-VPN routing aspects are under control of the VPN customer: the customer treats the provisioned tunnels as logical interfaces to CE devices at other VPN sites with a topology configured by the SP. It is clear that in this scenario, a very clear separation of management responsibilities between the customer and the service provider must be agreed upon (by specifying who gets to manage which specific parameters).

(b) the SP provisions the VPN tunnels, the security aspects and the routing aspects in the CE devices. This means that the SP has complete control of the CE device which has most likely been provided to the customer by that SP.
When dynamic routing is used, and the customers are responsible for the routing aspects on the CE devices (scenario (a)), the customers are free to choose the routing protocol(s) they want to use to distribute the reachability information (as long as these can be tunneled over IP or GRE, and as long as the peering CE devices support the subject routing protocols). Note that the CEs in different sites are direct routing peers. The Service Provider’s PE (and P) devices do not interact with the CE devices (or any other devices in the customer network) for the purpose of distributing the routes of the customer’s VPN.

In the case that the SP manages all aspects on the CE device (scenario (b)), the customers are limited in the choice of their IGP to the IGPs that the SP provides on the CE devices.

For provider provisioned CE-based IPsec VPNs, the topology of the VPN has an important impact on the scalability and the performance of the solution. All kinds of VPN topologies are supported by PP CE-based IPsec VPNs: hub and spoke topology, partial mesh topology, full mesh topology.

Note that the use of the IPsec protocol suite is not a requirement per se with regards to provider provisioned CE-based VPNs. A SP could offer a VPN service that uses non-encrypted or authenticated site-to-site tunnels (using e.g. IP-in-IP, GRE, L2TP). This use of non-secured CE-to-CE tunnels is not recommended for security reasons though, and is not discussed in [CEVPN].

2. SP Provisioning model

In provider provisioned CE-based VPNs, the SP is responsible for provisioning the CE devices with the VPN-specific configuration information.

The SP will install a secure management ‘channel’ towards every CE device, over which it can securely provision that CE device. This can for example be a specific IPsec tunnel, a secured Layer-4 channel, etc.

Note that [CEVPN] does not impose the use of a specific management protocol, as such allowing the described tunnel establishment, VPN routing distribution and data-plane security aspects to be de-coupled from the remote management and auto-discovery aspects. This allows different SPs to choose from their preferred remote management and auto-discovery solution, and for example to start with a manually (CLI-based) configured approach and finally migrate to a more scalable automatic approach. A complete ‘vertical’ solution would require the description of one (or some) remote management
architectures: set of protocols, security of the management channel, definition of the transported object models, protocol dynamics and interaction with for example the tunneling establishment to accomplish complete auto-discovery.

The SP will provision every CE device with the IP addresses of the peer CE devices the considered CE has to maintain a VPN tunnel with. The number of these peer CE devices depends on the number of sites the VPN contains and on the topology of the VPN.

In [CEVPN], the SP is responsible for provisioning the CE-devices with the necessary ‘security information’ that is needed to establish and maintain IPsec Security Associations with the peer CE devices: a set of transforms to use with IPsec, tunnel property information and IKE credentials. Indeed, the CE devices that will use IPsec to protect the inter-site traffic, need (long-term) secure credentials. These credentials will be used by a key exchange protocol (such as IKE(v2)) to generate the actual (short-term) keys that will be used to protect the data traffic.

One option for the (long-term) credentials is for the SP to directly configure them in the CE devices in the form of pre-shared keys (PSK). Alternatively, the SP can provide a public key infrastructure (PKI) to its VPN customers.

When this key distribution system provides the CE devices with pre-shared keys, then this key distribution can be done together with the configuration of the CE devices by the SP management system. If alternatively, the SP provides its VPNs with a Public Key Infrastructure, this adds extra complexity, but also supports the potential for multi-SP CE-based VPNs. Both the pre-shared key approach and the PKI approach have their scalability implications (see section 12.8).

For scalability purposes, the SP should use an ‘automatic update’ scheme such that the addition of a VPN site to an existing VPN requires the provisioning of only that new CE device (in contrast to the need to manually provision every existing CE device in the considered VPN). [CEVPN] does not describe such an ‘automatic update’ scheme, but the use of the mechanisms described in [CEVPN] is compatible with the use of any specific auto-discovery scheme. There currently is no IETF document describing a remote management protocol for CE-based IPsec VPNs, and describing a mechanism for CE-based IPsec VPN auto-discovery, but SPs commonly use remote management protocols such as for example CLI/Telnet/SSH or SOAP/XML/HTTP/SSH.

3. Supported Topologies and Traffic Types
Provider provisioned CE-based IPsec VPNs allow for all desired topologies: fully meshed VPNs, hub and spoke VPNs, partially meshed VPNs, etc. Configuring a specific required VPN topology is a matter for the SP of provisioning every member CE device with the IP addresses of the appropriate peer CE devices the considered CE device has to maintain a VPN tunnel with.

The customer VPN may carry both user data and control data. User data is the site-to-site traffic that carries user applications. The control data may contain site-to-site reachability information, keep-alives, etc.

Provider provisioned CE-based IPsec VPNs are not targeted at providing Layer-2 services. By (GRE- or IP-) encapsulating Layer-2 datagrams at the CE devices first, this traffic-type can be transported with CE-based IPsec VPNs.

