intoto

Enabling Security Infrastructure

Virtual Private Network

White Paper

White Paper

Virtual Private Network

Introduction

Businesses today have geographically distributed offices. Employees, working from home and traveling, need to access corporate resources. Businesses need to share the information with partners and customers. All this information shared across offices, with partners and employees needs to be secure and controlled.

Many businesses use dedicated leased lines, frame-relay or ATM circuits to connect to corporate and branch offices. However, these solutions are expensive and don’t scale well with the addition of branch offices. Moreover, service providers in some parts of the world may not provide these services.

Virtual Private Network (VPN) service is scalable and inexpensive solution that provides secure connectivity between corporate and branch offices. In addition, remote access capability of VPNs can be used to provide secure access to corporate resources for mobile employees and tele-commuters.

VPNs use shared infrastructure such as Internet and provides data security to the traffic flowing between the corporate office and branch offices, partners and employees. VPN addresses security issues by peer authentication, access control, per-packet authentication and data integrity, and by encrypting the traffic. IPSEC protocols are defined by IETF and conforming solutions are interoperable.

The VPN solution is scalable. Addition of a branch office, partner, customer or employee to the VPN does not require any additional hardware or software. It merely needs the addition of new policies in the existing IPSEC hardware or software solution.

The VPN solution is flexible. Multiple VPNs can be created. VPN created for intra-office communication is normally different from the extranet VPN created for partners and customers. IPSEC solutions provide flexibility to create multiple virtual private networks, which are independent of each other.

Challenges

Data on the shared infrastructure (Internet) can be subjected to multiple attacks. If the Internet is being used for communication with branch offices and partners, the data must be secured from attacks. The solution should satisfy the following security properties.

Data confidentiality – The perpetrator may observe the data as it traverses the Internet, using commonly available sniffer tools. The data should be encrypted before it is sent out into the Internet. At the other end, the packets should be decrypted and clear data sent to the intended recipient.

Data Integrity – The data in the packet can be manipulated when packets traverse the Internet. In commerce transactions, data such as credit card numbers, deposit, withdrawals, stock-transaction, etc. should not be vulnerable to manipulation in any way. Any modification to the data/packet should be detected and discarded.

Non-Repudiation – In business transactions, it is possible that one of the users later denies sending specific data, part of the data or any other communication. It is therefore essential that user authentication be done before any communication occurs between the parties. The security solution should facilitate mutual authentication using user identities.

Anti Replay – The perpetrator stores the packets being traversed and repeats them. Encryption and authentication mechanisms don't detect this. The security solution should detect replayed packets and discard them.

An IPSEC solution with encryption and authentication algorithms addresses the issues listed above, in securing the traffic and providing security equivalent to dedicated leased lines.

IPSEC explained

IPSEC, defined by IETF, consists of set of open standards to provide security equivalent to a private network in the shared infrastructure, the Internet. Unlike SSL, which is implemented in the application layer, IPSEC provides security at the network layer. It provides security to all the packets of applications belonging to a security policy. There is no requirement to change the applications to support security.

IPSEC makes use of different cryptography technologies to provide confidentiality, integrity and authenticity. Bulk encryption algorithms, such as DES, 3DES and AES, provide data confidentiality. Keyed hashed algorithms, such as HMAC MD5, and HMAC SHA1 provide per-packet authentication and data integrity. Digital certificates, based on RSA and DSA, provide identity verification and access control. The Diffie-Hellman algorithm provides key material for encryption and authentication.

IPSEC mainly consists of two components – IPSEC Packet Processing and Internet Key Exchange (IKE). The IPSEC Packet Processing component secures the packets by encrypting and authenticating them. The Internet Key Exchange component negotiates security proposals between two entities and generates the key material. The IKE component uses digital certificates and pre-shared keys to authenticate the peers, and Diffie-Hellman algorithm to create shared keys.

IPSEC Packet Processing

IPSEC defines Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols, which contain the header format for secured IP packets. The IP packets are secured using encryption/authentication algorithms using the key material. Then, ESP/AH headers are added. On the receiving end, based on ESP/AH headers, the key material and encryption/authentication algorithms are identified, followed by an authentication check and decryption on the packet to get the original clear packet.

