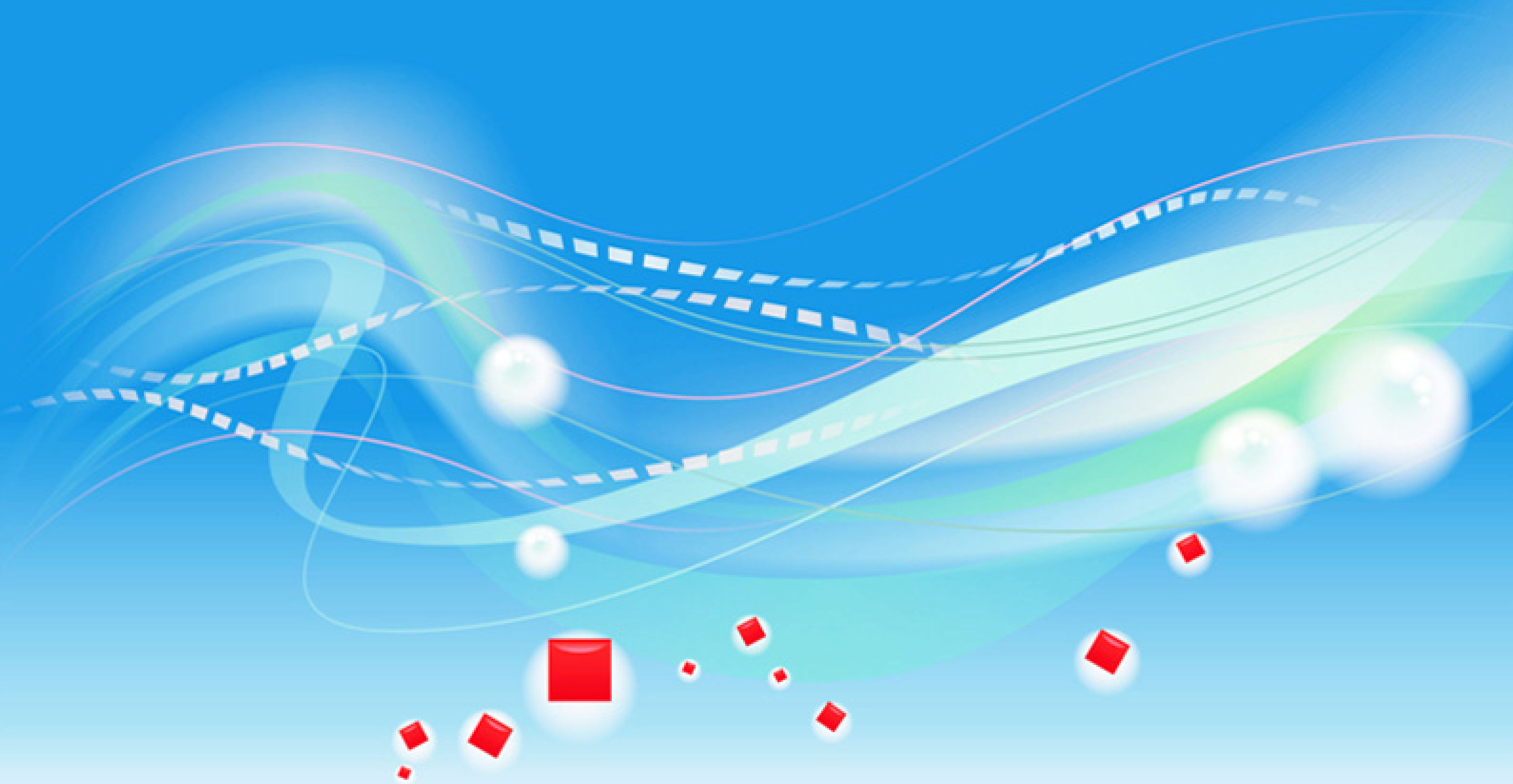

ViPNet Technology

General Information

ViPNet
Virtual Private Network

infotecs

Version: 00121-02 90 05 ENU

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

Email: support@infotecs.biz

Web: http://www.infotecs.biz

Contents

About This Document ... 4

About the ViPNet Technology ... 5

ViPNet Technology Features Overview ... 7

Core of the ViPNet Technology: Kernel-Level ViPNet Driver ... 9

ViPNet Driver in the OSI Model ... 10

Traffic Filtering by the ViPNet Driver ... 12

ViPNet Key System ... 15

Symmetric Keys in ViPNet Software ... 15

Key Generation in ViPNet Network Manager ... 18

Key Distribution in a ViPNet Network ... 19

ViPNet Technology Advantages ... 20

Technical Advantages ... 20

Commercial Benefits ... 25

Glossary ... 26

About This Document

This document contains background information about the ViPNet technology: the basic principles of its use and its key benefits.

Document Conventions

This document concerns the following conventions:

Table 1. Document conventions

Icon	Description
⚠	**Warning:** Indicates an obligatory action or information which may be critical for continuing user operations.
i	**Note:** Indicates a non-obligatory, but desirable action or information which may be helpful for users.
💡	**Tip:** Contains additional information.

Table 2. Conventions for highlighted information

Icon	Description
Name	The name of an interface element. For instance, the name of a window, a box, a button or a key.
Key+Key	Shortcut keys. To use the shortcut keys, press and hold the first key and press other keys.
Menu > **Submenu** > **Command**	A hierarchical sequence of elements. For instance, menu items or sections in the navigation pane.
`Code`	A file name, path, text file (code) fragment or a command executed from the command line.

About the ViPNet Technology

The ViPNet technology is designed for deployment of protected Virtual Private Networks (VPN) over global and local networks. It facilitates the transparent interaction of protected computers, independently from their location, IP address or the way they are connected to a network. The interaction can be established on the basis of client-to-client, client-to-site and site-to-site (VPN tunnel) schemes.

The key difference between the ViPNet technology and most modern VPN systems mainly designed to establish protected connection between local networks and to provide remote access to their resources, is the use of special VPN dynamic traffic routing protocols. These protocols ensure automatic exchange of protected data not only with a VPN gateway installed on the edge of a local network, but also between mobile and remote VPN Clients, also through a VPN gateway when necessary.

An important feature of the ViPNet technology is the usage of symmetric key infrastructure for a VPN, which helps to avoid periodic sessions for network host authentication and key generating procedures. These operations are required in systems with public key distribution, but they affect the use of VPN in local networks and reduce the interference immunity of sessions because a session may be disrupted at the synchronization stage. In the ViPNet network, you don't need to deploy a complicated PKI infrastructure required for using an asymmetric key structure securely. In the ViPNet technology, as opposed to most modern VPN technologies which also allow you to work with symmetric keys, there is an automated system for symmetric key management.

To deploy a protected network, install the following software on computers and mobile devices:

- ViPNet Network Manager, to administer the ViPNet network (create the ViPNet network structure, identify the connection type between hosts and the network, generate and update keys) and establish partner network connection with other ViPNet networks.

- ViPNet Client, to provide network security and to connect computers, mobile devices, and other types of network hosts to a VPN, independently of how they connect to your network infrastructure. ViPNet Client also has an integrated personal firewall with VPN technology. This firewall ensures protection of a host when it establishes connection to another host within its VPN, as well as to an unprotected host. Hereinafter, a computer with ViPNet Client installed is referred to as a “client”.

- ViPNet Coordinator. A host with ViPNet Coordinator installed functions as a VPN gateway to connect unprotected computers and other network devices to a VPN, organizes communication between ViPNet clients and between ViPNet clients and hosts behind the coordinator. ViPNet Coordinator also has an integrated firewall with VPN technology, which provides protection of public network hosts located behind it both within unencrypted connections with external hosts or VPN connections initiated by the coordinator itself. Hereinafter, a computer with ViPNet Coordinator installed is referred to as a “coordinator”. A coordinator is usually installed on the edge of a local network or a local network segment.