Carrying multicast traffic with CE-based IPsec VPNs will require the (GRE- or IP-) encapsulation of multicast-packets at the CE devices first. Multicast support in CE-based VPNs means for a basic scenario that CE devices need to be provisioned as to be able to duplicate multicast packets over the different VPN tunnels it maintains (which makes CE-based VPNs less resource efficient for Multicast traffic than e.g. PE-based VPNs).

4. Isolated Exchange of Data and Routing Information

4.1 Isolated forwarding of VPN data

With CE-based IPsec VPNs, tunnels are deployed between CE devices. These tunnels are either IP-in-IP (or GRE) tunnels that are protected via IPsec in transport mode [TOUCH-VPN], or IPsec tunnel mode tunnels.

In both cases, the forwarding in the shared infrastructure (access network and SP network(s)) is based on the IP addresses in the packets’ outer IP header. These IP addresses can be public IP addresses (e.g. when the Internet is used for the CE-to-CE forwarding), or more generally IP addresses that belong the SP’s addressing realm (these might be private or non-unique addresses when the interconnectivity between CEs is offered by one particular SP).

Isolated exchange of data information is assured because IP routing and forwarding in the shared infrastructure takes care of forwarding the encapsulated IP packets to the correct destination CEs, using the destination address in the IPsec packets’ outer headers. Indeed, the IP addresses in the outer headers are always IP addresses that belong to the CE devices and that are unique and routable in the SP backbone.
network(s).

In addition, the customer IP packets are encrypted on every CE-to-CE part of the network; as such, no intermediate router or other device that does not belong to the same VPN can read the customer traffic, even if mis-routing or intercept occurs. This is particularly applicable in the case that the Internet is used for forwarding the CE-to-CE traffic, as the SP then doesn’t have control on the actual path of the customer traffic.

Encrypting the data packets also makes sure that packets that would arrive at a wrong destination CE, would not be visible by the receiving device: a CE device that receives a packet that it cannot decrypt using its existing Security Associations, will drop that packet. This makes sure that packets that don’t belong to the considered VPN cannot (un)intentionally enter that VPN.

4.2 Constrained Distribution of Reachability Information

The distribution of VPN IP reachability information among devices at the VPN sites is achieved by tunneling the reachability information (in the form of routing protocol messages) through the CE-to-CE VPN tunnels. CE devices must be configured to forward VPN reachability information only to those interfaces that are associated with the particular VPN: that is, the intra-site interfaces and the IPsec-protected interfaces (tunnels) that lead to the other sites that belong to the same VPN.

As a CE only maintains VPN tunnels with CE devices that belong to the same VPN, the reachability information of one VPN site will only be distributed to other sites that belong to the same VPN. This also ensures that VPN routes will not be distributed into the Internet, and that Internet routes will not be distributed to VPN sites.

One special case and exception to the above is when a CE device also provides Internet Access to the VPN. In this case, a firewall should take care of the Internet Gateway function.

Of course, configuration errors by the SP can compromise the constrained distribution of reachability, and the overall security of the VPN (as discussed in section 5.2).

4.3 Hiding the Internal VPN Topology

Note that in addition to the fact that the VPN reachability information distribution is isolated, the reachability information is also carried in an encrypted form on the CE-to-CE part of the network (by sending the routing information messages through the provisioned
CE-CE IPsec tunnels). This means that even when misrouting or malicious snooping occurs, the global VPN topology and the internal topology of the VPN sites is not visible outside of the considered VPN.

The SP should take care not to configure a CE device such that it distributes its VPN routes directly to the PE device (instead of to the peer CE devices through the tunnels). Unless this is required for specific Internet Access scenarios.

5. Security

CE-based VPNs using IPsec are specifically applicable in situations where security is an important requirement and where the outsourcing of the complexity that comes with it is an important requirement. This type of VPNs allows the customer’s data and control traffic to be secured (via encryption) on every shared part of the network, using the very secure and reliable IPsec protocol suite. The result of this is that the customer traffic is not only isolated (via tunnelling) from the other traffic that uses the same backbone, but that the customer traffic is also unreadable (because encrypted) and as such protected against e.g. malicious eavesdropping.

IPsec encryption with optional authentication and replay attack prevention directly meet all of the security requirements in [REQS], as long as key distribution is not compromised.

Note that the provider provisioned CE-based VPNs using IPsec do not protect against accidental or malicious mis-configuration by the service provider, as the SP manages the CE device, which in the most common operation sends and receives VPN traffic in the clear with other customer-premise equipment.

5.1 Protection of User Data

Customer data, both control plane data and user plane data are encapsulated by IPsec before sent to the shared SP backbone. The customer data is protected until it reaches the peer CE. When the customer data is encrypted by IPsec, it is considered secure when it is being transferred through the shared IP backbone.

As such, VPN user data traffic that is intercepted by an entity that was not meant to receive it (e.g. a CE device from an other VPN), will not be visible by that entity because it is encrypted. And traffic that doesn’t belong to a particular VPN will not be able to enter that VPN because the traffic will not be recognized as belonging to one of the Security Associations the CE device maintains, and as such will be dropped by IPsec.
5.2 SP Security Measures

The SP is responsible for preventing illegitimate traffic from entering a VPN. Preventing illegitimate traffic is a matter of ensuring that the CE devices are provisioned with the correct set of peer CE device IP addresses and with the correct security policies and parameters. An intentional or unintentional misconfiguration by the SP whereby two CE devices that do not belong to the same VPN are configured as tunnel and IPsec peers, would make communication between two different VPNs possible in an undesired manner.