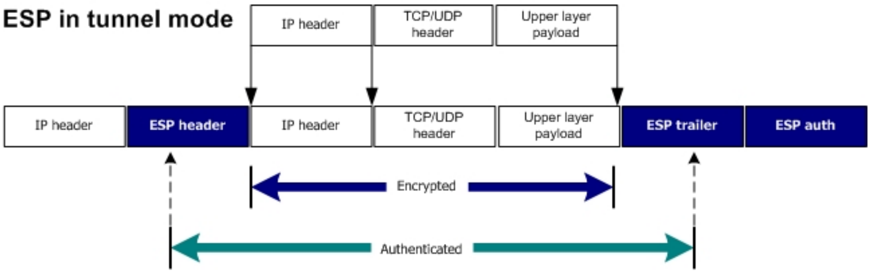
Authentication Header (AH) – This mechanism, when applied to IP packets, ensures the authenticity and integrity of the data, including the invariant fields in the outer IP header. It does not provide data confidentiality. It uses HMAC MD5 and HMAC SHA1 algorithms to create the keyed-hash.

Encapsulating Security Payload (ESP) – This mechanism, when applied to the IP packets, provides the confidentiality, integrity and authenticity of the data. When used to provide the integrity of the data, this mechanism does not include invariant fields of the outer IP header. The ESP mechanism uses DES, 3DES and AES to provide confidentiality, and HMAC-MD5 and HMAC-SHA1 to provide integrity and authenticity of the data.

Tunnel and Transport Modes

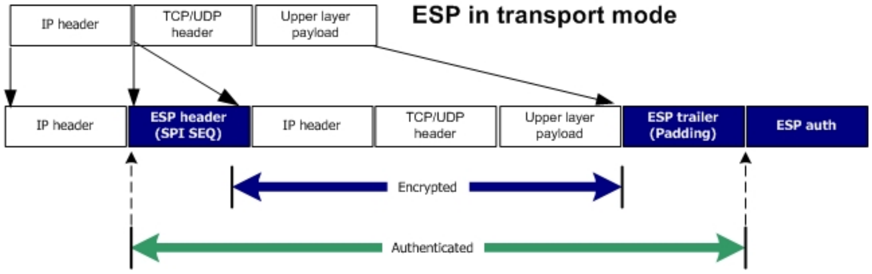
IPSEC provides two modes of operation –tunnel and transport. Tunnel mode is typically used to provide data security between two networks. Transport mode is used to provide data security between two hosts.

In tunnel mode, the entire original IP datagram is secured (with encryption and authentication) and sent by adding security headers and an outer IP header to it. Security gateways, providing data security between networks, typically use this mode. A Security gateway receives the packets from the network, encrypts and sends the packet to the peer security gateway. The Peer security gateway decrypts the packets and sends the clear packets to the network. In this scenario, the end systems on the network don't require any changes. Tunnel mode hides the original IP header, which provides true tunnel. It hides the original IP addresses on the Internet, which facilitates the networks to have a private IP address space.


ESP in tunnel mode

In transport mode, only the IP payload is secured and the original IP header appears on the shared infrastructure. This mode adds only the security headers

(ESP, AH), thereby saving bandwidth. Transport mode is only applicable for host-to-host security. It requires the host to have IPSEC software. Since, the IP addresses of hosts are visible to the shared infrastructure, they must be public IP addresses.



Security Policies and Security Associations

An IPSEC solution can support multiple VPNs. Security properties of VPNs are different and the machines/networks participating in a VPN are different. The VPN configuration consists of machines/networks/applications and the security properties it will use. A VPN is identified by its security policies – outbound and inbound. This is called Security Policy Database.

A Security Association (SA) is established by the Key Exchange Protocol for a given security policy. Security associations consist of proposals chosen, algorithms and corresponding keying material. Each tunnel contains outbound and inbound SAs. A set of SAs corresponding to one security policy is called a Security Bundle. The IPSEC Packet processing component secures the packets using information in security associations of outbound security bundle. Inbound security associations are used to decrypt and authenticate inbound packets.

The following steps provide the sequence of operations performed on outbound and inbound packets.