A coordinator can perform the following functions:

- **VPN server**, which means that a coordinator provides automatic communication between protected network hosts (clients and other coordinators) located within one or different ViPNet networks. This is possible due to a special VPN traffic dynamic routing protocol which contributes to network convergence. This protocol ensures most optimal VPN traffic routing between hosts in a ViPNet network regarding the connection type selected for the host.
- **VPN packets router**, which means that a coordinator routes forward VPN traffic to other VPN hosts. Routing is performed on the basis of the hosts' identifiers located in the VPN packets' unencrypted part, which is protected only against falsification. Also routing is performed on the basis of the data gathered during the VPN traffic dynamic routing over the protected protocol. At the same time, network address translation of the VPN traffic is performed, and all the VPN packets received by the coordinator are forwarded to other hosts using the coordinator's IP address.
- **VPN gateway**, is a standard feature for classic VPNs. Channels are protected due to encryption of the traffic from unprotected hosts (located behind the coordinator) to other VPN gateways, mobile and remote clients. These protected channels are called tunnels. In ViPNet Coordinator, a VPN gateway is integrated with a firewall for both protected and unprotected connections to hosts tunneled by this coordinator and the coordinator itself. Other VPN firewalls (possibly with an integrated firewall) filter only unencrypted traffic. As opposed to them, ViPNet coordinator filters traffic within the protected connection as well. Traffic filtering during the protected connection with tunneled hosts and the coordinator itself is performed on the basis of the protected hosts' identifiers and IP addresses.
- **Transport server**, which means that a coordinator ensures delivery of control messages and key set updates from ViPNet Network Manager to ViPNet hosts.

  Application and control packets are routed using the ViPNet MFTP transport module (see Transport module (MFTP) on page 28) which operates on the application layer. The transport module (see Transport module (MFTP) on page 28) receives packets from coordinators and other ViPNet hosts and forwards them to the destination host.

  Data routing from one coordinator to another is performed over logical communications channels created between these two coordinators. You can organize logical channels using any scheme. If there are several routes, data is transferred over the shortest one of them. To transfer data from one network to another, gateway coordinators are used in both networks. These coordinators are intended for these two networks to communicate with one another.

- **Firewall**, which means that a coordinator filters unprotected forward and local network connections by IP addresses, protocols, ports, connection directions, and some other parameters, according to set rules. At the same time, the coordinator translates addresses (performs NAT) for unencrypted traffic that passes through this coordinator.

  The function of translating IP addresses for unencrypted traffic allows you to configure rules for both static and dynamic address translation for two main purposes:

  - Connecting a local network to public resources of the Internet when the number of local hosts exceeds the number of public IP addresses issued by the Internet service provider.
  - Accessing the public servers of the local network from the Internet.

  At the same time, this functionality allows you to fulfill the following tasks:

  - Provide remote protected hosts with access to the hosts tunneled by this coordinator using the coordinator's internal address. Thus, configuring of routing within the local network becomes easier.
  - Provide any protected VPN host linked with this coordinator with access to public hosts of the Internet using the coordinator's external address. To do this, you should configure tunneling of several or all the Internet addresses (tunneling of the Internet). This functionality may be extremely useful when organizing centralized secure access of the protected hosts to the Internet, regardless of the hosts' location. Network of the local Internet provider is used as the transport environment for the connection with coordinator which is located in the corporate network and provides access to the Internet for the protected hosts.

Coordinators on Windows and Linux platforms, as well as ViPNet software solutions can be used as a built-in operating system in various network devices, for example, industrial or minicomputers. If you need a failsafe solution based on ViPNet Coordinator for Windows, you can use the ViPNet Cluster software. If you need a failsafe solution for Linux, use the ViPNet Failover system.

ViPNet Technology Features Overview

The core features of the ViPNet technology are as follows:

- **Enhanced information security**

  - Multilevel protection against network attacks both for unprotected and protected connections.
  - Privacy, integrity and availability of networked resources independent of used communications channels.
  - Centralized management of protection solutions.

- **Various network security mechanisms**
  - You can access other ViPNet hosts and their tunneled hosts from a ViPNet host or a tunneled host via unique virtual addresses, automatically assigned on each ViPNet host.
  - Hiding of entire protected network structure and transferred data. ViPNet hosts' internal IP addresses are encapsulated in an encrypted part of a VPN packet together with the body of the original packet.
  - A kernel-level driver protecting applications and the operating system. (see Core of the ViPNet Technology: Kernel-Level ViPNet Driver on page 9)
- **Transparent operation in modern multiservice communication networks**
  - Support of all available communication technologies: xDSL, Ethernet, Wi-Fi, LTE, GPRS/EDGE/3G, and others.
  - Fully compatible with TCP/IP protocols.
  - Transparent operation through NAT/PAT both in client and server modes irrespective of the NAT/PAT type. In this case, protected traffic is encapsulated into the standard UDP protocol. The source port and access address are automatically registered on other hosts or (in order to increase attack resistance) can be strictly locked by forwarding these parameters within protected service traffic over the VPN packets dynamic routing protocol. DHCP, DNS and other services are supported for assigning unique virtual addresses on each ViPNet host.
  - Correct processing of multimedia traffic and IP telephony using various protocols (SIP, SCCP, H323, and others).
- **Unlimited scalability and reliability**
  - Tens of thousands of network hosts in one protected network.
  - The ability to link any ViPNet host in one protected network with any ViPNet host in another protected network (partner network).
  - Configurations of server products with hot failover and clustering.
  - Automatic search of available access addresses for other hosts, support of metrics in case there are several access addresses for coordinators, and support of the dynamic DNS technology if the coordinator has no static address.

  - Automatic restoration of protected connections in case of disconnection (for example, after normal or emergency restart of a ViPNet host), and automatic establishment of protected connection at the operating system startup.

- **Advanced application services**
  - Protected mail client with support for digital signature.
  - Protected chat and conference, file exchange, and hosts availability notification system.
  - Support of standard interfaces for integration into customer's application software.

- **Compliance with TUV Rheinland Group's certification requirements**
  - Regular certification of products for compliance with TUV Rheinland Group's requirements for the means of protecting confidential information, including personal data.

TÜV
TÜV Saarland Standard
Geprüfte Software
Freiwilliges Prüfzeichen

Core of the ViPNet Technology: Kernel-Level ViPNet Driver

The ViPNet driver is the core of the ViPNet software. Its main functions are filtering and encryption of incoming and outgoing IP packets.

ViPNet Driver in the OSI Model

The ViPNet driver works between the data link and network layers of the OSI model, which allows processing IP packets before they reach the TCP/IP stack and, eventually, the application layer. Thus, the ViPNet driver protects IP traffic of all applications not affecting your usual workflow (seamless to applications).

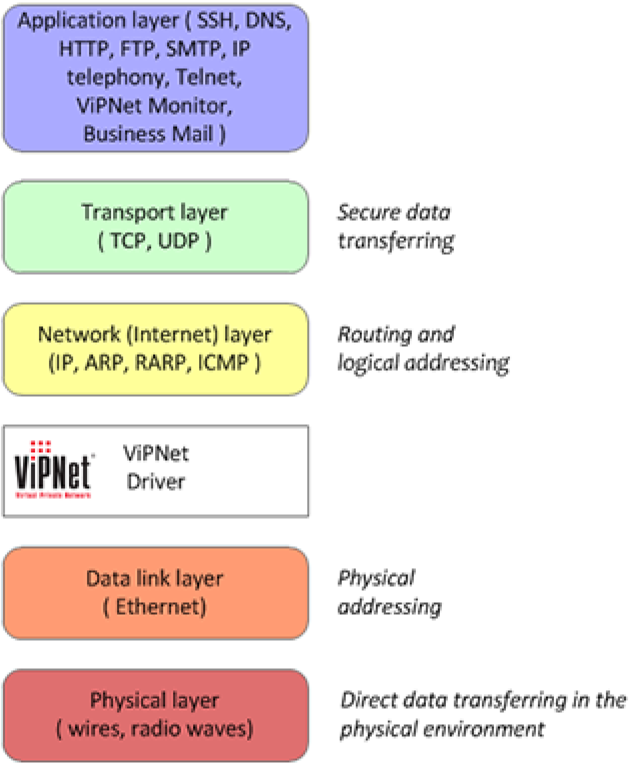
Application layer (SSH, DNS, HTTP, FTP, SMTP, IP telephony, Telnet, ViPNet Monitor, Business Mail)
Transport layer (TCP, UDP)
Secure data transferring
Network (Internet) layer (IP, ARP, RARP, ICMP)
Routing and logical addressing
ViPNet
ViPNet Driver
Data link layer (Ethernet)
Physical addressing
Physical layer (wires, radio waves)
Direct data transferring in the physical environment

Figure 1: The ViPNet driver in the OSI model

Due to this approach, you can seamlessly integrate the ViPNet driver with any application, and adoption of the ViPNet technology does not require any changes in well-established business processes.

