2/8/2006

A Cranite Whitepaper

SafeConnect

The Future of Remote Connectivity

Table of Contents:

1. Remote Connectivity—Not All It's Cracked Up To Be 2
2. Remote Connectivity—The Way It Needs To Be................... 3
3. Centralized Management, Distributed Enforcement 4
4. A Unique Layer of Protection.. 5
5. Privacy and Integrity 7
6. Conclusion 7

1. Remote Connectivity—Not All It's Cracked Up To Be

As enterprise networks have evolved over the past decade, organizations have deployed a variety of access control methods in an attempt to provide remote users with the same computing experience they receive when sitting at their desks. To date, this remote computing experience still falls woefully short of the goal, largely because remote users are still treated as untrusted users. In the early days of dial-in access, the threat model was largely confined to wardialers and dictionary attacks. At worst, organizations had to worry about data compromise on low-bandwidth links terminating at the very edge of the enterprise. As networks have become more complex and as users have become more mobile, leaders and managers have come to expect more and more productivity from their mobile users—resulting in an awkward tradeoff between locking down the perimeter to ensure security, and punching holes in the perimeter to ensure productivity. The result? A misguided attempt at network extension that swaps security for functionality, and vice versa.

Computer network defense has evolved from the early days of ensuring that dial-up users didn't lose the passwords written on sticky notes on their laptops to today's complex myriad of devices intended to keep bad guys out. In striving to keep out the bad guys, the good guys (i.e., authorized enterprise users) are forced to endure a less-than-complete and less-than-satisfying enterprise computing experience. Today's remote computing scenarios typically utilize one of two types of access devices—IPsec VPNs or SSL VPNs. While IPsec VPNs have to date been the dominant mechanism for providing remote access, significant shortcomings remain—sufficient security in public networks, reliability, ease of use, and ease of administration among them. Since the IPsec protocol was primarily designed for the protection of point-to-point connections, IPsec VPNs were initially deployed to secure site-to-site links; once configured by network engineers, these site-to-site VPNs rarely needed adjustment. With the growth in remote access IPsec VPNs, users are now frequently forced to tweak network configurations in order to actually perform their jobs; while changing a firewall configuration might be easy for a network engineer, this is not the case for the typical end user. As a result of so many individually uniquely modified devices, users end up with far less protection than administrators intended, placing at risk both end user devices and the enterprise network itself. Additionally, IPsec VPNs offer little or no support for network protocols besides IP (e.g., IPX or NetBIOS), limiting remote connectivity options for enterprises with legacy or customized applications.

Client-side ease of use (or lack thereof) is now driving many organizations to examine SSL VPNs. In theory, SSL VPNs are clientless; in reality, this class of VPN offers either web-based access to web-based applications, or uses downloadable client code (a.k.a. application "connectors") of varying "thickness" to offer access to a wider range of applications. These connectors become particularly bulky in those organizations which wish to provide access to existing enterprise applications, and become particularly costly (with potential development costs well into six figures per connector) if access to customized applications is desired.

VPNs of either flavor suffer from other notable shortcomings. Network and transport layer controls do not provide sufficient protection for network layer information, such as IP addresses, ports, and protocols, leading to vulnerabilities such as ARP cache poisoning and man-in-the-middle attacks, particularly in public locations such as wireless hotspots. VPN clients, personal firewalls, and other client-side solutions are often misconfigured, leading to a lack of sufficient client integrity and to vulnerabilities within the network. Worse, many hotels and other public networks actively encourage users to turn off personal firewalls to enable connectivity on their wired or wireless networks.

Finally, VPN implementations rarely deliver cost benefits; rather, they are viewed as a necessary evil mixing a level of reasonably secure access, a level of reasonable functionality, and an unreasonable level of end-user frustration. Users simply want to be as productive remotely as they are when they're at their desks, and do so with the same level of protection.

To do so, a new model of mobile computing is required, one enabling complete security and functionality. Instead of punching holes in the enterprise perimeter, we must securely extend the perimeter to encompass the mobile user. By treating the remote user as a trusted member of the network, rather than as an untrusted entity, we are able to reduce the mobile threat model to that of the enterprise threat model—providing the same level of protection to remote users as to users sitting at their desks.