Outbound processing:

1. Reassembles the packet.
2. Extracts selector information from the IP packet. The selector information includes the Source IP address, Destination IP address, Protocol, Source Port and Destination Port. Note that 'source port' and 'destination port' can be extracted only if the protocol is UDP or TCP.
3. Identifies the Security Policy in SPD.
4. Selects the Security Association Bundle for this packet.
5. If there is no SA Bundle, it initiates the key management module (IKE). IKE, after authenticating with the peer, creates an SA bundle.
6. If an SA Bundle is found, it ensures that the hard life Kbytes has not expired. If found to have expired, the security bundle is deleted.

For each SA in SA Bundle, it does following:

1. Applies crypto algorithm on the complete packet or IP payload, based on the mode of operation (Tunnel or Transport).
2. Encapsulates the packet with ESP/AH header and add trailer, per ESP. It then adds the right sequence number for anti-replay protection.
3. If NAT traversal is negotiated for this SA Bundle, then it adds the NAT traversal UDP header.
4. Adds the outer IP header, for tunnel mode. If AH and ESP are to be applied on the same packet, then headers for both, AH and ESP, are added before the IP header is added.
5. Finally, it sends the packet out, by referring to routing and ARP table (if required).

Inbound Processing

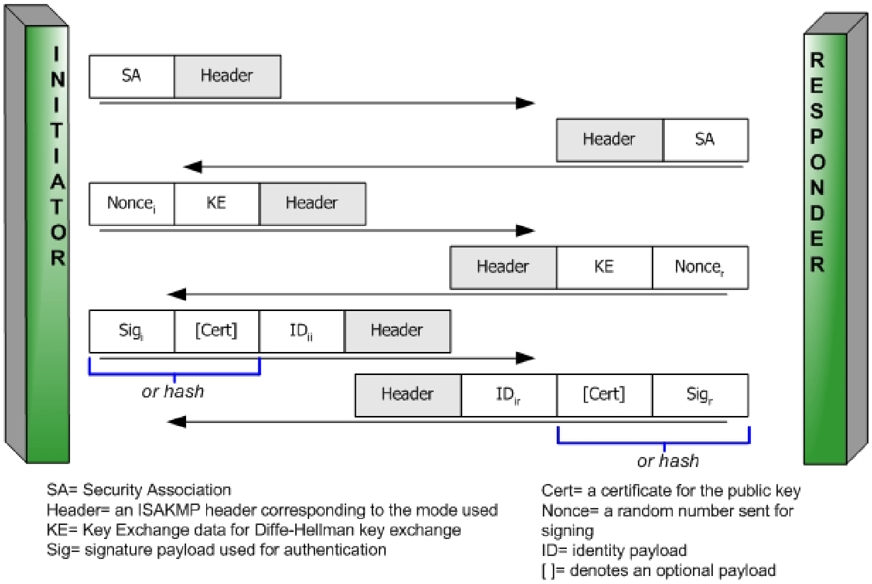
1. Reassembles the packet.
2. Extracts Protocol and destination IP address fields from the IP header. If the Protocol indicates 'AH' or 'ESP', and the destination IP address is one of the self IP addresses, then it extracts the SPI field from the AH or ESP header. For NAT traversal, the NON-IKE header is skipped to get to the AH or ESP header,
3. Finds SA using SPI, destination IP address and Protocol.
4. Based on the mode (tunnel or transport), it applies security algorithms on relevant parts of the packet. Next, it removes the ESP/AH header. Along with this, it also checks for replay attacks.
5. Updates the SA using this sequence number.
6. Checks the 'next protocol' field. If found to be AH or ESP, then it repeats all the steps, beginning with step 2.
7. Repeats this process until the clear packet (i.e., protocol is not AH or ESP or destination IP address is not one of the self IP addresses) is extracted.
8. Extracts the selector information, gets the Inbound Security policy, and checks whether the packet is sent out or given to local applications.

Internet Key Exchange

The IPSEC Packet processing component requires security associations for securing packets. The IKE (Internet Key Exchange) protocol is defined to create security associations. IKE does this in two phases. In the first phase, it authenticates the peer and provides its authentication credentials to the peer. In addition, using Diffie-Hellman algorithm, it generates shared keys. In second phase (phase 2), IKE negotiates the security policy identities, algorithms and other security properties, and generates keying material for bulk encryption and HMAC authentication. This information is passed to the IPSEC packet-processing module as security associations.

