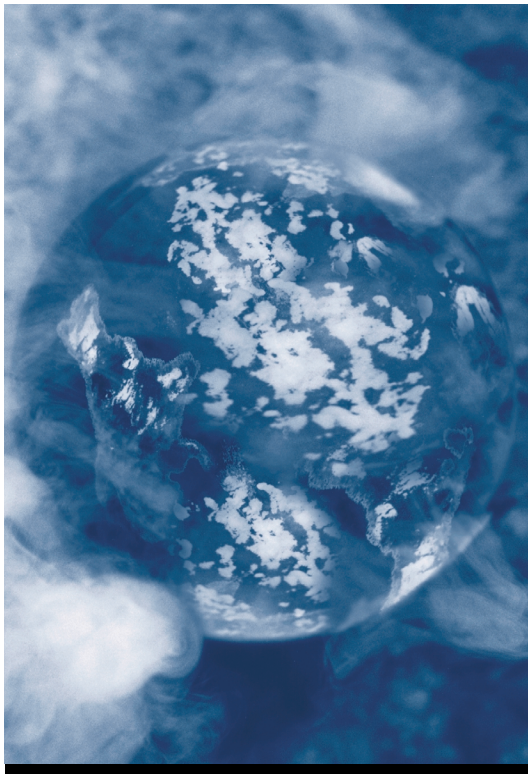
White Paper

IPsec VPNs with Digital Certificates: The Most Secure and Scalable Approach to Implementing VPNs



GTE

INTERNETWORKING

POWERED BY BBN

IPsec VPNs with Digital Certificates: The Most Secure and Scalable Approach to Implementing VPNs

Virtual Private Networks (VPNs) based on the Internet Protocol (IP) combine tunneling, encryption, authentication, and access control technologies to carry traffic securely over many types of shared networks, including the public Internet, privately managed internets, and commercial service provider backbones. The current excitement over VPNs stems from their ability to solve corporate communication problems while also providing significant cost savings. Interesting applications include remote access for road warriors, site-to-site connectivity, intranets, and extranets. Extranets are increasingly being used for intercompany communications that require private networks to be interconnected securely.

Because of these many application opportunities, VPN products and services are rapidly becoming available today. However, there are important differences between the vendors in their approach to protecting users against attacks, such as:

Spoofing — One machine or user on a network masquerades as another

Sniffing — An eavesdropper listens in on a transmission between users

Hijacking — Spoofing and other techniques are used to take control of a communications session, allowing the attacker to masquerade as one of the communicating parties

VPNs that use IPsec technology can counter these attacks effectively. IPsec refers to a suite of protocols that has been specified by the Internet Engineering Task Force (IETF) in order to add security to IP. This integration with an established standard is a key reason why there is industrywide acceptance and support for VPN products and services that use IPsec.

But as with many implementations of standards, not all IPsec VPN products and services provide the same results. This briefing describes why combining IPsec with a certification authority provides the most secure and scalable way to implement VPNs.

What Is IPsec?

The IETF developed the IPsec protocols (RFCs 2401-2412) to provide security services at protocol layer 3, the Network Layer. Because IPsec is integrated with IP, security is provided to any application using IP. IPsec provides three basic capabilities:

Authentication and data integrity — Either the AH (Authentication Header) protocol or the ESP (Encapsulating Security Payload) protocol can be used to provide connectionless integrity and data origin authentication for IP datagrams. These security services enable communicating parties to verify that received data came from the claimed IP source address and that the data was not modified in transit. These protocols also offer an optional anti-replay feature, to help protect against denial of service attacks.

Confidentiality — ESP can be used to provide both data confidentiality (by using encryption) and limited traffic flow confidentiality (if used in tunnel mode). Encrypting data secures it against eavesdropping during transit. Tunneling ensures that the source and destination IP addresses are hidden.

Secure communication establishment between parties — The Internet Key Exchange (IKE) protocol (formerly called ISAKMP/Oakley) enables communicating parties to negotiate their choices of protocols and algorithms to secure their user communication. IKE also distributes the needed encryption keys.

The AH and the ESP protocols are the building blocks of IPsec. They provide the fundamental mechanisms needed to build a VPN that can offer data confidentiality, data integrity, and data origin authentication services. But AH and ESP need supporting infrastructure to distribute the keys that are used for encryption and authentication, and to negotiate protocols between parties. IKE, especially when supported by a certification authority, provides this infrastructure by accomplishing three important tasks:

Negotiation — Establishing the protocols and encryption algorithms to use between parties

Key management — Putting keys in place easily (which might include changing them often)

Security association management — Keeping track of all these security arrangements

Why Choose IPsec Over Other VPN Security Technologies?

