White Paper

Telenor VPN

Table of contents

Abbreviations

API	Application Programmable Interface
GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile communication
GW	Gateway
IKE	Internet Key Exchange
IP	Internet Protocol
NAT	Network Addressing Translation
M2M	Machine to machine
MDA	Mobile Data Access
SMS-C	Short Message Services Center
UMTS	Universal Mobile Telecommunication System
VPN	Virtual Private Network
WAP	Wireless Application Protocol

1 Short introduction

Telenor VPN gives the customer/3rd party secure access to an internal network or dedicated services over an external unsecured network. Virtual Private Network (VPN) technology are used to attend to the security over the external network to make sure that the Customer can communicate with Telenors mobile network in a secure way.

2 Product information

With Telenor VPN, customers get a secure, reliable access to support corporate products from Telenor, see Figure 1.

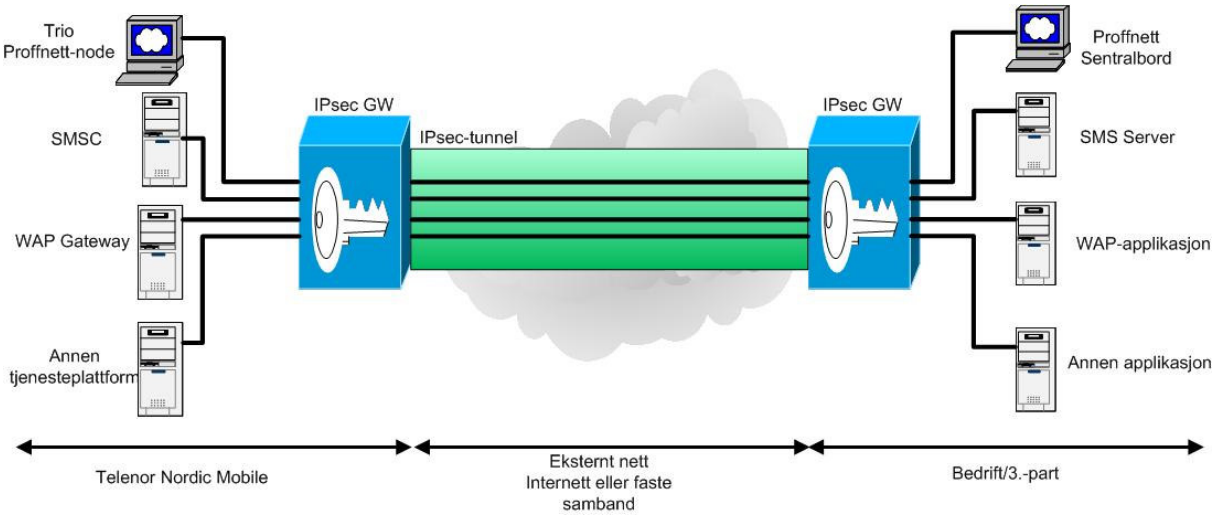

Figure 1 Simplified sketch of Telenor VPN

2.1 *Mobile Data Access*

The product Mobile Data Access gives the mobile users secure access to the companys internal data network and services like e-mail and intranet via the mobile network. The Customer authenticates the employees when they access the Companys LAN.
Mobile Data Access is used as infrastructure for several applications made for specific business sectors, access to e-mail and common files and also for cellular machine-to-machine communication.
It is recommended not to combine MDA traffic with other services in the same VPN tunell.