Note: For the sake of simplicity, in the figure above:

- The transport and session layers are combined into the transport layer.
- The application and presentation layers are combined into the application layer.

The figure below demonstrates how the ViPNet driver participates in a processing request to view a web page. A web page is located on the IIS server hosted on a computer B (in other words, a company intranet web server).

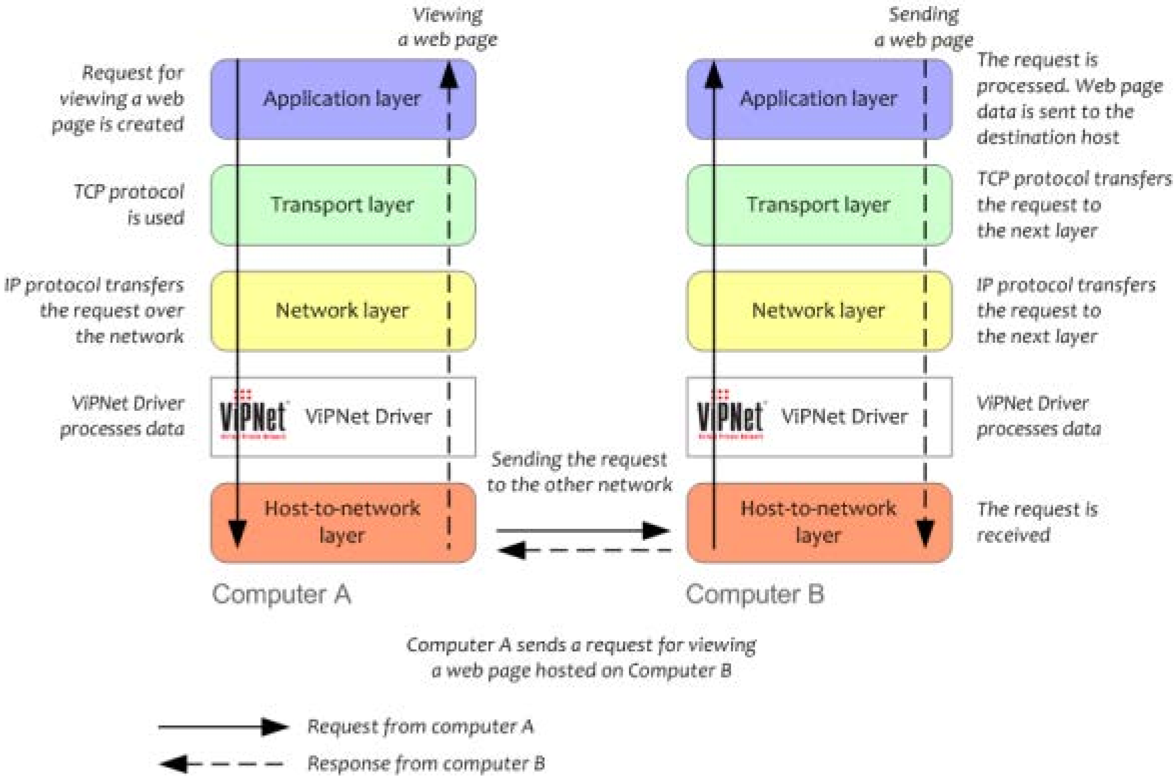
Viewing a web page
Sending a web page
Request for viewing a web page is created
TCP protocol is used
IP protocol transfers the request over the network
ViPNet Driver processes data
Application layer
Transport layer
Network layer
ViPNet Driver
Host-to-network layer
Computer A
Sending the request to the other network
Application layer
Transport layer
Network layer
ViPNet Driver
Host-to-network layer
Computer B
The request is processed. Web page data is sent to the destination host
TCP protocol transfers the request to the next layer
IP protocol transfers the request to the next layer
ViPNet Driver processes data
The request is received
Computer A sends a request for viewing a web page hosted on Computer B
Request from computer A
Response from computer B

Figure 2: TCP/IP network protected with the ViPNet software

Computer A requests computer B to display a web page over the HTTP protocol. This request is transferred to lower layers of the TCP/IP stack, and service information is added to this request on each of the layers. When an IP packet reaches the ViPNet driver on computer A, the ViPNet driver performs the following:

- if necessary, translates a virtual destination address into a real IP address of the destination host,
- adds unique IDs of the source and destination hosts and the sending time to the packet,
- generates the message authentication code (MAC),
- encrypts the original IP packet and part of service information (except for IDs),
- encapsulates the packet into a UDP or IP/241 packet,
- inserts relevant information about the nearest point of access to the destination host (as the access address and port) into this packet.

The ViPNet driver on computer B accepts the IP packet, decrypts it using the destination host's ID, and deletes the ViPNet service information from it; if necessary, it translates the source host's real IP address into the destination host's virtual address. After that, the ViPNet driver transfers the packet via TCP/IP stack to the application layer for processing.

In case there is a coordinator on the route of the IP packet, then the coordinator, without decrypting the packet and based on non-encrypted IDs, substitutes the destination address and port of the VPN packet with the relevant information about the nearest point of access to the destination host. The packet is forwarded on behalf of the IP address of a relevant coordinator interface.

Traffic Filtering by the ViPNet Driver

Each outgoing packet is processed by the ViPNet driver according to one of the following rules:

- If a packet requires no encryption, it is blocked or forwarded to the network according to public network filtering rules. On the coordinator, if NAT settings for unencrypted traffic are enabled, the forward IP packet undergoes the required transformations.
- If a packet requires encryption, it is blocked or undergoes the transformations described in the previous section and is forwarded to the network according to the private network filtering rules.

After processing by a ViPNet driver, the original IP packet addressed to a protected host becomes encrypted. A new IP packet is formed which consists of the encrypted original IP packet, public identifying header and private service headers protected with MAC, and headers of the new IP packet.