According to industry research firm GIGA Information Group, "The IPsec protocol will be most widely used to provide network-level packet encryption and authentication for remote access over the next three years." [1]

Why is there such support and optimism surrounding the adoption and implementation of IPsec VPNs? IPsec's strengths as a core component of a VPN service, as compared to other tunneling and security technologies, lie in three major areas:

Comprehensive security — With mechanisms that are relatively transparent to the user

Interoperability — Using open standards that are tightly integrated with IP

Designed for the future — Permitting modular upgrades as security technology evolves

Comprehensive and Transparent

One of IPsec's obvious strengths is that it integrates encryption and authentication mechanisms with robust and full-featured key exchange and protocol negotiation features to protect against IP security vulnerabilities. IPsec is both a tunneling technology and a security technology. The nature of its design makes the most of that integrated functionality. Using tunneling without encryption offers no protection against many forms of attack. Tunneling for an organization may not just be a matter of protecting external routers from dealing with internal addresses. It may also be a way of hiding those addresses from potentially hostile eyes beyond the firewall. And considering the powerful attacker tools that are available today, security methods that don't authenticate the source and destination of every IP packet may be worse than no authentication at all.

IPsec combines tunneling, authentication, and encryption in a seamless package that gives organizations what they really need — a safe route between private networks, or into a private network from a trusted user, while traveling right through a public network. This approach solves the private address problem and extends the security that users have come to expect for internal traffic to any IP network.

Interoperable, Integrated Standard

Another critical advantage that IPsec has over other methods of tunneling is its relationship to IP. The new IPv6 standard currently replacing IPv4 makes support of IPsec traffic mandatory for all IPv6 equipment. That's in keeping with the philosophy of the design of IPsec, which has been seen from the start as an extension of IP itself. This design philosophy, together with IPv6's requirements for IPsec, lead directly to another, more obvious advantage — interoperability that promises to span all vendors and all platforms, just as IP does today.

Built for the Future

The IPsec protocols are designed to be able to expand to provide support for:

Additional cryptographic methods — New cryptographic algorithms and longer key lengths for existing algorithms. These enhancements are easily adopted because encryption and authentication methods in IPsec are designed to be modular — easily upgraded and easily modified to take advantage of the best methods research can offer in the future

Additional protocols — IPsec is being extended to encapsulate other protocols beyond IP. This will enable organizations to expand the use of their VPN for all traffic, not just IP traffic

So, while there are other tunneling technologies available today, it's reasonable to assume that the most durable solution in the long run is going to be IPsec — the solution built from the beginning with the expectation that it would have to continue to meet the highest levels of security and support the largest of networks in the future.

IPsec provides the core technology for VPNs. However, to ensure scalability as well as the best possible security, your VPN must be integrated with a certification authority (CA).

1 "Internet VPNs: The Value of L2TP Relative to IPSEC, " GIGA Information Group, 1998, Doc No.: 915793-DM98

IPsec VPNs with an Integrated Certification Authority

A CA is an entity that is trusted by certificate users, or has been granted power, to issue digital certificates and vouch for the binding between the data items contained in a certificate. A CA is responsible for managing the life cycle of certificates and, depending on the type of certificate and the certification practice statement that applies, may be responsible for the life cycle of key pairs associated with the certificates.

The certificates can be used to verify the identity of people and organizations with whom you're trying to communicate. There are a number of steps involved in using certificates with IKE to exchange cryptographic keys, but from an end-user's perspective, this all happens in the background.

However, in order for the process to appear seamless to the end-user, either your VPN service provider or your organization must have a certification authority and the expertise to issue and manage digital certificates both to your VPN devices and to end-users.

Certificates solve the scalability problems of user names and passwords, and the problems of manual key distribution methods, making it practical to establish and maintain large VPNs involving many trading partners and millions of users.

Authentication with Digital Certificates versus Shared Secrets

Authentication in IPsec can be provided through use of digital certificates or shared secrets. These two approaches differ in security, in conceptual complexity, in the level of control over communications they allow, and in the amount of additional equipment you will require to use them.

Authentication that depends on shared secrets is practical only in small VPNs and where linking with trading partners' extranets is not an issue. For two nodes to communicate securely through the public network using shared secrets, the devices and client software involved in the exchange must be configured with identical shared secrets. Updating the shared secrets becomes more difficult as the number of nodes (devices and clients) involved increases, because new secrets are typically distributed manually on a pairwise unique basis.

