CE-to-CE Authentication for RFC 2547 VPNs

draft-bonica-l3vpn-auth-02.txt

The Problem

- SP maintains two VPNs
  - One for Customer A and one for Customer B
- SP provisions one of Customer A's interfaces into Customer B's VPN
- Customer A is first to know about the problem
- Customer B may never know about the security breach

How Could This Happen

- Administrative accident
- SP is victim of social engineering attack

The Solution: CE Based Authentication

- Each VPN site sends SP one or more “magic cookies”
- SP associates magic cookie with routes to VPN site.
- SP uses BGP to distribute both magic cookies and VPN routes through provider network
- SP delivers magic cookie to all remote VPN sites (BGP or SSL transport)
- CE authenticates magic cookies

Limits of Trust

- VPN customer must trust the SP to implement the solution correctly
- VPN customer need not trust the SP to be 100% immune to misconfiguration and social engineering attacks
- Solve 80% of the problem with a cheap solution

Next Steps

- Adopt draft as WG document
- Implement and obtain operational experience