2. Remote Connectivity—The Way It Needs To Be

To address this myriad of challenges, Cranite has introduced SafeConnect™. By providing simple, seamless access to all enterprise network applications, by providing device and network security unsurpassed by other remote access products, and by enabling dramatic throughput gains over other types of VPNs, SafeConnect solves the quandary facing both administrators and end users—how to provide users a satisfying enterprise computing experience regardless of location, without compromising connectivity, security, or sanity.

SafeConnect is a robust software solution delivering the ultimate in secure enterprise connectivity by combining Layer 2 security with a unique protective layer designed to abstract users from attack. On shared networks (e.g., hotspots), all users are visible and potentially vulnerable; neither IPsec nor SSL VPNs provide sufficient client-side integrity to ensure protection from attack. By extending the hardened enterprise perimeter and by preventing fingerprinting of remote users, SafeConnect reduces the mobile threat model to that of the enterprise threat model, ensuring that regardless of location, wired, mobile, and remote users receive the same level of protection as if at their desks.

Based on an open architecture, SafeConnect combines existing Internet transport protocols such as IP, UDP, and EtherIP; IEEE MAC protocols such as 802.3, 802.11, and 802.16; and Layer 2 security and integrity to provide an integrated solution enabling assured connectivity, whether in the office or working remotely. SafeConnect provides a tightly integrated framework enabling interoperability with existing identity management, policy, and security applications while providing broad-based support for a wide variety of wired and wireless devices.

Based on products proven in the toughest government networks, SafeConnect provides military-grade security while running on standard, commercially available off-the-shelf (COTS) hardware. As SafeConnect is independent of the type of network technology deployed, the system can support any mix of wired 802.3/Ethernet; 802.11/WiFi access points from any vendor; 802.16/WiMAX customer premises equipment (CPE); and (forthcoming) most wide-area network adapters (e.g., EVDO, HSDPA, GPRS) supporting the Point-to-Point Protocol.

3. Centralized Management, Distributed Enforcement

SafeConnect integrates easily with existing enterprise architecture, including support for LDAP-based directory services, RADIUS-based authentication services, and two-factor authentication solutions based on smart cards, physical tokens, and PKI.

As shown in Figure 1, SafeConnect has three main components:

Cranite Management System—The Cranite Management System (CMS) is an application server providing centralized configuration, monitoring, and management of the secure remote access network via a secure browser interface. The CMS utilizes credentials and group information stored in existing enterprise identity management systems for authentication, authorization, and policy selection.

SafeConnect Access Controller—The SafeConnect Access Controller (SAC) allows administrators to securely integrate remote wired and wireless users into their enterprise architecture. Running on COTS hardware, the SAC provides secure connectivity between remote users and the enterprise network. Acting as the gatekeeper to the enterprise, the SAC enforces all policies created on the CMS and performs all session management tasks required for secure remote access operation, including secure authentication tunneling, data encryption and decryption, and firewall filtering.

SafeConnect Client—The SafeConnect Client is a lightweight client which runs on each SafeConnect-enabled mobile device. The Client communicates with the SafeConnect Access Controller to ensure secure authentication, to encrypt and decrypt wireless traffic, to provide proper and secure routing, and to provide client-side protection from external threats on the shared public network.