The CE device should be secured against break-in, both from someone having physical access to the CE device as from the Internet. As the CE device is physically located at the customer’s premises, securing the CE from compromise by someone physically present is a customer responsibility. Securing the CE device from break-ins via the Internet is accomplished at the CE device by configuring it (by the SP) to limit the types of traffic that are accepted. Indeed, CE devices that do not provide Internet Access to the VPN over the CE-PE link must only accept traffic that is authenticated by this CE device as being either SP management traffic (carried by a secure and authenticated management channel) or intra-VPN traffic (carried by an IPsec secured tunnel). All other traffic must be dropped. CE devices that do provide Internet Access to the VPN over the CE-PE link should accept traffic that is authenticated by this CE device as being either SP management traffic or intra-VPN traffic; all other traffic should be sent to a firewall before accepting it into the VPN.

A management channel exists between SP and the managed CE. It is important for SP to build a secure (authenticated and encrypted) management channel to prevent attacks from the adversary.

The SP must make sure that breaking in into its VPN management system is prohibited (both from someone physically present in the provider’s premises, as via the Internet) in order not to compromise the secrecy of e.g. the VPN tunnel security parameters that the SP maintains.

The SP must ensure the security of its key management infrastructure.

5.3 Security Framework Template

Section 8 of [SEC-FW] provides ‘‘a brief template that may be used to evaluate and summarize how a given PPVPN approach (solution) measures up against the PPVPN Security Framework.’’ It further states ‘‘an evaluation of a given PPVPN approach using this template should appear in the applicability statement for each PPVPN approach.’’ The purpose of this subsection is to provide the information in the form
1. The approach provides complete IP address space separation for each L3 VPN.

The base VPN approach completely addresses the requirement by maintaining and handling the VPN IP address prefixes only in the routing tables of devices that are specific to the particular VPN. They are distributed through encrypted tunnels between devices that are specific to the particular VPN.

2. The approach provides complete L2 address space separation for each L2 VPN.

The requirement is not applicable to the VPN approach because it is applicable only for L2VPN approaches while the discussed VPN approach is a L3VPN approach.

3. The approach provides complete VLAN ID space separation for each L2 VPN.

The requirement is not applicable to the VPN approach because it is applicable only for L2VPN approaches while the discussed VPN approach is a L3VPN approach.

4. The approach provides complete IP route separation for each L3 VPN.

The base VPN approach completely addresses the requirement by having the CE devices distribute the VPN routes through CE-to-CE secure tunnels only.

5. The approach provides complete L2 forwarding separation for each L2 VPN.

The requirement is not applicable to the VPN approach because it is applicable only for L2VPN approaches while the discussed VPN approach is a L3VPN approach.

6. The approach provides a means to prevent improper cross-connection of sites in separate VPNs.

In the VPN approach, the requirement is addressed in a way that is beyond the scope of the VPN mechanisms. In PP CE-based IPsec VPNs, a site is made part of a particular VPN by configuring the CE device with the correct peer CE IP addresses, security policies and IPsec parameters. It’s the SP’s management function that is
responsible not to provision certain CE devices as being part of the wrong VPN.

7. The approach provides a means to detect improper cross-connection of sites in separate VPNs.

If a routing algorithm is run on a particular CE-to-CE (tunnel) interface, any security procedures which the routing algorithm provides (e.g. MD5 authentication) can be used; this is outside of the scope of the VPN scheme. This does not help however if it is the SP who manages the routing aspects on both CE devices and misconfigures the routing aspects too.

8. The approach protects against the introduction of unauthorized packets into each VPN.

The base VPN approach completely addresses the requirement by authenticating all packets that are received at the CE device from a PE-CE link. Packets will only be accepted by the CE device if any the following conditions apply:

- the packet is authenticated as an IPsec protected packet that comes from a peer CE device that belongs to the same VPN;

- the packet is authenticated as belonging to the SP’s management traffic managing the considered CE device.

- the CE device is configured to provide Internet Access to the VPN over the considered CE-PE link, and is configured to direct all packets to a firewall if they don’t fullfil one of the two previous conditions;

The described protection applies for unauthorized packets introduced in any of the following scenarios:

a. In the CE-PE link
b. In a single- or multi- provider PPVPN backbone
c. In the Internet used as PPVPN backbone

9. The approach provides confidentiality (secrecy) protection for PPVPN user data.

The base VPN approach partially addresses the requirement by encrypting any PPVPN user data that leaves a particular site (at a CE device) and by only decrypting the PPVPN user data when it enters a particular site (at a CE device). This means that the user data secrecy is assured by encryption in every part of the network that is not in the customer’s premises. The only reason
why the requirement is only partially addressed is because the SP has access to the CE devices where the PPVPN user data appears in an unencrypted form.

Confidentiality protection of user data within the customer premises is outside of the scope of PPVPN approaches.

The described protection applies for PPVPN user data travelling in any of the following conditions:

   a. In the CE-PE link
   b. In a single- or multi- provider PPVPN backbone
   c. In the Internet used as PPVPN backbone

10. The approach provides sender authentication for PPVPN user data.

The base VPN approach partially addresses the requirement by IPsec processing any PPVPN user data that leaves and enters a particular site (at the CE device). The requirement is only partially addressed as the PPVPN user data is not authenticated as coming from a specific sender, but only as coming from a specific VPN site.