IKE defines main mode and aggressive mode for phase 1 exchange. It defines quick mode for phase 2. In the main mode, the user/machine identities are protected. It takes six UDP messages to complete phase 1. In aggressive mode, the user/machine identities are sent in clear and the transaction is completed in three UDP messages.

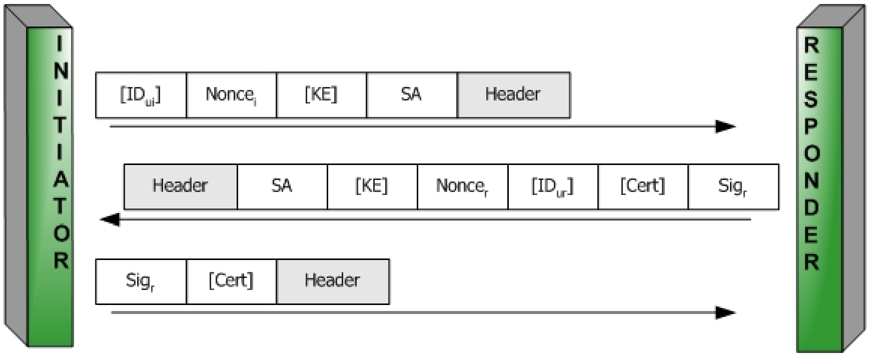
In the main mode, the parties use first two messages to negotiate security properties for phase 1 and phase 2 exchanges. Both parties perform Diffie-Hellman key exchange in the next two messages. In addition, they exchange nonces, which are used later to authenticate peers with their identities. The last two messages are used to send and receive identities and authentication information.



SA= Security Association
Header= an ISAKMP header corresponding to the mode used
KE= Key Exchange data for Diffe-Hellman key exchange
Sig= signature payload used for authentication

Cert= a certificate for the public key
Nonce= a random number sent for signing
ID= identity payload
[ ]= denotes an optional payload

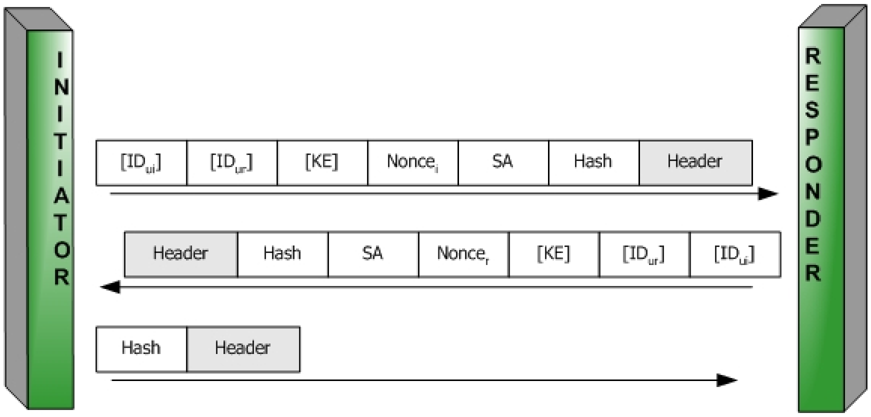
In aggressive mode, the initiator uses the first message to inform other party of security properties, Diffie-Hellman public key component, identity and nonces. The second message is used by the responder to pass selected security properties, its own Diffie-Hellman key information, nonces, its identity and any certificate information. In the third message, the Initiator authenticates itself to its peer.



SA= the negotiated Security Association
Header= an ISAKMP header corresponding to the mode used
KE= Key Exchange data for Diffe-Hellman key exchange
Sig= signature payload used for authentication

Cert= a certificate for the public key
Nonce= a random number sent for signing
ID= identity payload
[ ]= denotes an optional payload

In quick mode, both parties generate keying material to secure the data traffic. Optionally, the Diffie-Hellman operation can be performed, to support Perfect Forward Secrecy for keys.



SA= the negotiated Security Association
Header= an ISAKMP header corresponding to the mode used
KE= Key Exchange data for Diffe-Hellman key exchange
Nonce= a random number sent for signing

ID= identity payload
Hash= the output of a hash function
over specified payload data
[ ]= denotes an optional payload

Steps in IKE as Initiator

The IPSEC Packet-Processing component informs IKE, if it cannot find the security association information for the security policy.

