*Ingate VPN - Whitepaper*

## Summary

Ingate VPN is an extension module to Ingate Firewall, enabling secure connections between geographically separated offices. Ingate VPN consists of software only. Using Ingate VPN you can connect several local networks into a Virtual Private Network (VPN), where information can be transmitted in a secure way, even through insecure networks such as Internet. This provides an internal secure network for your company without having to buy your own external cables.

Ingate VPN is based on IETF standards for the IPSec and IKE protocols. This makes Ingate VPN easy to combine with other clients and firewalls. Ingate VPN works regardless of which operating system is used on the internal network and works transparently for user applications.

Ingate VPN works with other firewalls as well as with single computers. The system requires no user licenses, which means low costs for your company.

Ingate VPN is developed in Sweden by programmers highly skilled in Internet communications.

## What is a VPN?

Data communication through any open network such as Internet is always subject for eavesdropping. By encrypting the information before transmitting it on the insecure network, you can protect it from this attack. This, however, requires that the receiver of the information is able to decrypt the message.

Virtual Private Networks (VPN) enables communication between two separate offices (e. g., offices in different cities) through an encrypted connection without making the users encrypt their data communication. The firewall encrypts the information going into the insecure network and the firewall receiving the information decrypts it and passes it on to the final receiver. You don't have to install complicated encryption software on all your office computers and remind all users to use the software. With VPN, the data communication will look the same from the view of the user. All this makes VPN a cost effective way of providing a private network.

VPN is also useful when wanting to create an encrypted connection between an internal office network and a single computer connected to the insecure network. This case requires the single computer to have VPN client software for creating a VPN encryption tunnel. The connection will be as secure as the regular VPN connection between two firewalls. This means that you won't need modem pools for creating private connections.

A company could create a private network thus: The firewalls of the main office and the local branch office creates a VPN connection. A marketing executive travelling abroad connects her laptop to Internet and creates a secure VPN connection to the firewall.

## Ingate VPN

Ingate VPN consists of software only and is an extension to Ingate Firewall. It can be preinstalled on a new Ingate Firewall or be purchased as an upgrade to an Ingate Firewall already in use. Ingate VPN is configured in the same way as Ingate Firewall, which means that you only need a computer connected to the internal network with a common web browser.

Being based on the IETF standards for the IPSec and IKE protocols, Ingate VPN communicates with other firewalls, VPN clients, and other products supporting IPSec.

Ingate VPN can be used connecting different local networks (branch office VPN) as well as connecting single computers (road warriors) through an encrypted VPN tunnel. To connect single computers, special VPN client software is required. Several parallel VPN connections can be handled.

## Encryption

Encryption of messages is a special distortion used for protecting them from being read by unauthorized people. Encrypting a message involves an ALGORITHM and a KEY. The algorithm tells you how to distort the message. An example of an algorithm is the Caesar Cipher, explained below.

