



A framework for Provider Provisioned CE-based VPNs using IPsec

draft-ietf-ppvvpn-ce-based-00.txt

J. De Clercq, O. Paridaens, M. Iyer, A. Krywaniuk (Alcatel)



AGENDA

draft overview

reference model

configuration

exchanging routes

tunneling VPN traffic

issues

future



draft overview

reference model



- ▼ synchronise with draft-ietf-ppvpn-framework-XX.txt
- ▼ CE-device
 - assumed reachability: IP connectivity with Provider Network via PE device
 - VPN functions to be managed by Service Provider
- ▼ PE-device
 - no VPN-specific functions on data plane
- ▼ Service Provider Management system has a secure control channel to every attached CE device

configuring the CE-based VPN



- ▼ configuration of SP VPN database
- ▼ configuration of CE-device
 - 'control channel' information
 - peer CE devices
 - security information
- ▼ updating configuration information
 - e.g. adding/deleting a VPN site to/from existing VPN
 - use of a dynamic 'management protocol'
 - pushes VPN info from SP to CE-devices
 - or triggers CE device to pull VPN info from SP database
 - e.g. : COPS, LDAP, SNMP, etc.

configuring the CE-based VPN (bis)



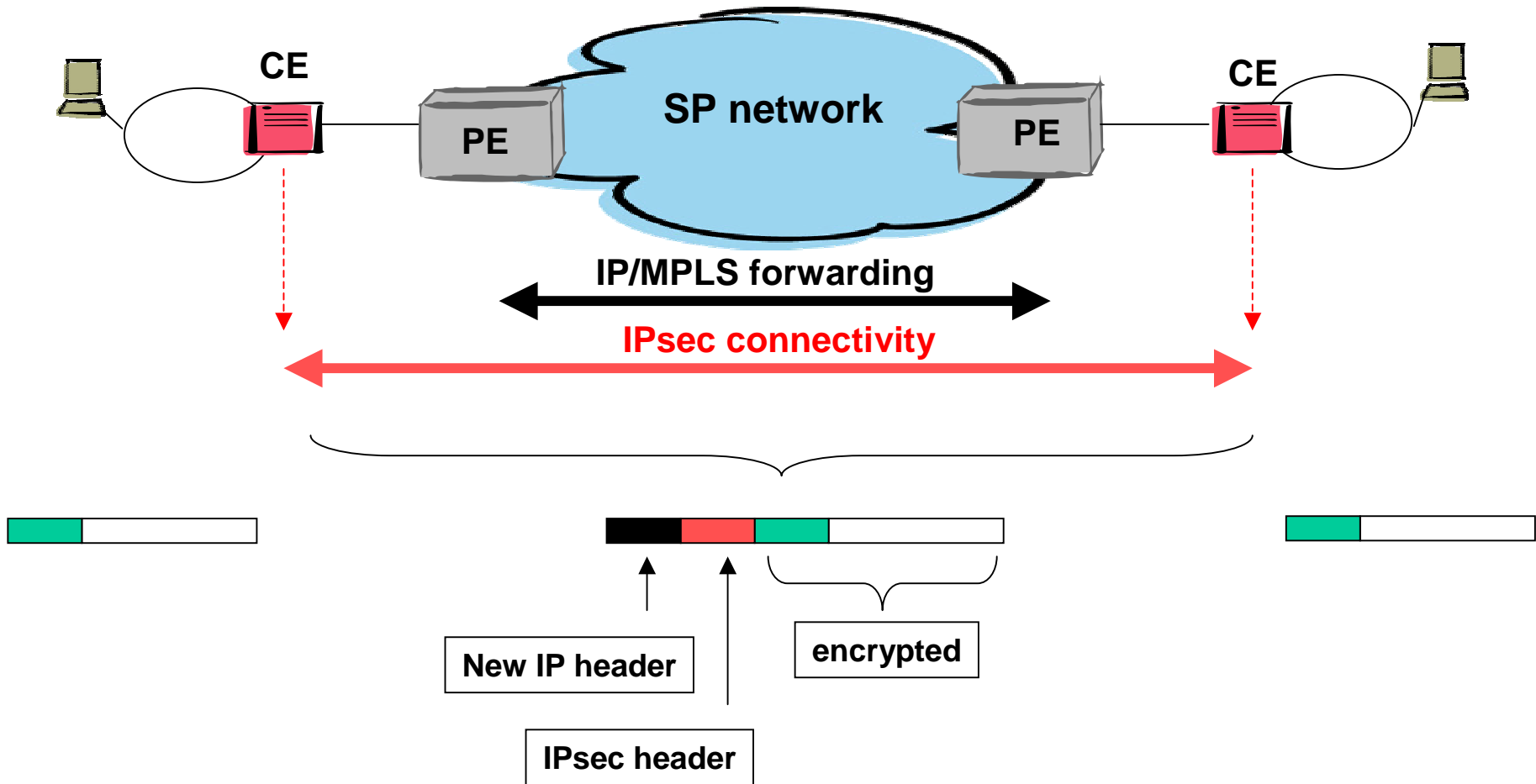
- ▼ setting up the VPN tunnels
 - IKE or alternative to be used for dynamic set-up of SA
 - IPsec tunnels
 - traffic-driven
 - or 'permanent' IPsec tunnels
 - number of IPsec tunnels is dependent on 'role' of VPN site
 - hub, spoke, etc.

exchanging and maintaining VPN routes



- ▼ exchange of VPN reachability information
- ▼ proposed mechanism 1 : tunneling routing information between CE devices through the IPsec tunnels
 - routing protocol messages need to be carried in IP
 - issue with traffic-driven tunnel set-up
- ▼ proposed mechanism 2 : exchanging VPN reachability information via SP's management
 - CE communicates updated reachability information to SP management
 - SP management updates other CE devices in VPN

tunnelling IP traffic among VPN sites



tunnelling IP traffic among VPN sites



- ▼ dependent on the IPsec 'mode'
 - in tunnel mode
 - IPsec process does SA selection, encapsulation and authentication/encryption
 - in transport mode
 - as in draft-touch-ipsec-vpn
 - private IP packet first IP-in-IP encapsulated according to routing table
 - then processed by IPsec engine



issues/discussion



- ▼ ID as it is now is neither a complete framework, nor a detailed solution specification
 - e.g. only IPsec is considered for tunnelling
 - alternatives : L2TP, GRE, MPLS, IPinIP, etc.
- ▼ SP management system
 - no protocol suggested
 - securing the 'control channel'
- ▼ some mechanisms might require IPsec extensions
 - see draft-gleeson-ipsec-ppvnp
 - routing through tunnels
 - 'permanent' tunnels



future

future of the draft



- ▼ PPVPN charter requires set of PPVPN solution documents
- ▼ synchronize/add some parts with/to PPVPN framework draft ?
- ▼ evolve this work to **solution proposal** (including required technical details) for CE based IPsec VPNs ?
 - on 'secure control channel'
 - on 'security information'
 - etc.
- ▼ line up with IPSP, IPsec, etc. work



THANK YOU, QUESTIONS ?

jeremy.de_clercq@alcatel.be