The discussed protection applies for PPVPN user data travelling in any of the following conditions:

   a. In the CE-PE link
   b. In a single- or multi- provider PPVPN backbone
   c. In the Internet used as PPVPN backbone

11. The approach provides integrity protection for PPVPN user data.

The base VPN approach partially addresses the requirement by encrypting any PPVPN user data that leaves a particular site (at a CE device) and by only decrypting the PPVPN user data when it enters a particular site (at a CE device). This means that the user data integrity is assured by encryption in every part of the network that is not in the customer’s premises. The only reason why the requirement is only partially addressed is because the SP has access to the CE devices where the PPVPN user data appears in an unencrypted form so that nothing prevents the SP from touching the PPVPN user data.

Integrity protection of user data within the customer premises is outside of the scope of PPVPN approaches.

The described protection applies for PPVPN user data travelling in
any of the following conditions:

a. In the CE-PE link  
b. In a single- or multi- provider PPVPN backbone  
c. In the Internet used as PPVPN backbone

12. The approach provides protection against replay attacks for PPVPN user data.

The base VPN approach completely addresses the requirement by IPsec processing any PPVPN user data that leaves and enters a particular site (at the CE device).

The described protection applies for PPVPN user data travelling in any of the following conditions:

a. In the CE-PE link  
b. In a single- or multi- provider PPVPN backbone  
c. In the Internet used as PPVPN backbone

13. The approach provides protection against unauthorized traffic pattern analysis for PPVPN user data.

The VPN approach does not meet the requirement. Even though the PPVPN user data is encrypted over every public or SP’s network part, nothing prevents a third party from examining the outer IP header’s IP addresses (the CE WAN addresses), the traffic timing, volume etc. Preventing against this threat is outside of the scope of the discussed VPN approach.

14. The control protocol(s) used for each of the following functions provide for message integrity and peer authentication:

a. VPN membership discovery

   The [CEVPN] approach requires any VPN membership discovery scheme to fulfil the above requirements, though [CEVPN] currently does not specify a membership discovery mechanism.

b. Tunnel establishment

   The base VPN approach completely addresses the requirement by using the IKE(v2) protocol for the tunnel establishment.

c. VPN topology and reachability advertisement

   The base VPN approach partially addresses the requirement because the advertisement of VPN topology and reachability is
done through the IPsec protected CE-to-CE tunnels. The only reason why the requirement is only partially addressed is because the Service Provider has access to the CE device and as such could influence topology advertisements.

i. PE-PE

The requirement is not applicable to the VPN approach because the PE devices are not participating in the VPN topology and reachability advertisement.

ii. PE-CE

The requirement is not applicable to the VPN approach because the PE devices are not participating in the VPN topology and reachability advertisement.

d. VPN provisioning and management

The [CEVPN] approach requires the VPN provisioning and management function to fulfill the above requirements, though [CEVPN] currently does not specify a provisioning and management approach.

e. VPN monitoring and attack detection and reporting

The VPN approach itself does not meet the requirement: the protocols and procedures for monitoring the VPNs are outside the scope of the VPN scheme.

15. Describe the protection, if any, the approach provides against PPVPN-specific DOS attacks (i.e. Inter-trusted-zone DOS attacks):

a. Protection of the service provider infrastructure against Data Plane or Control Plane DOS attacks originated in a private (PPVPN user) network and aimed at PPVPN mechanisms.

For the SP’s network infrastructure (PE and P routers), there is no difference between a DOS attack originated in a PPVPN user network using CE-based IPsec VPNs as compared to a DOS attack originated in any other user network.

The matter in which the SP’s network is protected against DOS attacks originated in a user network is outside of the scope of the CE-based IPsec VPN architecture.

b. Protection of the service provider infrastructure against Data
Plane or Control Plane DOS attacks originated in the Internet and aimed at PPVPN mechanisms.

The protection of the SP’s VPN management infrastructure against DOS attacks originating from the Internet is not different than the protection of any other SP’s management infrastructure against DOS attacks originating from the Internet.

c. Protection of PPVPN users against Data Plane or Control Plane DOS attacks originated from the Internet or from other PPVPN users and aimed at PPVPN mechanisms.

As the CE device’s WAN IP address is routable in the SP’s backbone network (and possibly in the Internet), nothing prevents other PPVPN users (and possibly Internet users) to send excessive amounts of traffic to a particular CE device. The effect of such an attack would be the same as the effect of a DOS attack on any device that uses IPsec secured connections.

Extra protection against such DOS attacks could be achieved by having the PE devices implement VPN-specific access control lists. At first glance this appears to be in contradiction with one of the CE-based VPN characteristics that PE devices be VPN unaware. However, in this case the knowledge required at PE devices would be limited to knowledge of which other devices in the Internet are permitted to send traffic to the CE. This does not, for example, require any PE knowledge of the private network address space nor of the private network routing.

16. Describe the protection, if any, the approach provides against unstable or malicious operation of a PPVPN user network:

a. Protection against high levels of, or malicious design of, routing traffic from PPVPN user networks to the service provider network.

Intra-VPN reachability information is never distributed to SP’s P or PE devices. Dynamic routing between CE and PE devices may however be used in the SP’s routing space for the purpose of distributing the CE’s WAN IP address into the SP’s backbone network. This is not different however from any non-VPN (customer) access router peering with a SP’s edge router, and the same protection mechanisms may be used (such as limiting the amount of PE resources dedicated for the considered routing peer).

b. Protection against high levels of, or malicious design of,
network management traffic from PPVPN user networks to the service provider network.