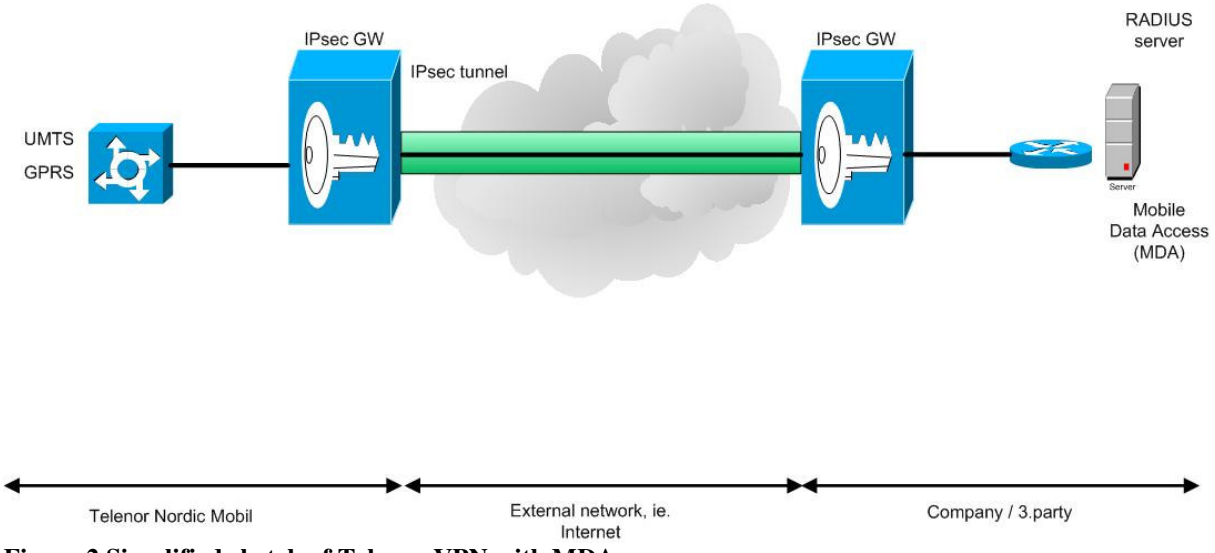

Figure 2 Simplified sketch of Telenor VPN with MDA

2.2 SMS Acess and SMS Bedrift

SMS Access and SMS Bedrift are using Telenor VPN for secure transport of SMS between the SMS service center (SMSC) at Telenor and the SMS server at the customer. The target group for SMS Bedrift are companies with needs in communications in SMS with customers and employees or in m2m-solutions. SMS Bedrift traffic is not permitted for resale. SMS Access are targeted mainly for service providers who will offer value added services based on SMS.

SMS Access and SMS Bedrift are enableing two-way SMS communication between a server at the customers premises and mobile terminals in the Telenor mobile network. Companies are offered a direct connection from their own central server to the Telenor SMSC. The customers are given a five-figure number that can be used for sending and receiving messages.
SMS can be used for sending ordinary messages to and from a mobile terminal, but such a message can also be used to carry different kinds of information, such as readings from a weather station, transport of GPS information etc.

2.3 ProffNett

ProffNett uses Telenor VPN for secure transport of signalling information between the Proffnett server at Telenor and the switchboard server at the customer. Proffnett is a voice service ensuring low cost mobile telephony between the company's employees.

3 Telenor VPN

Hardware
Telenor VPN requires a VPN-enabled router or dedicated VPN hardware on the customer's side. Reuse of existing router at the customer is possible as long the router satisfies the requirements in this document and is powerful enough to handle additional processing. The customer owns and administrates its VPN gateway.

If a Cisco router is used, Telenor can generate a configuration file that the customer can use to configure the router. If other routers or VPN terminating devices are used, the customer itself must configure the equipment. Alternatively, a third party can install, configure and administrate the customer's VPN gateway.

Experiences shows that the Telenor VPN solution may be used with most VPN-enabled routers.
The customer uses the same VPN GW for terminating VPN connections from mostly all existing and future services from Telenor.

Access lists
Telenor 's VPN gateway uses access lists to control which traffic, based on sender address, receiving address or both, that is sent through which VPN tunnel. In this access list it is stated which server(s) in Telenors network the customer can reach trough the VPN tunnel. For each new customer, or if an existing customer shall implement a new service, the access lists must be updated with this information. The access list on the customer's side must match the access list in Telenor VPN gateway to accept the traffic from Telenor and handle it correctly.

Requirements to the customer
Before a customer can connect to Telenor using Telenor VPN, the following requirements must be fulfilled:

The customer's internal network must be protected by a firewall. The firewall must be able to forward IKE- and IPsec traffic between Telenor and the terminating point in the customer's premises on IP layer 3.
VPN gateway feature set supporting IPsec with 3DES must be available at the customer premises.. If the VPN service is to be incorporated into an existing multi-purpose router, the customer must make sure that this router is capable of handling the increased processor load resulting from IPsec encryption/decryption processing.
If a Cisco router is used, Telenor can help configure the router by sending over to the customer a suggested configuration. If a router from another manufacturer is used, the customers must do the configureation

themselves. The router must run an IOS supporting IPsec 3DES. If existing VPN router is used, the customer must ensure that it is powerful enough to handle the extra processing.
The customer VPN router must be assigned a public IP address, making the router accessible from the Internet.
Requirements for placement of the VPN GW:
Preferably the VPN GW should be placed on a dedicated leg on the firewall. The firewall must then be configured to allow IPsec traffic from Telenor 's VPN GW to the customer's VPN GW.
Alternatively, the VPN GW can be placed on the open segment between the firewall and the Internet edge router. In this configuration, the VPN GW must be protected using access lists to prevent unauthorised access.
Requirements for addressing:
The customer is allocated a subnet of private IP-addresses from a predefined IP-range in Telenor. This address space will be dimensioned based on the number of servers in the customer's network that need to communicate through the VPN tunnel.
Each server in the customer's network is assigned an IP-address from the address space mentioned above. This address can be assigned as a secondary address, or the customer can use NAT in the firewall. The advantage by using NAT is that then the address allocation is transparent to the customer's internal network. The VPN GW will be defined as the default Gateway for the network that shall be reached in Telenor 's network.
If all official IP addresses are places outside the firewall, a host route must be made in the Customers router. This in order to route traffic going to the VPN terminating point to the Customers firewall. As a minimum solution the Customer must route a /30 network with official IP addresses through the firewall, and assign an address to the firewalls interface on the inside as a secondary address and the other to the VPN GW.