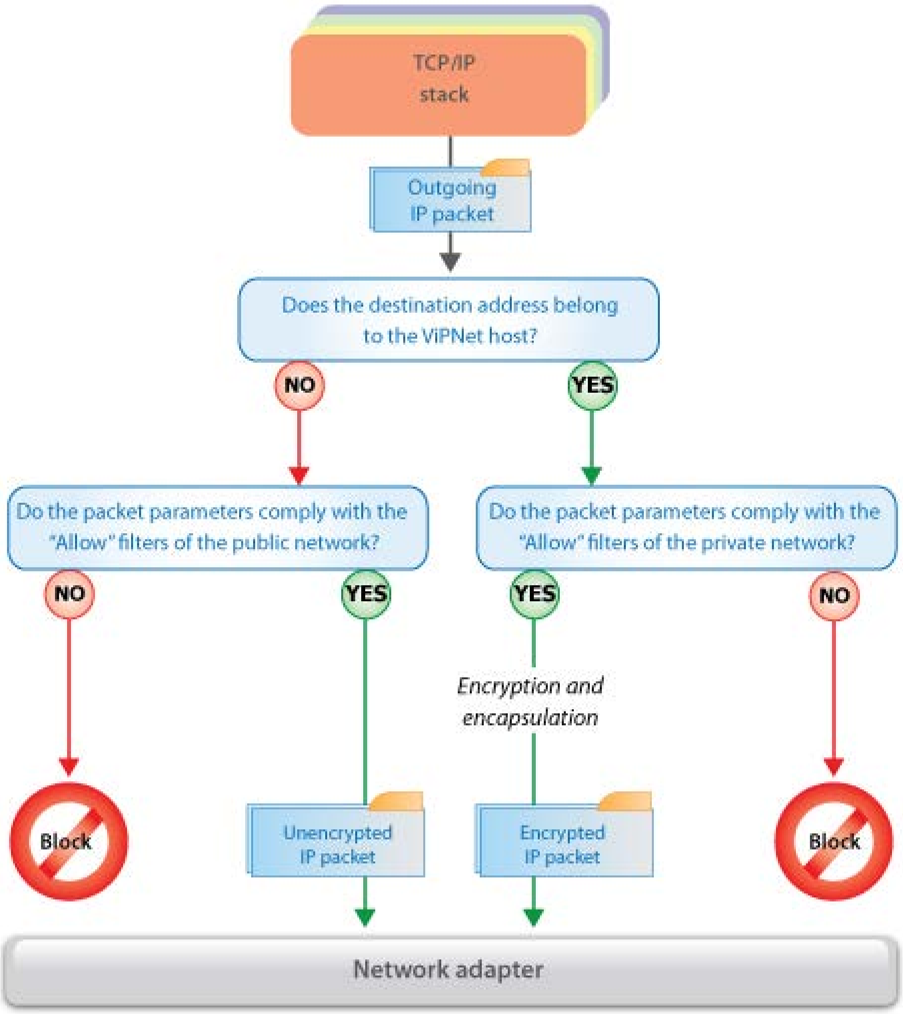
TCP/IP stack
Outgoing IP packet
Does the destination address belong to the ViPNet host?
NO
YES
Do the packet parameters comply with the "Allow" filters of the public network?
Do the packet parameters comply with the "Allow" filters of the private network?
NO
YES
YES
NO
Encryption and encapsulation
Block
Unencrypted IP packet
Encrypted IP packet
Block
Network adapter

Figure 3: Processing of an outgoing packet by the ViPNet driver

Each incoming packet is processed in the following way:

- Unencrypted packets received from unprotected hosts are blocked or passed in accordance with the public network filtering rules. An unencrypted packet received from a protected host is blocked as potentially false.
- Encrypted packets addressed to this host (according to its ID) are decrypted, blocked or translated (according to the private network filtering rules specified above), and forwarded to the TCP/IP stack.
- If an encrypted packet addressed to another host (according to the packet's ID) is received by a coordinator, the packet is not decrypted, and IP addresses and ports of the VPN packet are substituted in accordance with the relevant information about the nearest point of access to the destination host. The packet is forwarded to the network through a

coordinator interface, which is most suitable for packet transmission to the destination host according to the routing tables.

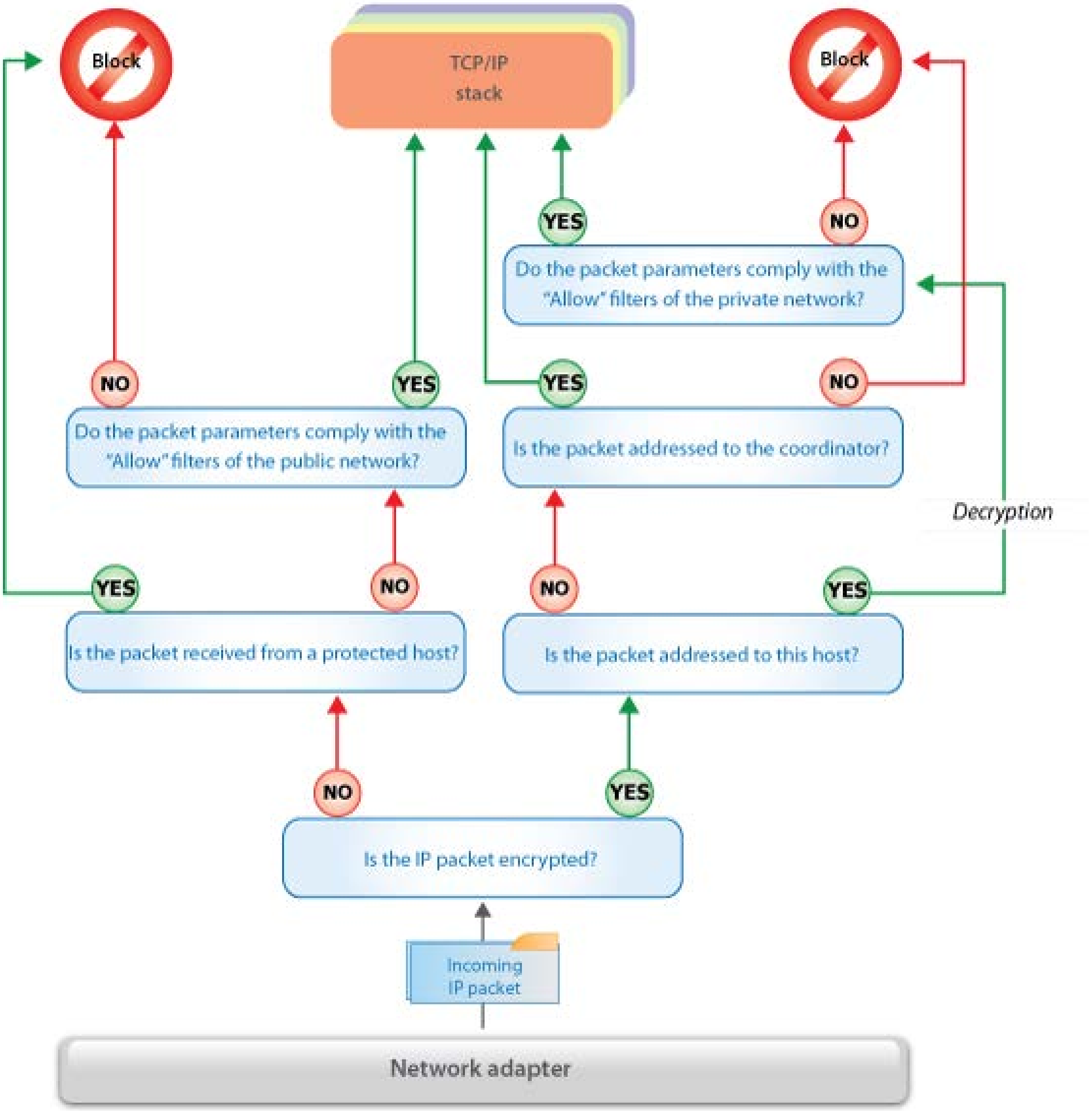
Block
TCP/IP stack
Block
YES
NO
Do the packet parameters comply with the "Allow" filters of the private network?
NO
YES
YES
NO
Do the packet parameters comply with the "Allow" filters of the public network?
Is the packet addressed to the coordinator?
Decryption
YES
NO
NO
YES
Is the packet received from a protected host?
Is the packet addressed to this host?
NO
YES
Is the IP packet encrypted?
Incoming IP packet
Network adapter

Figure 4: Processing of an incoming packet by the ViPNet driver

ViPNet Key System

Protected communication of ViPNet network objects is provided with the help of symmetric keys of different types.

The keys are required for organization of communication between the following objects:

- between a ViPNet host (client or coordinator) and a ViPNet host (client or coordinator);
- between a ViPNet host user and a host with the ViPNet Network Manager software installed;
- between a host with the ViPNet Network Manager software installed and a ViPNet host (client or coordinator).

Keys (see Symmetric key on page 27) for a new ViPNet host are generated centrally in the ViPNet Network Manager program and securely transferred to users or administrators of the corresponding hosts. Keys are updated remotely from the ViPNet Network Manager program through the same protected VPN network channels.

