CE-to-CE Authentication for RFC 2547 VPNs

draft-bonica-l3vpn-auth-01.txt

Why the Paranoia

- SP can accidentally provision Customer_A interface into Customer_B VPN
- Consequences
  - Customer_B receives no automatic indication of VPN breach
  - SP receives no automatic indication of misconfiguration
  - Customer_A notifies Service Provider of misconfiguration (sooner or later)

How Do We Fix This

- PE does not permit CE to participate in a VPN until VPN site submits *magic cookie(s)* to PE
- Provider distributes *magic cookies* to other CE routers that support VPN
- CE routers use *magic cookies* to authenticate remote VPN sites
  - If CE receives cookie that it cannot authenticate, it issues alarm and withdraws from VPN if required to do so by local security policy

How Does This Work

- Using BGP or new protocol, CE sends cookie(s) to PE
- PE associates each prefix for which CE is next hop with cookies learned from that CE
- PE uses new BGP extended community attribute to distribute cookies along with prefixes to other PE routers that support VPN

How Does This Work (continued)

- Remote PE uses BGP or new protocol to distribute all cookies associated with VPN routes to CE
  - Null cookie

What Does This New Protocol Look Like

- Largely TBD
- But we know
  - It is very simple
  - Runs over TCP
  - Probably needs some kind of authentication

Proposal

- Adopt as WG draft
- Continue work on new protocol