IKE identifies the security profile from the information provided by the IPSEC Packet Processing component, and extracts the peer security gateway IP address. It then initiates the phase 1 exchange.

As part of the phase 1 exchange, peers identify security properties to secure the rest of the exchange in phases 1 2. They generate a shared secret using the Diffie-Hellman algorithm. They mutually authenticate each other using a defined authentication mode.

Once phase 1 is completed, the quick mode negotiation starts with the exchange of security policy information. Optionally, if PFS is enabled, new shared keys are generated using the Diffie-Hellman algorithm. Keying material is produced using nonces and the shared key from phase 1.

At the end of phase 2, security associations (inbound and outbound) are created with keying material, life times, algorithms, etc., and given to the IPSEC Packet Processing component.

Steps in IKE as Responder

The IKE module receives phase 1 messages and completes phase 1 with the exchange of security properties, key exchange payload and identity payload, as part of main and aggressive mode exchanges.

On receiving the phase 2 message, it finds out the validity of the security policy attributes it received, by referring security policy database. If a matching inbound security policy is found, phase 2 continues and results in the creation of security associations (outbound and inbound) with keys, algorithms and lifetimes, etc.

IKE informs the IPSEC packet-processing component of the newly created security associations.

From this point onwards, the IPSEC Packet Processing component honors the inbound packets and decrypts them, validates the authenticity of the packets, and sends clear packets to the internal network.

The iGateway-VPN solution from Intoto

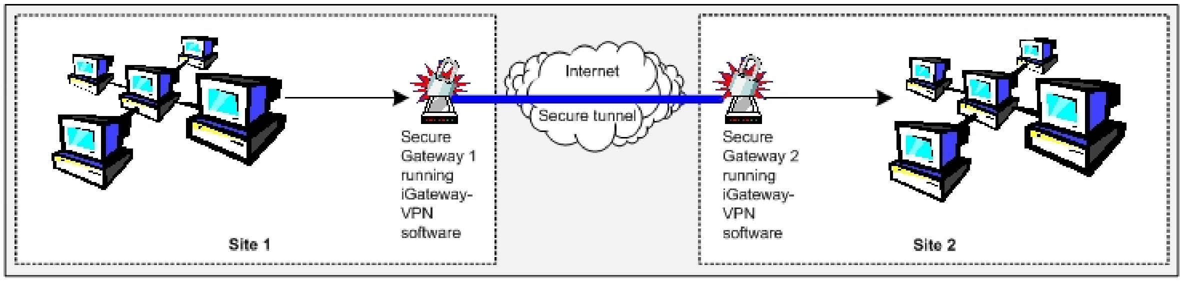
VPNC
CERTIFIED
Basic
Rekeying
Certificates

Intoto's iGateway-VPN is a source code software solution certified by ICSA and VPNC. iGateway-VPN is a complete data security solution with IPSEC Packet Processing and Internet Key Exchange components, and includes PKI support with X.509 certificates, SCEP support for certificate enrollment, and OCSP for certificate validation. In addition, iGateway-VPN solution provides management via CLI and HTTP, and comes with embedded HTTP server and CLI engine. It supports Mod-Config for secure remote access support, and X-AUTH for legacy authentication.