Keys are distributed in the network in the application layer with the help of a special automatic key update system, regardless of the network layer. This provides for reliable operation of the ViPNet network, especially in local networks.

Symmetric Keys in ViPNet Software

Symmetric algorithms are used to encrypt information and control its integrity.

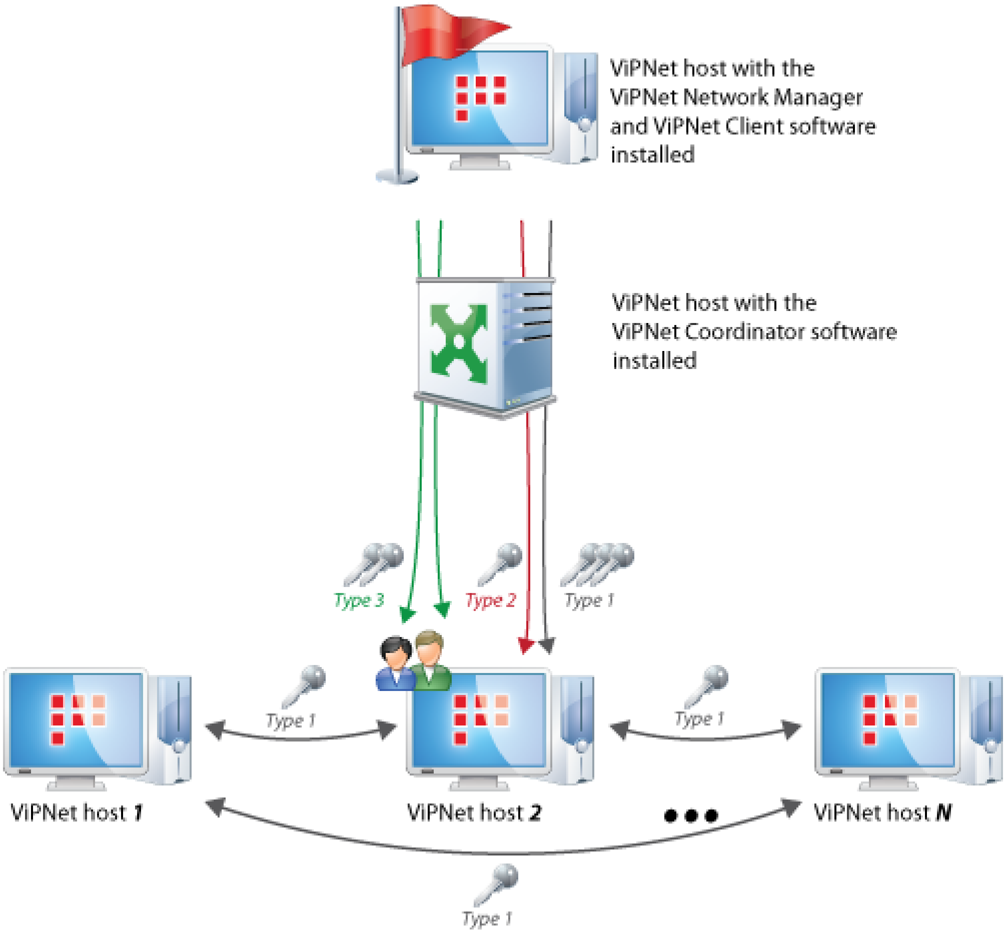
ViPNet host with the ViPNet Network Manager and ViPNet Client software installed
ViPNet host with the ViPNet Coordinator software installed
Type 3
Type 2
Type 1
Type 1
Type 1
ViPNet host 1
ViPNet host 2
ViPNet host N
Type 1

Figure 5: Protection of ViPNet network objects with the help of keys of different types

In the ViPNet software, the following symmetric keys are used (see the figure above):

- Type 1. **Exchange keys** are used for traffic encryption on the network layer between hosts, but not directly. Encryption is performed using the keys derived from exchange keys; these keys are unique for each IP packet. In cases of a scheduled keys' change, hosts' keys compromise, and changes in the network structure, exchange keys are transferred from ViPNet Network Manager to appropriate ViPNet hosts. Being stored on ViPNet hosts, these keys are encrypted using special protection keys (type 2).

- Type 2. **Protection keys of exchange keys** are used for organizing interaction between a ViPNet host with ViPNet Network Manager installed and all other hosts of the ViPNet network on the application layer. These keys are used for encryption of exchange keys (type 1). Being stored on ViPNet hosts, these keys are encrypted using special protection keys (type 3).

- Type 3. Protection keys of type 2 keys, or **personal keys**, are used for organizing access security of several users to various data. These keys are used for encrypting the type 2 keys of each user, as well as other personal information of an individual user. You can store personal keys on an external device as well as on your ViPNet host. When personal keys are being saved, they are encrypted using the user password key.

  A **password key** is a byte sequence received by calculating the user password's hash function value. A password key is used for encrypting personal keys of each user. Password keys can be generated in ViPNet Network Manager, or by a user on a ViPNet host. Password keys are generated as often as required, for temporary usage, and are not stored on devices.

  A **password** is a sequence of alphanumeric symbols from 9 to 32 bytes long. Passwords can be generated in the ViPNet Network Manager program, or by a user on a ViPNet host. If an external device protected with a PIN code is used (in other words, SmartCard), you can use a PIN code instead of a password.

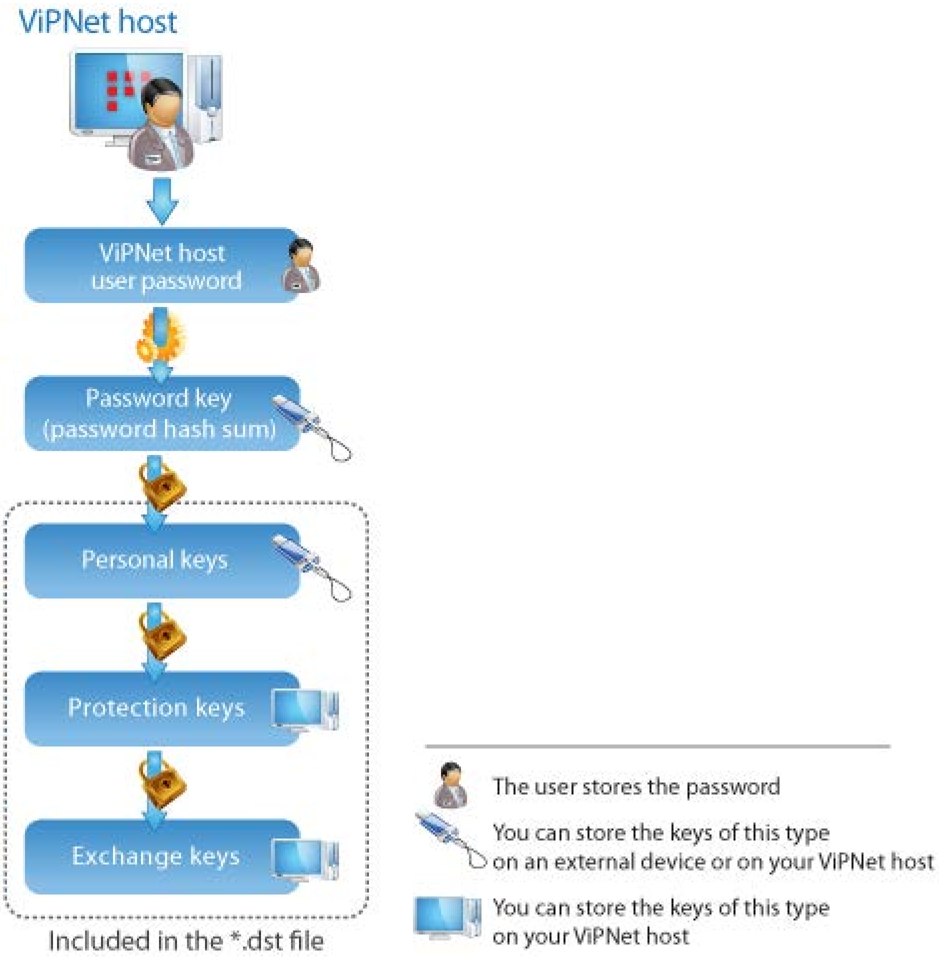
ViPNet host
ViPNet host user password
Password key (password hash sum)
Personal keys
Protection keys
Exchange keys
Included in the *.dst file
The user stores the password
You can store the keys of this type on an external device or on your ViPNet host
You can store the keys of this type on your ViPNet host

Figure 6: Protection scheme for symmetric keys in the ViPNet software

Key Generation in ViPNet Network Manager

All keys of a ViPNet network are generated using master keys of several types.