The discussed CE-based IPsec VPN approach partially protects the service provider network from excessive or malicious network management traffic originated in the PPVPN user networks. Indeed, except for the CE devices, no other devices in the customer’s private network have the ability to send traffic to service provider devices. However, for attacks from the CE device itself, the situation is no different from attacks from devices with normal Internet access. In addition, for attacks originated by other devices in the customer network that have Internet access via some CE device, the situation is no different than for other user devices (not belonging to a CE-based IPsec VPN) that have Internet access. Protection against such attacks is out of the scope of CE-based IPsec VPNs.

c. Protection against worms and probes originated in the PPVPN user networks, sent towards the service provider network.

With CE-based VPNs, the same protection mechanisms against worms and probes originated in the PPVPN user networks apply as against worms and probes originated from e.g. the Internet; these mechanisms are outside of the scope of the considered VPN approach.

6. Addressing

In CE-based IPsec VPNs, it is assumed that the CE devices have one IP address (their ‘WAN’ IP address) that is public or that belongs to the SP’s routing realm. These are the IP addresses that will be used in the encapsulating (outer) IP headers of the tunneled packets that will be sent on the CE-PE link. Beyond use of this CE IP address (that will never be used by the customer’s IGP for intra-site routing and forwarding), there is no constraint on the IP addresses that are internally used within the VPN. In summary, every CE device has to have one WAN IP address that is routable in the SP’s IGP and that doesn’t need to be routable in the customer’s IGP. In order to achieve this, the CE devices will operate in two distinct routing spaces (that they need to keep separate in the CE): the VPN routing space, and the SP’s routing space.

Overlapping customer addresses are supported in different VPNs (meaning that different VPN customers that are provisioned by the same (or different) SP may use overlapping address spaces). There is no requirement that such addresses be in conformance with RFC 1918. There is no requirement that customer VPN-internal addresses be
distinct from addresses in the SP network.

Any set of addresses used in the VPN can be supported, irrespective of how they are assigned, how well they aggregate, whether they are public or private. However, the set of addresses which are reachable from a given VPN site must be unique.

Network address translation for packets leaving/entering a VPN is possible, and is transparent to the VPN scheme.

7. Interoperability and Interworking

As all the different types of Layer-3 VPNs are IP networks, they can of course interwork in the same way that any two IP networks can interwork. For example, a single site can contain a CE router that participates in one VPN scheme (e.g. a Provider Provisioned CE-based VPN solution) and a CE router of another VPN scheme (e.g. a CE that is attached to a 2547bis PE’s VRF), and these CE routers could be IGP peers, or they might even be the same CE router. This would result in the redistribution of routes from one type of VPN to the other, providing the necessary interworking.

8. Network Access

8.1 Access types supported

CE-based IPsec VPNs are applicable in every access scenario where the CE device has IP connectivity with the PE device. Every CE device only needs one IP address that is routable in the shared backbone. This CE-PE IP connectivity may be provided over any Layer-1 and Layer-2 infrastructure (PPP, Ethernet, ATM, Frame Relay, etc.).

8.2 Access QoS support

Providing QoS in the access network is a non VPN-specific feature. Any existing layer-2 QoS mechanism could for example be used for this purpose. General QoS aspects are discussed in section 13.

8.3 Access security support

CE-based IPsec VPNs have the additional advantage that the security of the VPN is not dependent on the security of the access network. Customer data packets traverse the access network in an encrypted way.

Note however that, as IP packets that are sent from CE to PE are not authenticated by the PE devices, the CE-based IPsec VPN model does not protect against resource spoofing and Denial of Service Attacks.
by invalid users. An intruder can still inject traffic on the access link, which will be forwarded by the PE device towards the destined CE device.

When a CE device that is configured for a certain VPN would be moved and placed in a different location (e.g. in a different VPN’s premises), the following scenarios are possible:

- the CE device would receive a new WAN IP address, and as the other CE devices belonging to the original VPN will not recognise this new IP address, this would prevent the establishment of VPN tunnels from this new location; in addition, the SP’s management system would detect this connectivity loss from the old IP address;

- the CE device would keep its own WAN IP address but without distributing this outside of its new location via a routing protocol; this would make the CE device unreachable and would prevent the establishment of VPN tunnels from this new location;

- the CE device would keep its own WAN IP address and distribute it via a routing protocol via its new location into the SP’s backbone; in this situation, the CE device will be able to access the other VPN from within its new location. This situation should not be allowed by prohibiting the movement of the CE devices outside of the VPN customer’s premises.

When the configuration of a CE device, located at the VPN customer’s premises, is deliberately or unintentionally changed without prior agreement of the SP, access to the VPN from the Internet or from sites belonging to different VPNs may become possible, and VPN data may leak out of the VPN. As such, the customer must make sure that access to the CE device is restricted to the VPN SP, or to authorized and knowledgeable people from the customer’s IT department.

Note that it is not possible for a particular customer to intentionally misconfigure its CE device in an attempt to access some other VPN. Indeed, there is no way for this particular customer to know the necessary keys and authentication credentials that are specific to every VPN tunnel.

9. Service Access

9.1 Internet Access

Internet access and VPN access are possible from the same site. Different ways to accomplish this service are possible. One restriction is that the VPN’s internal addresses must be distinct from the IP addresses of the systems which must be reached via the
Internet. The required NAT and firewall functions are implemented in one or more of the VPN’s CE devices or dedicated gateways.

A typical scenario is that the CE would have to direct all non-IPsec traffic to a firewall.