Applications

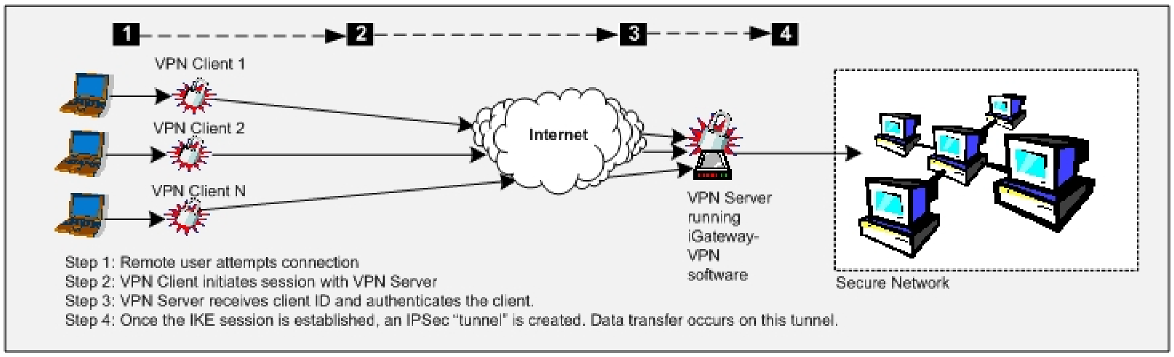
Site-to-Site Security

iGateway-VPN solution, when integrated with a box, can act as security gateway. Security gateways setup private ‘tunnels’ between physically separated sites of an organization, and employ powerful cryptographic algorithms to protect data transferred on the network.


Internet
Secure tunnel
Secure Gateway 1 running iGateway-VPN software
Site 1
Secure Gateway 2 running iGateway-VPN software
Site 2

Remote Access Security

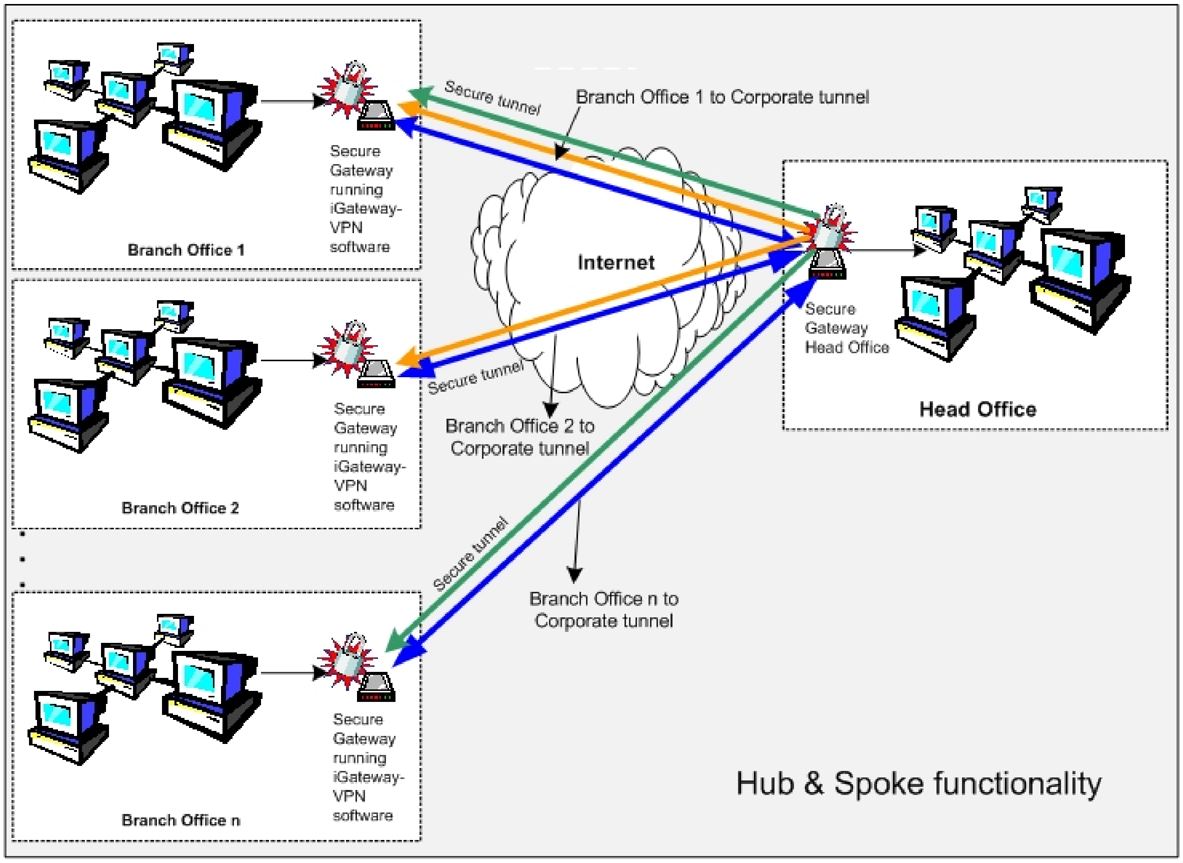
To provide site-to-site security, security gateways require static public IP addresses. Mobile users and tele-commuters don't have static public IP addresses. iGateway-VPN provides a solution for secure remote access to corporate resources. iGateway-VPN can be configured to receive IKE messages, even though the identity can't be determined in the initial states of IKE transactions. In addition, iGateway-VPN, through Mod-Config functionality assigns internal IP address, DNS server IP addresses and WINS IP addresses to the VPN clients running on the mobile users' machines.