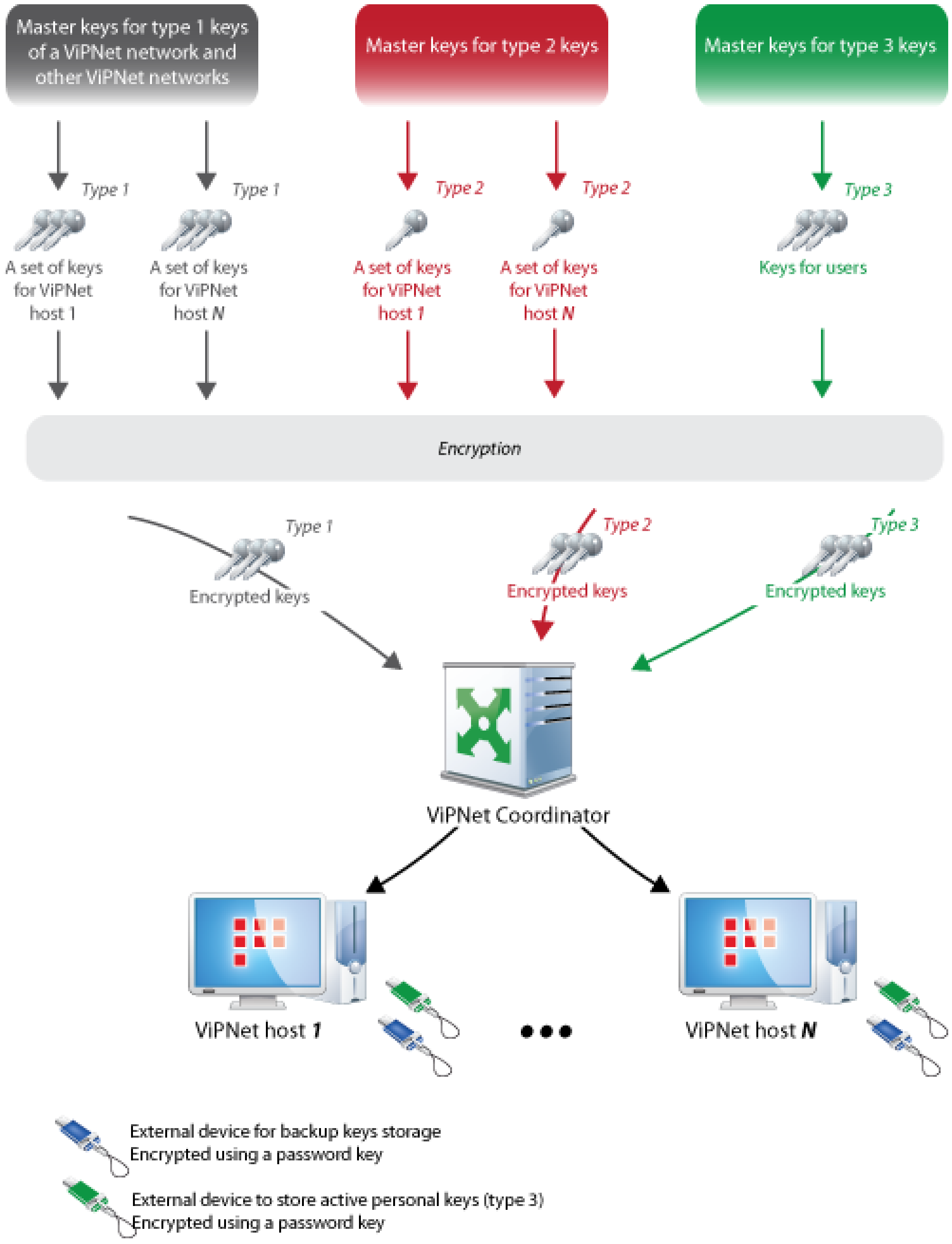
Master keys for type 1 keys of a ViPNet network and other ViPNet networks
Master keys for type 2 keys
Master keys for type 3 keys
Type 1
Type 1
Type 2
Type 2
Type 3
A set of keys for ViPNet host 1
A set of keys for ViPNet host N
A set of keys for ViPNet host 1
A set of keys for ViPNet host N
Keys for users
Encryption
Type 1
Encrypted keys
Type 2
Encrypted keys
Type 3
Encrypted keys
ViPNet Coordinator
ViPNet host 1
ViPNet host N
External device for backup keys storage
Encrypted using a password key
External device to store active personal keys (type 3)
Encrypted using a password key

Figure 7: Generation of keys of different types using master keys

To generate keys for linking with hosts of other ViPNet networks, a cross-network master key is used. A separate cross-network master key is required for every ViPNet network, with which you want to establish partner network connection.

You can generate a cross-network master key using one of the following methods:

- On a random basis, in one of the ViPNet networks. After that, a master key is encrypted using the password key and securely transferred to the other ViPNet network.
- Using the Diffie-Hellman (see Diffie–Hellman protocol on page 26) protocol, by exchange of signed public keys between ViPNet network administrators.

Key Distribution in a ViPNet Network

The above-described multilevel symmetric keys structure allows you to deploy a scalable and reliable system of symmetric keys distribution, as well as an easy-to-manage system, protected with cryptographic methods, for access control to shared information resources and users' information resources.

Symmetric key distribution is fully automated and requires no additional user operations.

A ViPNet host can connect to a VPN under the following conditions:

- The host and its users should be registered in the ViPNet Network Manager program.
- You should set links between this host and other ViPNet hosts.
- For the host, you should create a key set file, containing user keys (a personal key and, when necessary, signature keys), a set of exchange keys for exchange with other ViPNet hosts, host links required for connection with other ViPNet hosts, and a registration file `infotecs.re`. A key set is protected with a personal key, and a personal key is encrypted using a password key.

After you have a key set, you can install a ViPNet program on your computer. After you complete the setup, you can connect the computer to the VPN and interact with other hosts in the same ViPNet network and in other ViPNet networks (partner networks), with which you have established partner network connection in the ViPNet Network Manager program. A ViPNet Network Manager administrator creates links with other ViPNet network hosts by mutual consent with ViPNet Network Manager administrators of those partner networks.

If you need to add new hosts to the existing ViPNet network structure, you should register these hosts in the ViPNet Network Manager program as well. After that, you should create new keys both for the new hosts of your network, and for the hosts of your network which are allowed to communicate with these new hosts. Together with the keys, host links are generated. A key set is securely transferred to the new host. Before you send the keys and host links to an existing ViPNet host, they are encrypted using the exchange keys of the ViPNet Network Manager host and this ViPNet host. After that, the encrypted keys and host links are sent to the host through existing VPN tunnels (either through the ViPNet coordinator or directly, if the required settings have been made). Upon receiving the new keys and host links, the ViPNet host automatically updates its key and host links base. The same procedure is performed when you remove a ViPNet host from the network structure, or in case of changing links with other hosts. When the links are deleted, the unnecessary keys are also deleted from the key base.

If host links with hosts of other ViPNet networks are changed, new host links for these networks are automatically generated. After that, the host links are automatically sent through established VPN connections to ViPNet Network Manager programs of the partner networks.