Digital certificates make scaling secure VPNs much easier and, thus, are more practical in larger secure VPNs or in secure VPNs that may grow at unpredictable rates. This scaling is possible because of the implicit workings of a public key infrastructure (PKI). The key advantages are:

User added easily — Adding a new user requires only that the user be granted a digital certificate with the appropriate additions made to the access control database. Then, the user can present the certificate to gain access to a VPN.

Keys managed easily — Key updates can be set up to be entirely automatic. Also, the IT manager can easily remove selected users or groups of users from the system by revoking their certificates, without disturbing the rest of the system.

Digital certificates are also portable and support interoperability across organizations:

Portablility — Users can store their certificates, private key data, and the public key of their CA on a token, carry this token with them, and log on to the network securely from any workstation running the VPN client software.

Interoperability — Cross-certification, in which two CAs issue certificates to one another, is particularly useful for extranets in which a secure VPN is formed among trading partners that each have their own CA. Any node in a combined secure VPN served by cross-certified CAs can then authenticate the identity of any other node. As a result, any two nodes in the system can communicate securely, subject to access control.

What About VPN Advantage and IPsec?

"It [VPN advantage] will achieve savings and also give us the opportunity to outsource our remote access in a way that is secure. GTE Internetworking has the experience to provide that service, and Crown won't have to worry about growing experts in a very complex security technology."

—Miguel Montanez, Group Manager,
Information Services,
Crown Central Petroleum Corporation

VPN Advantage represents the most innovative and comprehensive managed IP-based VPN service offering available :

IPsec with CA support — It is the first service to be based on a complete IPsec implementation, including a managed certification authority as an integral part of the service. This means users do not need to contract with another vendor to either purchase or subscribe to CA services, thus lowering costs.

Proven CA experience — VPN Advantage's CA products are also proven with in-market experience serving tens of millions of digital certificates for clients with the largest customer bases, such as telecommunications firms and financial institutions. This level of scalability is critical for any organization looking to grow their VPN or expand to extranet applications in the future.

Consulting support — VPN Advantage customers can also leverage the SecureNET family of modular and sequential consulting and professional service offerings, which cover all aspects of networking and security requirements for organizations small and large.

Service guarantees — VPN Advantage offers the most comprehensive and aggressive proactive Service Level Guarantees (SLGs) in the industry. These guarantees extend into the customer premises and cover the user experience.

In-house control — VPN Advantage offers customers extensive web-based tools to gather information about their VPN and take control of their implementation while GTE manages the infrastructure beneath it on a 24x7x365 basis. This "shared control" allows customers to get out of the business of running a network infrastructure in-house, while retaining the control over access and security they require as a matter of business.

Extranet control — Finally, GTE Internetworking is the only service provider to support Internet connections from other ISPs with a consistent management and security implementation. This is a requirement for not only extranet applications, where customers cannot control the ISP that their business partners or customers use, but also distributed organizations that may have ISP contracts with multiple providers.

GTE Internetworking Services

Managed Connectivity

Dial-Up Access

Virtual Private Networks

Managed Internet Security

Certificate Management Systems

Web Hosting

Web Applications

Enhanced IP services

Consulting Services

About GTE Internetworking

GTE Internetworking, a unit of GTE Corporation (NYSE:GTE), offers customers, from consumers to Fortune 500 companies, a full spectrum of integrated Internet services using IP networking technologies. GTE Internetworking delivers complete network solutions, including dial-up and dedicated Internet access, high-performance Web hosting, managed Internet security and Virtual Private Networks, enhanced IP services, network management, systems integration, and the enabling technologies for electronic business. GTE Internetworking has secure distributed data centers, a unique load-balancing technology for Web hosting, and seamless dedicated access in more than 65 countries. The company also develops advanced technologies through funded research and development at BBN Technologies.

For More Information:

GTE Internetworking
3 Van de Graaff Drive
P.O. Box 3073
Burlington, MA 01803

Tel: 800.472.4565(toll-free from U.S. or Canada)
or +1 781.262.2905
Fax: +1 781.262.2310
URL: http://www.bbn.com
E-mail: vpn-info@bbn.com

GTE Internetworking International
Centro Direzionale Milano Oltre
Palazzo Tintoretto
Villa Cassanese 224
20090 Segrate (Milano), Italy

Tel: +39-02-2692-6142
Fax: +39-02-2692-2101
URL: http://www.bbn.com
E-mail: vpn-info@bbn.com

GTEI/0091/4.99/WP/VPN/8K

INTERNETWORKING
POWERED BY BBN