Write down the alphabet in a row. In the next row, write down the alphabet again, but start in a different position. For example, start the second alphabet by writing A right below K in the first row. When you reach the end of the row, go to the left end and write down the letters still left, like this:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
QRSTUVWXYZABCDEFGHIJKLMNOP
Key: 10
```

The key in this cipher is the number of letters you skip before writing A in the second row. You encrypt your message by substituting letters from the top row with the corresponding letters from the bottom row. All "A" letters in the message will be substituted with "Q" letters in the encrypted message.

Even if you know the algorithm, you also need the key in order to decrypt the message. But an intruder, not knowing the key, could manage to extract it by analyzing enough encrypted messages and knowing the algorithm in use. To enhance security of the encryption, the key should be changed regularly.

The encryption algorithm in Ingate VPN is 3DES, which is a block cipher algorithm, meaning that instead of substituting single letters (as in the Caesar Cipher), whole blocks of characters are substituted. This makes eavesdropping and cryptanalyzing harder, even if the intruder can get the encrypted messages.

Ingate VPN automatically regenerates data traffic keys at the interval of your choice. This enables you to adjust the interval to your traffic intensity.

## Authentication

Authentication is the process of assuring that the one who sent a message really is who he claims to be, and of controlling that the information hasn’t been altered during transmission. Authentication also protects from receiving resent packets.

Ingate VPN uses the authentication algorithms MD5 and SHA1, both of which are one way hash functions. Hash functions use the message and a key (a "secret" or a certificate in Ingate VPN) to produce a check sum. The message and the check sum are sent jointly or separately through the insecure network. If the message is changed in any way, the check sum most likely will not be the same. Computing the check sum of the received message also will show if the message was sent by someone else, since they will not have used the expected key. With Ingate VPN you choose your secret or enter your certificate, and share it with the message receiver in a secure way, such as manually entering it on both computers.

## X.509 certificates

### *Why use certificates?*

Certificates is a solution to the problem of distributing public keys in a secure way. Now there are several Certification Authorites (CA:s) signing this information for others, thereby guaranteeing that the information is valid and reliable. When you want to securely exchange data between two computers, you could request a signed certificate with the public key of the other computer. The signature guarantees the validity of the information, provided that you trust the CA who issued the certificate.

The certificate has two parts. A private one, containing the private keys of the computer. The private certificate should under no circumstances be disclosed to anyone. A public part, containing details on the computer including the public part of the key. This is the part being sent to other computers as an identity verification.

### *How does it work?*

These are the necessary steps for the certificate exchange between the CA, the firewall and the client.

#### *Cisco client*

1. The firewall and the CA signs their own certificates. This means that they guarantee their own information. This works if the client trusts the firewall, which shouldn’t be a big issue, as the firewall probably is your own firewall.

2. The public certificate of the CA is exported to the client. This certificate should be used to verify other certificates.

3. The client sends a certificate request to the CA. A certificate request is roughly an unsigned public certificate. The private certificate is also created and stored in a secure way on the client.

4. The CA returns a signed certificate (the public part) to the client. This part should also be forwarded to the firewall, enabling it to verify the identity of the client.

5. The public certificate of the firewall is exported to the client.

Now, the firewall and the client know the public certificates of each others, and are therefore able to verify their identities in future communications.

#### *PGPnet client*

1. The firewall and the CA signs their own certificates. This means that they guarantee their own information. This works if the client trusts the firewall, which shouldn’t be a big issue, as the firewall probably is your own firewall.

2. The public certificate of the CA is exported to the client. This certificate should be used to verify other certificates. The CA also creates the entire certificate, as the PGPnet client is unable to make a certificate request.

3. The CA sends the private certificate to the client. This is the most critical moment, since the transmission must be done securely to make sure that no one else can get the certificate.

4. The CA sends the public part of the signed certificate to the client. This part should also be forwarded to the firewall, enabling it to verify the identity of the client.

5. The public certificate of the firewall is exported to the client.

Now, the firewall and the client know the public certificates of each others, and are therefore able to verify their identities in future communications.

## Technical specification

* Extension to Ingate Firewall
* Software only
* Based on IETF proposed standards for the IPSec and IKE protocols
* Encryption algorithm: 3DES (168 bits)
* Authentication algorithm: HMAC-MD5-128, HMAC-SHA1-160
* Supports preshared keys
* Requires Perfect Forward Secrecy group 2 or 5.
* Supports X.509 certificates
* Supports connections to fixed IP addresses as well as mobile clients
* Automatic regeneration of traffic keys
* No upper limit on VPN connections

## VPN clients

When creating VPN connections from single computers (such as a laptop at home) certain VPN client software is required. Ingate VPN does not contain any such software. Common VPN client software is FreeS/WAN for Unix and SafeNet for Windows.

## Ingate VPN upgrades

For a security product such as Ingate VPN to remain secure and to be able to meet new threats, it must be upgraded regularly. You can find upgrades at http://www.ingate.com/support/ .

## Support

You can choose to get a one year support contract with your Ingate VPN, also including support on your Ingate Firewall. This will give you support from Ingate Systems via email and telephone.