1
2
3
4
VPN Client 1
VPN Client 2
VPN Client N
Internet
VPN Server running iGateway-VPN software
Secure Network
Step 1: Remote user attempts connection
Step 2: VPN Client initiates session with VPN Server
Step 3: VPN Server receives client ID and authenticates the client.
Step 4: Once the IKE session is established, an IPSec "tunnel" is created. Data transfer occurs on this tunnel.

iGateway-VPN solution also can be used in branch offices, which have either static public IP address or dynamic public IP address. iGateway-VPN on branch offices will always act in Initiator mode. The following figure illustrates the scenario where branch offices and mobile users communicate with their head office.

Hub and Spoke

Another application of VPN is to share the data securely across offices of businesses. To facilitate secure data transfer, all offices install security gateways. All security gateways will need to be configured with many security policies to communicate with other offices. It requires administration of security gateways in all offices. In addition, it requires all security gateways to be of similar capability. The Hub and Spoke functionality in security gateways reduces the administrator in all branch offices. The security gateways in branch offices will only need to hold one security policy to communicate with the security router in the head office. The security gateway in the head office will need to be more capable , as it will be required to hold the security policies for all branch offices, and relay the traffic across branch offices.


Secure tunnel
Branch Office 1 to Corporate tunnel
Secure Gateway running iGateway-VPN software
Branch Office 1
Internet
Secure Gateway Head Office
Head Office
Secure tunnel
Branch Office 2 to Corporate tunnel
Secure Gateway running iGateway-VPN software
Branch Office 2
Secure tunnel
Branch Office n to Corporate tunnel
Secure Gateway running iGateway-VPN software
Branch Office n
Hub & Spoke functionality

Partners in Progress

Embedded systems on the Internet are the fastest growing class of devices using Internet technologies. Uncompromised security over the Internet is an undeniable need for businesses communicating over networks.

Positioned as the enabler of gateway infrastructure, Intoto Inc. provides complete embedded security software providing for security, connectivity, convergence, and management and network processor solutions. Used extensively in a majority of gateway equipment in conjunction with embedded microprocessors, system-on-chip communications processors, and next-generation network processors, Intoto's iGateway^{TM} software platform integrates security, wired and wireless connectivity, advanced networking protocols, web based management and WAN / LAN interfaces to provide a complete infrastructure for next generation gateway products.

Intoto has successfully established strategic licensing relationships with processor vendors to pre-integrate iGateway on multiple processor such as x86, MIPS or ARM-based SoCs, PowerPC and specialized Network Processors. Its licensing-based business model allows equipment manufacturers to create and rapidly deploy fully validated, reliable gateway equipment. Equipment manufacturers have successfully reduced development costs, and re-used the modular software across multiple products to maximize returns.

In the area of network security, iGateway™ Security Solutions are licensed to a large number of customers including over 15 blue-chip equipment manufacturers and processor vendors. Intoto licensed its embedded iGateway™ solutions to over 100 customers.

For high performance gateways, Intoto's innovative architecture in npFastPath Application Layer APIs, seamlessly integrate with iGateway to provide optimized performance and rapid deployment through separation of data plane software for individual network processors from the control plane.

The iGateway™ Security Solutions have been extensively validated by leading equipment manufacturers and processor vendors. Intoto solutions are certified by ICSA, a leading security assurance organization[1].

Intoto Inc.

3160 de La Cruz Blvd., Suite #100
Santa Clara, CA 95054-0480, USA
Voice: 408.844.0480
Fax: 408.844.0488
www: http://www.intotoinc.com

[1] All trademarks and copyrights referred to are the property of their respective owners.