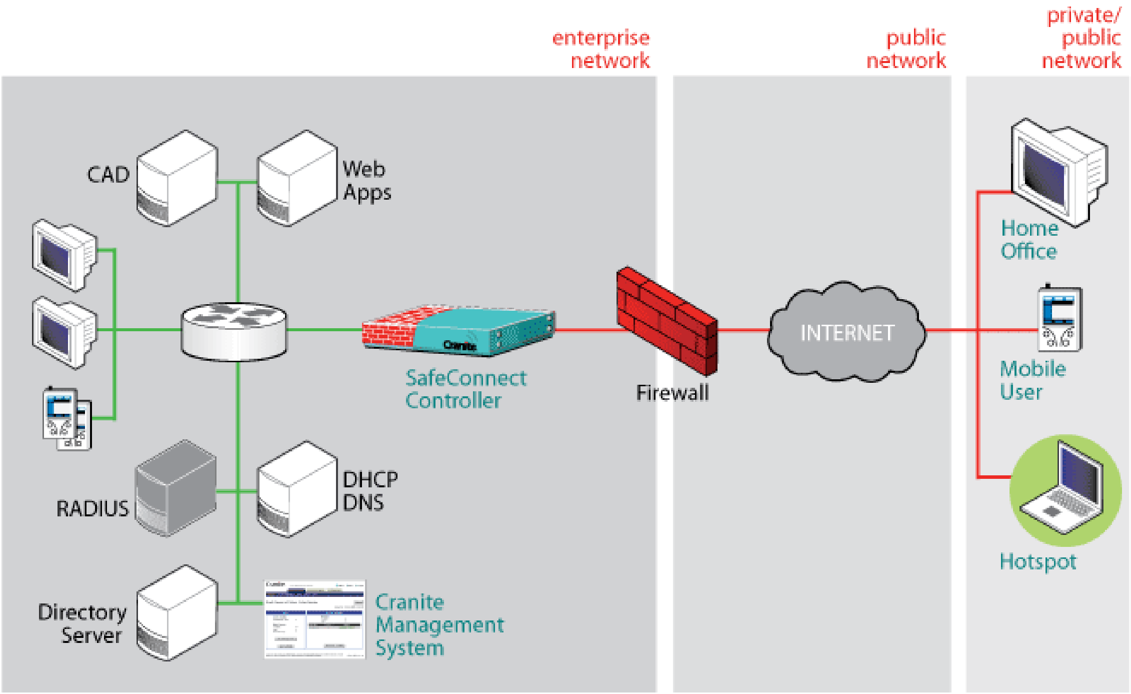

Figure 1

4. A Unique Layer of Protection

In addition to issues mentioned earlier, IPsec VPNs also have one significant additional shortcoming. Whether used in transport mode or in tunnel mode, IPsec clients depend upon the Windows system's routing capabilities, making IPsec routing challenging or impossible to execute securely. As a result, IPsec clients often perform routing incorrectly, leaving devices less protected than believed—devices can still be visible to anyone on the same public LAN, and are therefore still vulnerable to attack. This shortcoming is a fundamental weakness of IPsec implementations, and is exacerbated by the fact that end stations relocate often in a mobile world. Further, route conflicts abound, particularly since private subnet address spaces are so commonly used on public networks

As a result, attackers who gain access to the physical medium (as is typical in any public hotspot) can launch attacks using freely available tools to perform man-in-the-middle attacks, ARP cache and route table poisoning, exploits against the local machine via port and protocol weaknesses, and many more. Even managed personal firewalls cannot prevent this entire class of attacks, particularly when enterprises manage their computers remotely for services such as software updates.

To counter these vulnerabilities, SafeConnect contains a patent-pending abstraction layer designed to protect the local Windows network interface from the publicly visible network interface. As a result, Windows knows nothing about the public network to which it is attached—and attackers cannot exploit the device or the enterprise network to which it is attached. By controlling all routing decisions within the SafeConnect client, users are protected from attack, and also do not encounter NAT traversal issues so common when using public networks.

Attackers who attempt to exploit devices running SafeConnect are unable to fingerprint the device, causing SafeConnect users to appear to be “invisible” on the public shared network, as shown in Figure 2.

