The GABRIEL Connection Technology

GABRIEL Connection Technology

GABRIEL Connection Technology was developed by VirnetX scientists and engineers to empower individuals, organizations of all sizes and government agencies to establish and administer their own private network enclaves or *Safe Neighborhoods* across the Internet. These enclaves provide cryptographic privacy for all data within the enclave and cryptographic authentication of all of its participants. Figure 1 illustrates how VirnetX Security Platform (VSP)-enabled *Safe Neighborhoods* have changed the way people think about network enclaves. Instead of networks being secured by physical barriers, they're defined cryptographically, thereby allowing secure domains to be dynamically established on demand without regard to the physical location of the domain participants.

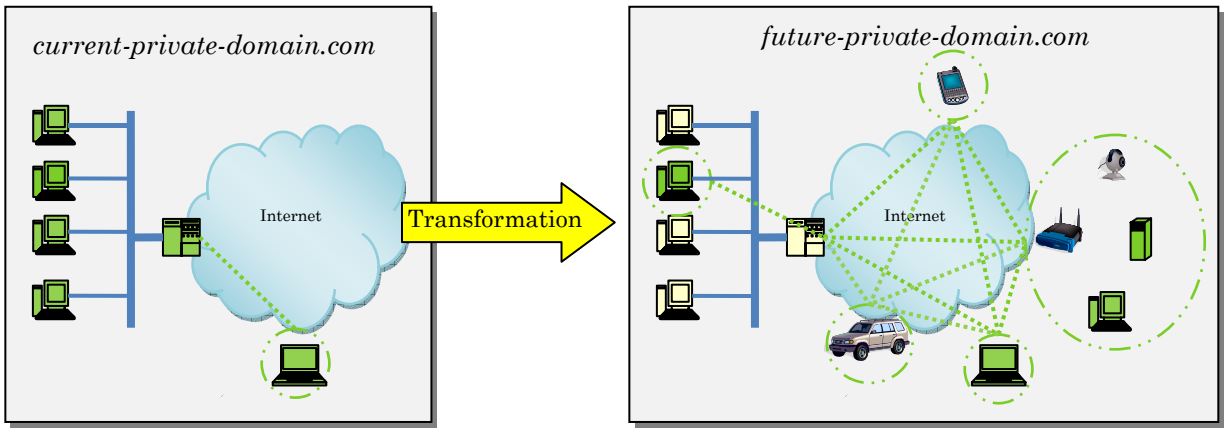

Figure 1 Secure virtual private domains will change the way we think about network enclaves.

The establishment and administration of these enclaves is achieved through the registration of secure domain names and the issuance of user and device host names within the secure domain. Authentication and control of users joining the domain is achieved by requiring signed certificates. Users and/or devices can be removed from the domain by either expiring or revoking their certificates.

Once an individual or organization registers a domain, that entity is then empowered to invite other participants within the domain by issuing sub-domain names, which include cryptographic digital certificates signed by VirnetX. The name and user information associated with that name are then authenticated. The domain administrator can also revoke or retire sub-domain names to remove users or devices from the domain. For example, the Smith family can register a secure domain name such as *smith-family.net*. Members and devices within the Smith family are then registered with sub-domain names

such as *dad.smith-family.net*, *mom.smith-family.net*, *susan.smith-family.net*, *john.smith-family.net*, *media-server.smith-family.net*, *kitchen.smith-family.net*, *home-gateway.smith-family.net*, etc. These secure domain names enable users and devices to connect safely within their own secure virtual private domain or virtual local network, regardless of where the users and devices are physically located across the Internet.

Virtual network privacy is provided by peer-to-peer encrypted Internet protocol (IP) connections for all application communications between user/device platforms. This peer-to-peer encryption is achieved by the dynamic on-demand, setup and tear-down of virtual private network (VPN) tunnels between peer platforms. Cryptographic peer authentication and security policy enforcement is automatically performed by the VirnetX connection services software hosted on the peer devices. Private keys never leave the peer platforms, and public keys are certified by VirnetX signed digital certificates. Presence of domain users and devices is discovered through domain name lookups and automatic registering and querying of VirnetX-enabled connection servers. Applications can automatically initiate VPN tunnels through the legacy domain name service (DNS) lookup paradigm.

Network address translation (NAT) and firewall device traversal are achieved by the automatic discovery and negotiation of relay services that are required on a peer-to-peer connection basis. When relay services are mandatory, the peer-to-peer encryption is maintained and the relay server receives and forwards encrypted data packets to maintain end-to-end data privacy.

Because all peer domain participants are cryptographically authenticated, each individual user can establish and maintain a unique security policy for their platform. This policy can identify domain participation parameters such as:

- Who the peer is willing to connect with
- Who the peer is willing to share presence with
- The level of machine access given to each participant
- Peer-specific file/folder sharing
- Peer-specific login privileges

The VirnetX technology suite includes infrastructure security code that is application-agnostic, enabling all TCP-UDP/IP application protocols. This is distinguished from current approaches to dynamic on-demand peer-to-peer secure connections, which are enabled at the application level. While application-level secure connections serve the purpose of protecting individual application communication, they have the disadvantage of requiring explicit secure networking features in each program, which makes integrating multiple applications more difficult. VirnetX believes that secure networking should be a platform/network infrastructure function in much the same way that current IP networking, host-based firewall security, file access management, and process isolation and scheduling are basic platform system functions. The VirnetX approach is to implement security at the IP layer using industry-standard VPN encryption technology and the VirnetX

proprietary DNS-triggered instant secure connect (ISC) dynamic on-demand VPN initiation technology. This approach brings the benefits of cryptographic authentication and privacy to all legacy and new platform applications, without requiring application developers to incorporate their own secure networking.