If a ViPNet host is compromised, you should remove this host in ViPNet Network Manager and create it from scratch. In this case, new keys will be generated for this host. Then, you should securely transfer new key sets to the users of this host and send updated keys to all other ViPNet hosts to be linked with this host. The former keys of the compromised host will be deleted on all ViPNet hosts.

It is critically important to provide synchronous updating of keys. To achieve this, in ViPNet Network Manager, you can set the time for sending updates and control the updates acceptance process on the hosts. This ensures smooth operation of the ViPNet network, even if keys are updated on all network hosts.

ViPNet Technology Advantages

Today, along with the ViPNet technology, there are many other technologies for secure data transfer via a public network. However, there is an entire range of advanced functional solutions which single out the ViPNet technology in a range of classic tools for VPN building, such as IPSec, OpenVPN, PP2P, and others.

Technical Advantages

- **Protection of traffic within a local network**

Classic VPN solutions. From the outset VPN technologies were designed to provide secure data transfer over the Internet: it was assumed that there was no risk of intercepting confidential information within a local network. Such an approach remains unchanged in most modern VPN technologies. These technologies provide secure connections of local networks and remote access to local networks, but they don't solve the task of creating an isolated environment in a heterogeneous network infrastructure and providing protected information exchange between its end users.

Since a local network is deemed to be trusted, traffic from a VPN gateway (a device that is an access point to a VPN network) to the end host of a local network is not encrypted. Thus, confidentiality of the information transferred through a local network after its decryption on the VPN gateway can't be guaranteed. All information on the gateway is decrypted and potentially available for interception in a local network.

ViPNet. A VPN gateway (coordinator) also functions as a VPN traffic router. A VPN gateway routes confidential information to other VPN network hosts without decrypting it. Thus, the information is protected from interception (by anybody, including the administrator) on the coordinator as well as in the segments of the local network this IP packet passes through.

At the same time, you can transfer the information through several coordinators (the so-called "cascade connection of coordinators"). In this way, the information can be forwarded over a particular route or to other additionally protected segments of a local or corporate network. Coordinators route VPN traffic in accordance with information about points of access to VPN hosts. Such protected service information is transferred over the VPN packets dynamic routing protocol. This excludes unauthorized changing of the routing paths.

The ViPNet technology combines the functionality of traditional VPNs and features of dynamic VPN traffic routing by means of a special protocol. Thus, this technology enables you to build securely protected network structures in complex distributed systems and organize protected interaction of any kind easily, including interaction of multiple organizations.

- **Flexibility and the ability to build a wide range of schemes**

  Classic VPN solutions. Allow you to organize schemes of secure exchange of confidential information, mainly of the "client-to-site" and "site-to-site" types. A client, when establishing connection with another client, first connects to a server to undergo the initial authentication procedure. Using other schemes and implementing a wide range of scenarios are hindered due to the lack ability to route VPN traffic without its decryption on the edge of the local network (on a VPN gateway). You can use "client-to-client" schemes, but generally these are flat schemes in routable networks for protecting access to particular servers.

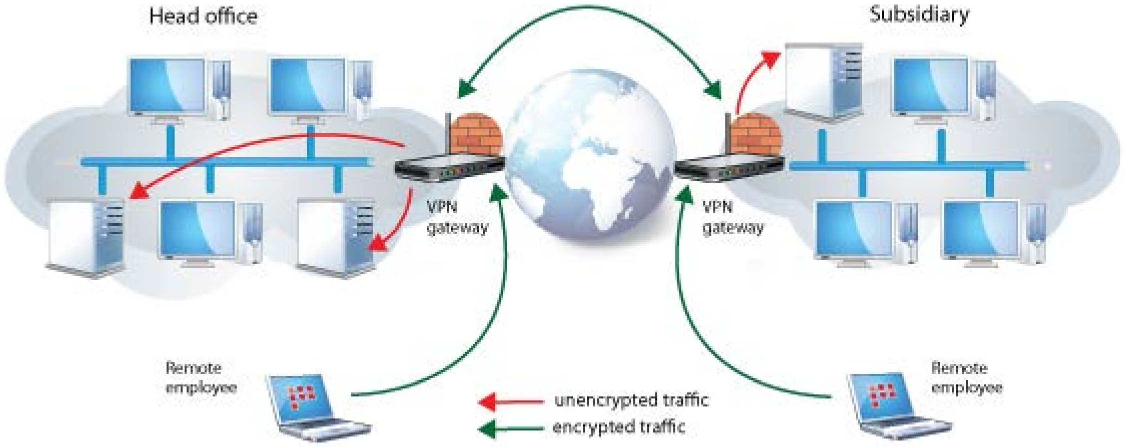

Figure 8: A VPN network scheme based on IPsec technology

ViPNet. The dynamic IP traffic routing technology ensures easy implementation not only of the client-to-site and site-to-site schemes, but also of the client-to-client scheme and of schemes for direct traffic transfer or transfer through coordinators without decrypting. Thus, you can implement any required access control policies within the entire protected network and reduce the load on VPN servers.

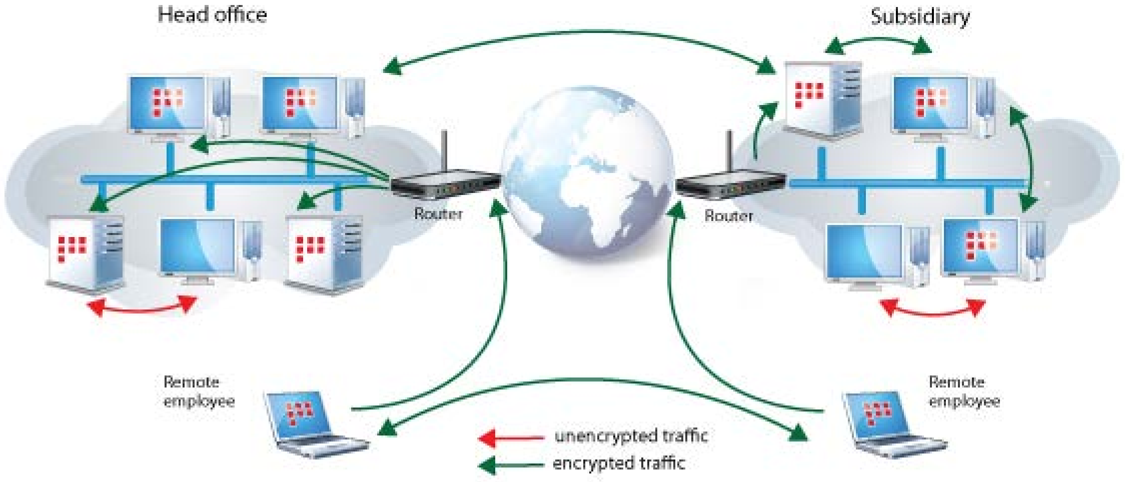

Figure 9: A VPN network based on the ViPNet technology

- **Solution for a problem of IP addresses ranges' intersection**

  Classic VPN solutions. If integration of several local networks is required, this may entail the intersection of IP address ranges (for example, during interaction with a partner network which has the same private IP addresses). This problem may also arise when connecting a remote user. The OpenVPN technology solves this problem for remote users by creating a virtual adapter on the remote computer; the adapter receives an IP address from a VPN gateway. However, such a solution has the following disadvantages:

- A conflict of IP addresses may occur in the provider's network, to which a remote user is trying to connect.
- It is difficult to organize interaction with networks located behind other VPN gateways.
- Traffic encryption is controlled by routing the traffic to the virtual adapter. However, the routing table may be easily changed on a local host by some means or other, and encryption of the traffic forwarded to a tunnel may be cancelled.

ViPNet. A conflict of IP addresses is eliminated by means of the virtual IP addresses technology. All remote hosts receive virtual IP addresses on each ViPNet host regardless of their real IP addresses. Other ViPNet hosts are accessible from this host by unique virtual IP addresses which are generated automatically. If the remote ViPNet host is a coordinator, it will be accessible from any unprotected host tunneled by it, due to the virtual IP addresses technology, and this tunneled host will have access to other tunneled and protected hosts.