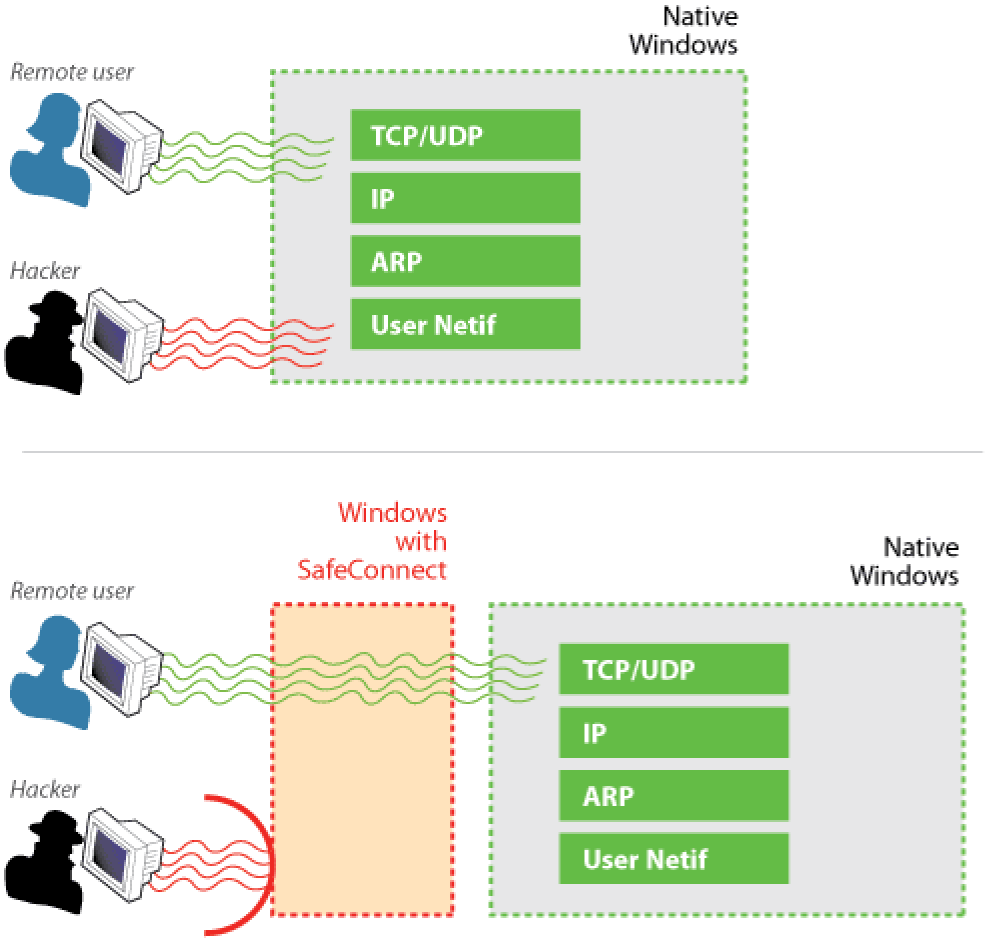

Figure 2

5. Privacy and Integrity

SafeConnect uses the Advanced Encryption Standard (AES) to protect sessions and networks from attack and compromise. AES is a Federal Information Processing Standard (FIPS-197) which specifies a cryptographic algorithm for use by U.S. government organizations to protect sensitive information. AES' combination of security, performance, efficiency, ease of implementation, and flexibility make it an appropriate selection for mobile applications using SafeConnect. Contrast AES with Triple DES, used by many traditional VPNs, which can suffer overhead of 30% or more; further, the processor-intensive nature of Triple DES drains battery life at a much greater rate than does AES.

SafeConnect shares much of its security architecture with Cranite's WirelessWall product, which is designed to provide privacy and integrity inside the enterprise itself. By extending that privacy and integrity to remote locations, users can enjoy the benefits of encrypted wireless or wired communication inside or outside the office.

As does WirelessWall, SafeConnect implements its role-based firewall with robust policy capabilities based on highly granular network traffic filtering. The CMS' simple secure browser-based dashboard enables administrators to define security policies based on each user's existing group/domain associations as defined by the enterprise's directory service. This greatly simplifies ongoing management while lowering total cost of ownership by ensuring that user moves, adds, and changes within the enterprise directory automatically propagate throughout remote access policies.

6. Conclusion

Remote connectivity to enterprise networks has traditionally required a tradeoff between security, compatibility, and ease of use. While IPsec VPNs have attempted to address enterprise remote access, user frustration levels have driven organizations to consider newer technologies such as SSL VPNs. However, SSL VPNs suffer severely from limitations in application compatibility and throughput, in addition to being extremely costly in comparison to other solutions.

Only SafeConnect elegantly combines the best of both worlds, by providing end users the simplicity they expect from SSL VPNs with the application and network access too often missing from IPsec VPNs. By putting remote users on the enterprise network, providing full intranet connectivity while delivering client and network protection not available with any other remote access solution, SafeConnect finally delivers on the promise of true enterprise computing for remote users.

Cranite Systems, Inc., provides secure network access, enabling organizations to safely take advantage of wireless, mobile, and wide–area networking technologies. By encrypting all transmitted information–network addresses, applications and ports–as well as the data itself, Cranite's software provides better security, with greater mobility, while meeting the government's highest security standards. Headquartered in California's Silicon Valley, Cranite was founded in 2000 and is privately held. For more information, e-mail info@cranite.com, call +1 (408) 340–9600, or visit www.cranite.com.