When the CE-based VPN traffic shares the access (CE-PE part of the network) with Internet-traffic, a denial of service attack from sites outside the VPN is possible.

9.2 Hosting, ASP, Other Services

Externally provided services can be accessed from the VPN through a firewall located at a VPN site, provided that it can be addressed with an IP address that is not otherwise in use within the VPN. If the considered service is offered by the same server for a number of VPNs, and a certain client with a non-unique IP address is accessing the server, NAT has to be performed at the client’s CE device.

10. SP Routing

Routing through the backbone(s) is independent of the VPN scheme, and is unaffected by the presence or absence of VPNs. The only impact is that the backbone routing (or Internet routing) must carry the routes to the CE devices.

The use of CE-CE IP tunnels is not impacted by (and is thus complementary with) any PE-PE tunneling that the Network Provider might deploy in its backbone network (e.g. PE-PE MPLS LSPs for Traffic Engineering reasons).

11. Migration Impact

The migration impacts that are discussed here deal with:

(i) a customer who migrates from a legacy (frame-relay type) IP over Layer-2 VPN to a provider provisioned CE-based IPsec VPN, or

(ii) a customer who migrates from a customer provisioned CE-based IPsec VPN to a provider provisioned CE-based IPsec VPN.

11.1 Functions to be added to the customer’s CE device

- migration scenario (i)

Assuming that the customer CE router has IP connectivity with the PE router, the following functionality needs to be added on the customer equipment:
- the customer’s CE device needs to implement the IPsec protocol suite and an IPsec key exchange functionality, such as IKE.

- the CE device needs to support the secure management protocol that is used by the SP’s management system.

- the CE device’s routing protocol(s) needs to treat the different IPsec secured CE-to-CE tunnels as independent interfaces.

- in the scenario where both the customer and the Service Provider have management responsibilities on the CE device, the CE device must support a management security infrastructure that allows for the separation of management responsibilities according to specified rules.

- the CE device must have its frame relay port replaced with whatever is needed to access the SP’s network (unless this is FR).

- the customer’s virtual topology may need to be redesigned, including a study of the impact of this design on the customer’s IGP. Note that it is not necessarily the case that the FR DLCI’s should be replaced one by one with IPsec SAs.

- migration scenario (ii)

- the customer’s CE device needs to implement the IPsec key exchange functionality (IKE(v2))

- the CE device needs to support the secure management protocol that is used by the SP’s management system.

- if a public key infrastructure is provided by the SP, the CE device needs to support this infrastructure.

- in the scenario where both the customer and the Service Provider have management responsibilities on the CE device, the CE device must support a management security infrastructure that allows for the separation of management responsibilities according to specified rules.

11.2 functions to be added by the Service Provider

- The SP needs to deploy a secure management system that is able to configure and manage a large amount of CE devices per VPN customer.
- In the case that the SP is also the backbone network provider, the SP needs to provide IP connectivity between CE devices.

- The SP needs to be able to define topology, security protection, and reachability attributes for each customer VPN it manages.

- The SP needs to be able to configure each managed CE, based on the attributes of the VPN that the CE belongs to.

- The SP needs to be able to update each VPN, based on customer needs from time to time. Changes such as adding or deleting VPN sites, upgrading VPN functions are common.

- The SP may need to have the capability of managing and monitoring the SLA of the customer’s VPN.

- The SP needs to be able to gather and create appropriate usage and accounting report for each VPN it manages.

12. Scalability

This section discusses how certain specific VPN-metrics affect the scalability of the VPN-solution.

12.1 Number of supported VPNs

It is assumed that a certain site is only part of one VPN. Architectures that allow sites to be a member of multiple VPNs will have impact on the CE devices and on the supported addressing schemes.

When a site can be a member of only one VPN, the number of VPNs that a SP can support has an impact on the SP’s management system.

For every supported VPN, the SP’s management system will need to be able to provision every site’s CE device that belongs to that VPN. The management system will need to maintain information that is specific for every VPN site (IP addresses of the other peering sites in the considered VPN, security information, etc.).

The number of VPNs that a SP can support is dependent on the number of sites per VPN and is limited by the number of management sessions the SP’s VPN management system can support and the amount of VPN information the SP’s VPN database can maintain.

Note however that when the number of VPNs increases, the SP can deploy additional management systems with their own VPN databases: the SP can use multiple independent management systems as there is no
interaction between different VPNs.

12.2 Number of sites per VPN

In a fully-meshed VPN, the number of sites per VPN has an impact on the CE devices within that VPN, on the SP’s management system and on the SP’s key distribution system.

In one particular fully-meshed VPN, for every additional site, a certain CE router needs to maintain an additional VPN tunnel (in the form of an additional IPsec Security Association) and additional reachability information.

For every VPN site, the SP’s management system will need to maintain some information and will need to be able to establish a management connection to the site’s CE device.

The number of sites per VPN (n) has an impact of O(n) on the CE devices, and has an impact of O(n^2) on the number of tunnels that the SP management system needs to provision (in a fully-meshed VPN).

In VPNs that are not fully meshed (partial mesh or hub and spoke topology), the impact of the number of sites per VPN on the scalability of the system is reduced.

In a hub and spoke VPN, the CE of the hub site still needs to maintain as many tunnels as there are other sites (n-1), and will still need to maintain the complete set of VPN routes. The CEs of the spoke sites on the other hand, need only to maintain one tunnel towards the hub CE. Moreover, in a hub and spoke topology, the spoke CEs may not need to maintain the other CE’s routes: a default route towards the hub CE may suffice. The SP’s management system needs to maintain O(n) tunnels in a hub and spoke VPN.

