Establishing a Dynamic Security Perimeter

Protecting the ever changing WAN boundaries

The evolving WAN perimeter

Adoption of Internet links for WAN transport, and the popularity of direct Internet access (DIA) from branches completely altered your enterprise security boundaries. The old practice of securing the network at a centralized DMZ is becoming obsolete, just as branches are increasingly targeted. Placing a firewall at each branch is complex and costly; you need a different approach.

Create a secure, Application-defined Fabric

Simply deploy CloudGenix ION software at each branch. The ION nodes establish secure peer-to-peer channels and form a “fabric” across your hybrid WAN. Use the ION central controller to define application security policies, and they

Hybrid-WAN protection

Adding Internet links to a private MPLS network establishes a cost-effective hybrid WAN. Yet its newly shaped ‘WAN surface’ is a prime target for attacks. Traditional methods based on backhauling traffic to a centrally located DMZ no longer apply. Hybrid WANs require a different approach, based on a software-defined WAN (SD-WAN) that dynamically adjusts to a changing WAN perimeter and automatically applies application-defined security policies where and when they are needed.

Copyright CloudGenix 2014
will be applied at each branch, dynamically protecting your changing WAN perimeter.

**Instantly securing a Hybrid WAN**

Traffic between ION nodes is encrypted using dynamically rotating security keys, creating a fully secured network fabric, independently of underlying transports. Hybrid WANs, which combine MPLS with public Internet, are instantly secured.

**Traffic isolation via Secure Contexts**

Use the central ION controller to define ‘secure contexts’ based on apps and user groupings. Traffic in each context is encrypted and isolated from all other contexts. This alleviates the need to grapple with low-level routing-based segmentation (e.g. VRFs), and quickly achieve regulatory compliance (e.g. PCI, HIPAA).

**Auto-adjusting Application firewalls**

ION nodes have built-in application firewalls. Policies are derived from ‘secure contexts’ defined at the ION controller. Applications are auto detected by each ION node, triggering activation of the associated security policies. The WAN security perimeter is dynamically adjusted without any extra configurations.

**Security services projection**

ION nodes redirect (i.e. project) application traffic to the closest security service node, based on each context policies. Security functions are instantly enforced across the WAN perimeter, without having to roll-out special devices to each edge location.