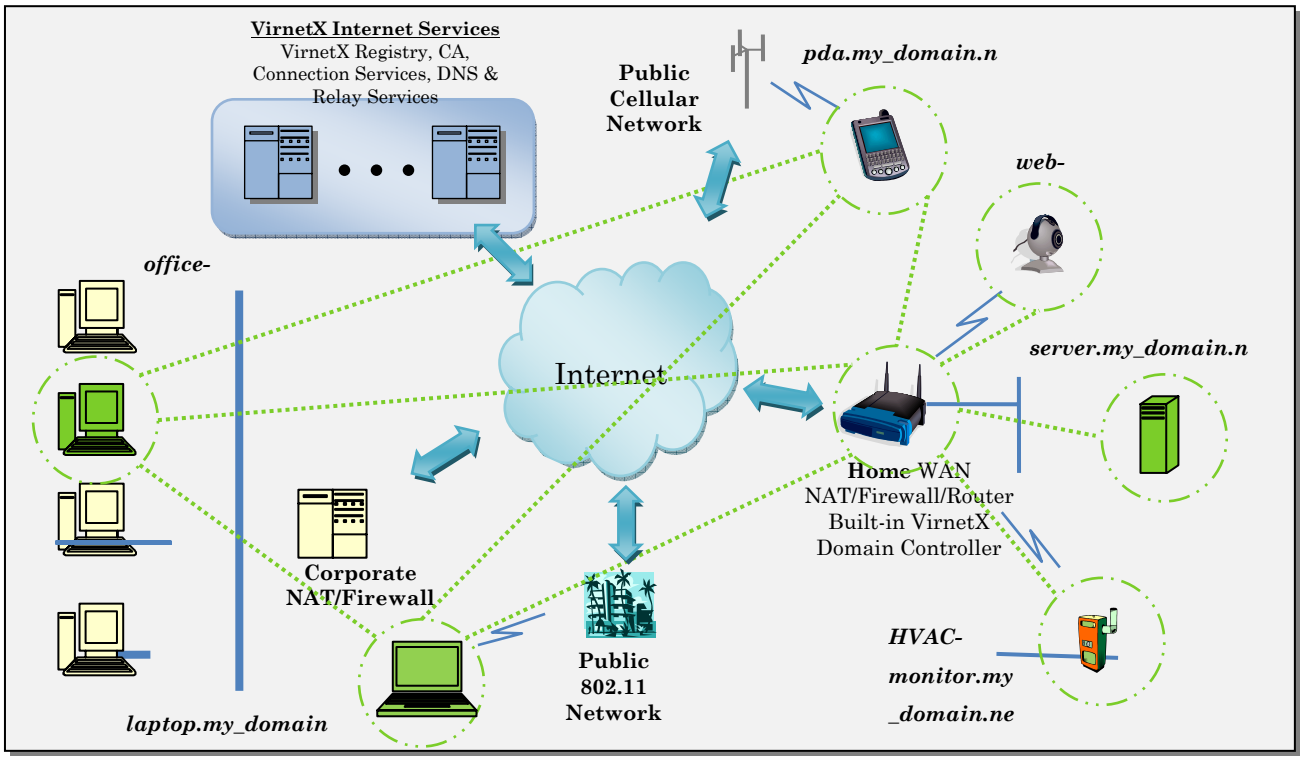

Figure 2 The VSP architecture enables secure private domains with network boundaries defined cryptographically rather than by physical connections.

VirnetX Security Platform™

The VirnetX Security Platform is implemented using the *GABRIEL Connection Technology* within a distributed architecture, which modularizes the security, communication and administration functions into separate components. These functional components interoperate across a widely distributed physical network of computing devices consisting of static IP address computers, dynamic address computers, gateway devices, mobile laptops, personal digital assistants (PDAs), cell phones and any number of next-generation network appliances. Figure 2 illustrates a sample view of the VSP-enabled *Safe Neighborhoods* product suite.

In this illustration, each network device within the *my_domain.net* secure domain has VirnetX client software, which enables platform security. This platform security software provides:

- User-defined security policy
- On-demand no-click peer-to-peer VPN initiation
- DNS intercept for:
  - Automatic VPN initiation
  - Remote peer address private resolution

  - Certified peer IP address reverse lookup
- Cryptographic peer authentication
- NAT/firewall discovery and relay service request
- Peer presence discovery
- Own presence network registration

In addition to the secure network infrastructure functions, the VirnetX client software offers seamless access to a select number of high-utility peer-to-peer applications. The initial set of candidate offerings include:

- File sharing – including user-defined folder access policies on a per-peer basis and drag-and-drop user interface
- Real-time communication (RTC) – incorporating instant messaging (*e-chat*), Voice-over-IP (VoIP) (*e-talk*), and message posting with attachments (*e-post*).
- Remote Desktop – allowing secure desktop access across the Internet
- Distributed file backup and synchronization – providing opportunistic data backup and synchronization of data files regardless of a platform's physical location as a background, non-interfering process

VirnetX's GABRIEL Connection Technology makes secure real-time communications seamless, automatic and transparent, and it fits everyone's needs. For more information on VirnetX's GABRIEL Connection Technology and VirnetX Holding Corporation, visit www.virnetx.com.