Note that the total number of CE devices to support may prove to be the most critical scalability factor for the SP’s management system, especially in terms of automatically updating the CE devices’ configuration upon a certain change. The reliability mechanism involved may have a per-CE scaling component.

12.3 Number of tunnels per VPN

The number of tunnels per VPN depends on the number of sites per VPN and on the VPN topology.

The hub-and-spoke topology requires the least amount of tunnels to provide inter-connection among all participating sites (O(n)), while a fully meshed VPN requires the most tunnels (O(n^2)).
Aside from the number of tunnels, the VPN security attributes also affect the scalability of a VPN. For example, when a VPN uses 3DES as the tunnel encryption scheme, the total number of tunnels that a hub may support may be smaller than the case when e.g. DES is selected.

The number of tunnels that are required specifies the number of SAs that need to be maintained, and this has an impact on the number of keys to be supported and thus on the SP’s key distribution system.

12.4 Number of tunnels per CE

The number of tunnels to be supported by a CE device has implications on the performance of that CE device: every supported tunnel represents a new interface; every tunnel is protected by a specific Security Association.

The overall CE performance will decline when the number of tunnels increases as the memory consumption increases and the processing increases: every Security Association that protects a tunnel needs to be frequently re-negotiated. This (frequent) re-keying of existing (permanent) tunnels requires a certain amount of processing (key generation) and of control protocol message exchanges (via IKE or an alternative key exchange protocol).

The number of tunnels a CE will need to support at a given time can be dependent on whether 'traffic-driven' tunnel set-up or 'traffic-independent' tunnel set-up is used.

Note that the use of traffic-driven tunnel set-up has important implications. In traffic-driven tunnel establishment, if a certain tunnel does not carry traffic during a certain amount of time, the IPsec SA will be removed. When traffic starts flowing again, a new Security Association will need to be established first. The two tunnel endpoints will re-negotiate the necessary SAs, and will generate the necessary key material. This not only introduces control protocol message exchanges but also delay in the forwarding of the user packets.

Note also that the inter-site reachability distribution interacts with traffic-driven tunnel establishment: routing protocols send routing updates and keep-alive messages, even when no actual user traffic is flowing.

As such, traffic-driven tunnel set-up may be applicable in CE-based IPsec PPVPNs that use statically provisioned routing information. The use in an environment that dynamically distributes inter-site reachability is much more complicated and not advised.
Note that the number of tunnels per CE has a scalability impact on the customer’s IGP, as every tunnel is seen as an interface from the IGP point of view.

12.5 Number of routes per VPN

The number of routes per VPN has only an impact on the CE devices. The SP network and management system are not affected by the number of routes per VPN (except when static routes are configured by the SP).

In a fully-meshed VPN, the number of routes a VPN can support is limited by the maximum number of routes that the ‘smallest’ CE can maintain.

In a VPN with a hub and spoke topology, the number of routes a VPN can support is limited by the maximum number of routes that the hub CE can maintain (as the spoke CEs can be provisioned with a default route towards the hub CE).

Independent of the VPN topology, the number of routes that a PE device needs to maintain is limited to one per CE interface.

12.6 Impact of configuration changes

The impact of configuration changes (e.g. the addition of a new site to an existing VPN) highly depends on the ‘auto-discovery’ mechanism used by the SP. The specifics of the autodiscovery mechanism used (reliability etc.) may have an impact on:

- the number of devices to separately provision,
- the increase of control traffic,
- the convergence time, etc.

Note that [CEVPN] does not specify an auto-discovery mechanism.

Note also that other factors such as the rate of configuration changes may have an impact on the scalability of the VPN service.

12.7 Performance impact

The deployment of a CE-based VPN will have a performance impact on the system.

With regards to the control plane, the CE devices will need to negotiate Security Associations and generate cryptographic key
material. The initial SA negotiations are triggered by SP provisioning or by traffic flowing (traffic-driven SA setup). Established SA’s need to be frequently ‘refreshed’: new key material needs to be generated and exchanged. As such, the maintenance of SA’s introduces a constant load on the CE’s control plane.

In the data-plane, the use of IPsec protected CE-to-CE tunnels means that every IP packet that is sent from one CE to another needs to be encrypted and/or authenticated by IPsec. This affects the performance as it requires additional processing and introduces some delay.

Note that in a hub and spoke topology, this impact is doubled: a packet that flows from one spoke site to an other spoke site will be encrypted at the first spoke’s CE, decrypted at the hub CE, routed at the hub CE, encrypted at the hub CE and finally decrypted at the destination spoke’s CE router.

12.8 Scalability of Key Distribution Infrastructure

In the case where pre-shared keys are used by IPsec for the CE-to-CE SA, the Service Provider needs to maintain pre-shared keys for every CE-CE pair of the same VPN that need to protect a VPN tunnel. Securely storing these pre-shared keys, and more or less frequently generating and distributing fresh pre-shared keys for all established SAs may become a scalability concern when the number of SAs grows and when the rate of site addition/deletion grows.