Applications are notified about virtual IP addresses of remote hosts by means of special names resolution traffic processing for all main protocols and services: DNS, NetBios, WINS, multimedia services, such as SIP, SCCP, H323, H225, H245, and others. When the applications communicate with remote hosts, IP addresses in original IP packets are substituted when necessary (from real to virtual and vice versa).

Besides solving the problem of IP address ranges intersection, virtual IP addresses usage also prevents potential IP address spoofing. When the ViPNet driver receives a packet, it substitutes the real source address with a respective virtual address, and then forwards it to an application. It occurs only in case of successful decryption of the packet using the sender's keys, in other words, after identification of the sender. This ensures protection from substitution of the source address and makes it possible to control access to the hosts, based on the virtual addresses assigned to protected ViPNet hosts.

- **Working with public Internet resources**

  Classic VPN solutions. On remote hosts, work with a VPN channel is usually organized through virtual adapters specially created on a computer; these adapters receive IP addresses from a VPN gateway over the DHCP protocol. Interaction of a remote computer with public Internet resources via a corporate office firewall can be provided by redirecting all traffic through a VPN tunnel to the VPN gateway of this office. This allows processing the unencrypted traffic in accordance with corporate requirements. However, to use this functionality, you need to edit the routing table of the operating system (notably, to specify a virtual IP address as the default gateway, which is generally done by means of the DHCP protocol). The scheme may appear to be unprotected: a malicious user can edit the routing table on a local host by some means or other and redirect the Internet traffic through a local provider. Moreover, as described above, this may lead to cancellation of encryption of the private traffic intended for tunneling.

ViPNet. The technology is based on IP traffic interception without creating virtual adapters and the necessity to use the operating systems routing table. The ViPNet driver provides traffic encryption in accordance with registered addresses of protected hosts. In order to provide access to public resources via a corporate firewall, the driver blocks any traffic, except for the DHCP traffic with your provider, and redirects the Internet traffic to the tunnel with a VPN gateway.

- **Reliable operation when changing connection types frequently or when accessing another VPN gateway (when using mobile devices)**

  Classic VPN solutions. A frequent change of base stations (for example, in case of 3G connections) can cause unstable operation. In case of disconnection, re-authentication is required, and, if you need to access another VPN gateway, you should change the configuration parameters. Thus, uninterruptable operation of the VPN network is not guaranteed.

  ViPNet. In case of disconnection, a connection is re-established automatically without prompting you to re-enter your user credentials. If you want to access other networks, you don't need to change the configuration parameters. The VPN packets dynamic routing protocol provides automatic routing of VPN packets to a relevant coordinator.

- **Key structure**

  Classic VPN solutions. When organizing remote access in the “client-to-site” scheme, it is possible to use symmetric keys only on some single keys. In the “site-to-site” scheme, it is possible to generate different symmetric keys for each pair of ViPNet hosts; however, there are no mechanisms for keys distribution or control over the symmetric keys structure. Therefore, in large distributed protected networks the use of symmetric keys becomes insecure and extremely inconvenient.

  ViPNet. A personal unique automated system of managing the symmetric key structure is more secure and reliable than the unprotected keys distribution infrastructure.

- **Filtering of protected IP traffic independently from the source IP address**

  Classic VPN solutions. Traffic is filtered by source IP addresses, because traffic filtering is generally performed on a firewall which is independent of the VPN technology, and, after decrypting the IP packets, all information about these packets, except for their source IP addresses, is lost. However, an IP address is not protected against potential spoofing by an internal malicious user in any way.

  ViPNet. The firewall is integrated with the VPN technology. The protected traffic is filtered before decryption of the packet on the basis of the source host ID. That is why filtering rules are set for a ViPNet host, and not for its IP addresses which are of no importance. This prevents any attempts of internal malicious users to substitute the source IP address in order to bypass private network filters.

Commercial Benefits

- Compared with classic VPN solutions, the ViPNet software provides an entire range of advanced secure data exchange features: integrated services for instant exchange of messages (chat and conference) and files, as well as a protected mail service with the function of automated mails and files exchange and digital signature support.

- Advanced network features of the ViPNet software, such as control of applications network activity, strict Internet access control and mechanisms of emergency restart (panic button) allow you to organize protection from most network attacks and minimize total expenses on the security system.

- ViPNet software solutions are self-sufficient, so you don't need to purchase any additional software components, such as DBMS or specialized server platforms. ViPNet products entail no hidden expenses — you pay only for the components you need.

- Since ViPNet products can be delivered in the form of software solutions, their installation and configuration require no specialized equipment and can be performed on your existing computer base. In most cases, re-configuration of network equipment is also not required.

- Flexible pricing and an opportunity to purchase additional licenses for ViPNet components when necessary allow us to create the best pricing solution for each particular customer. You pay only for the components you need at the moment; you can buy other components later when you need them.

Glossary

C

Client (ViPNet client)

A ViPNet host that is the start and the end point of data transfer. Opposite to a coordinator, a client does not route VPN traffic and service data.

See also: Coordinator (ViPNet coordinator) (on page 26), Routing, ViPNet host.

Coordinator (ViPNet coordinator)

A network node with installed ViPNet Coordinator or ViPNet Secure Gateway software. A ViPNet coordinator functions as a server in a ViPNet network and routes VPN traffic and service data.

See also: Routing, ViPNet network (on page 28).

D

Diffie–Hellman protocol

A public key distribution protocol, used by two parties to agree on a shared secret by dynamic interaction based on exchanging unencrypted messages that don't contain any pre-distributed shared secret.

Digital signature

An attribute of an electronic document intended to protect the document authenticity. It is generated when encrypting information using a private key of a digital signature. A digital signature identifies the public key certificate owner, as well as proves non-repudiation of the document contents.

See also: Private key, Public key certificate (on page 27).

E

Exchange key

A symmetric key known both by the sender and by the recipient of encrypted information.

See also: Symmetric key (on page 27).

K

Key compromise

Loss of confidence that the current valid keys provide security of information (its integrity, confidentiality, source authentication, non-repudiation).

If the keys are compromised, the ViPNet network administrator should generate user and host keys and send updates to ViPNet hosts. Both shared and personal keys, as well as exchange keys, will be changed, so the administrator should send host keys to all the ViPNet hosts linked with this ViPNet host.

See also: Exchange key (on page 26), User keys, ViPNet host, ViPNet host keys.

Key container

A file where a private key and the corresponding public key certificate are stored.

See also: Public key certificate (on page 27).

P

Public key certificate

An electronic document of a previously specified format that uses a digital signature to bind a public key with an identity, information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. A certificate contains information about the key owner, the public key, about its purpose and usage, about the certification authority that has issued the certificate, the certificate validity period, and some other parameters. In a ViPNet network, certificates are issued in ViPNet Key and Certification Authority or in ViPNet Network Manager and verified with the digital signature of the ViPNet Key and Certification Authority administrator or ViPNet Network Manager administrator. This provides authenticity and integrity of the information specified in the certificate, including its public key and description of its subject.

See also: Digital signature (on page 26), Public key, ViPNet Key and Certification Authority, ViPNet Key and Certification Authority administrator.

S

Symmetric key

A bits sequence of a defined length used both to encrypt and decrypt information.

In ViPNet software, symmetric keys are used to encrypt and decrypt IP traffic, applications' data (including mail data), services and applications packets.

See also: Application packet, Service packet.

T

Transport module (MFTP)

A program intended to transfer data in a ViPNet network.

V

ViPNet network

A virtual network that is created and maintained with ViPNet software and consists of ViPNet hosts. Each ViPNet network has its own unique number (an identifier).

See also: ViPNet host.

ViPNet Network Manager

A program that is a part of the ViPNet VPN software suite. It is intended to create, configure, and administer small and middle-sized ViPNet networks. ViPNet Network Manager also functions as certification and key authorities.