In the case where private/public keys are used in combination with digital certificates, the Service Provider must install/use a public key infrastructure (PKI). This has a number of implications for the SP. The SP needs to maintain a database that contains the digitally signed public keys of every participating CE device. The SP also needs to maintain a revocation database that contains the digitally signed public keys that are no longer valid (e.g. for removed VPN sites). The SP needs for every CE device to verify the integrity of the <CE-device, public Key> association. The SP must make sure that the CE device’s private keys are (more or less frequently) re-generated, and must as a result of this re-keying generate a new certificate and distribute this. The SP must (more or less frequently) refresh its own private and public key that it uses to sign the necessary certificates, and as a result of this sign all existing certificates with its new keying material.

These procedures are not different from any other PKI, and the scalability is dependent of the number of end-nodes (CE devices), of the number of secure connections to maintain and on the dynamicity of end node creation/deletion (VPN join and leave operations.)
13. QoS, SLA

In addition to the VPN service (reachability and security) from the SP, the VPN customer may want to acquire QoS features for its VPN. Depending on the business scenario, the SLA will be provided by the VPN SP or by the Network Provider.

Note that the fact that customer IP packets are encapsulated (and possibly encrypted) at the CE devices has an impact on the QoS treatment of the IP packets: QoS-related information inside the customer IP packets may become invisible.

An eventual translation of QoS-related fields (e.g. DSCP) in the inner IP header to QoS-related fields in the outer IP headers need to be done at the CE-level and configured as such by the SP. Also the ‘policing’ rules (e.g. certain customers not being allowed to use certain QoS values, etc.) need to be configured by the SP in the CE devices. The security infrastructure of the CE device must prevent the customer from messing with this provider-controlled configuration.

The CE-CE tunneling applied in Provider Provisioned CE-based IPsec VPNs easily meets the DSCP transparency requirements of [REQS].

14. Management

14.1 Configuration/provisioning

Configuration by the SP comes in at two levels: VPN level and CE level.

At the VPN level, the topology and security requirements must be determined. Common topologies include hub and spoke and full mesh. For large VPNs, a combination of simple topologies may be used, such as a full mesh core that connects individual hub and spoke topologies. A given VPN must have a general security grade selected, since every link of the VPN is expected to meet this security grade. In addition to the topology and security information, at the VPN level, when no inter-site tunneled dynamic routing is required, the reachability information may also be determined.

At the CE level, each CE must know all of its CE peers in the same VPN, the security parameters, the tunnel attributes, the device or tunnel authentication credentials, and any associated routing setups.

14.2 Customer management
Since a customer outsources the VPN provisioning and management, it may not have the permission to change any of the VPN parameters in its CE devices.

In a scenario where both the customer and the provider have VPN management responsibilities, the provider’s management protocol will need to specify which parameters can be customer managed and which parameters cannot. An agreement between the customer and the service provider will need to specify which of the parameters that can be managed by the customer will be managed by the customer.

It must be possible for the SP to retrieve the CE’s actual configuration state, in order to verify whether the customer has not violated the agreement (e.g. an unintentional misconfiguration, or an intentional theft of QoS service).

14.3 SLA monitoring

It must be possible for the SP to retrieve the CE’s actual configuration state, in order to verify whether the customer has not violated the agreement (e.g. an unintentional misconfiguration, or an intentional theft of QoS service). In addition to this, the SP may want to collect statistics by retrieving specific files from the CE devices.

14.4 Security

The security aspects of the VPN management system are extremely important.

De SP’s management system itself needs to be secured against misconfiguration, intrusion and denial-of-service attacks.

De management protocol that is used to remotely provision the CE devices needs to provide for mutual authentication, encryption of the transported data, etc.

The CE device must support the necessary security architecture, allowing for eventual dual-management, firewall support etc.

14.5 Fault handling

The faults that occur in the network(s) that interconnect CEs have an impact on the CE-to-CE routing.

If the timers used for the CE-to-CE routing peering are shorter than the timers used for the routing peering within the service provider(s) network, then a single failure within a service provider
network may look like a collection of uncorrelated failures in the VPN.

Moreover, since a CE doesn’t really "know" what causes the failure, the CE may react to such a failure by re-routing along some other tunnel, while this other tunnel may be also affected by the same failure. As a result, this would slow down routing convergence within the VPN.

To avoid the problems mentioned above one may consider making the timers used for the CE-to-CE peering longer than the timers used for the routing peering within the service provider network (so that failures within the service provider network would be "invisible" to the CE-CE tunnels). But that has its own set of problems. While this may be possible to accomplish within a single routing domain (one needs to appropriately set the IGP timers within the domain), doing this in a network that includes more than one routing domain may be fairly problematic (as timers include both IGP and BGP timers, and moreover, timers include IGP timers in several routing domains). Moreover, making the timers used for the CE-to-CE peering over the tunnels longer than the timers used for the routing peering within the service provider network would increase the amount of traffic that will be "black holed" in the case of CE failures.

15. Security considerations

This draft contains sections that discuss in detail the security of provider provisioned CE-based IPsec VPNs.

16. Acknowledgements

The authors of this draft would like to thank Eric Rosen, Yakov Rekhter, Tom Nadeau, Marco Carugi and Ross Callon for their valuable comments and suggestions.

17. References


Layer-3 Provider Provisioned Virtual Private Networks," work in progress


18. Authors’ Addresses

Jeremy De Clercq
Alcatel
Fr. Wellesplein 1, 2018 Antwerpen, Belgium
E-mail: jeremy.de_clercq@alcatel.be

Cliff Wang
E-mail: cliff.wang@us.army.mil

Dave McDysan
WorldCom
22001 Loudoun County Parkway
Ashburn VA 20147, USA
E-mail: dave.mcdysan@wcom.com