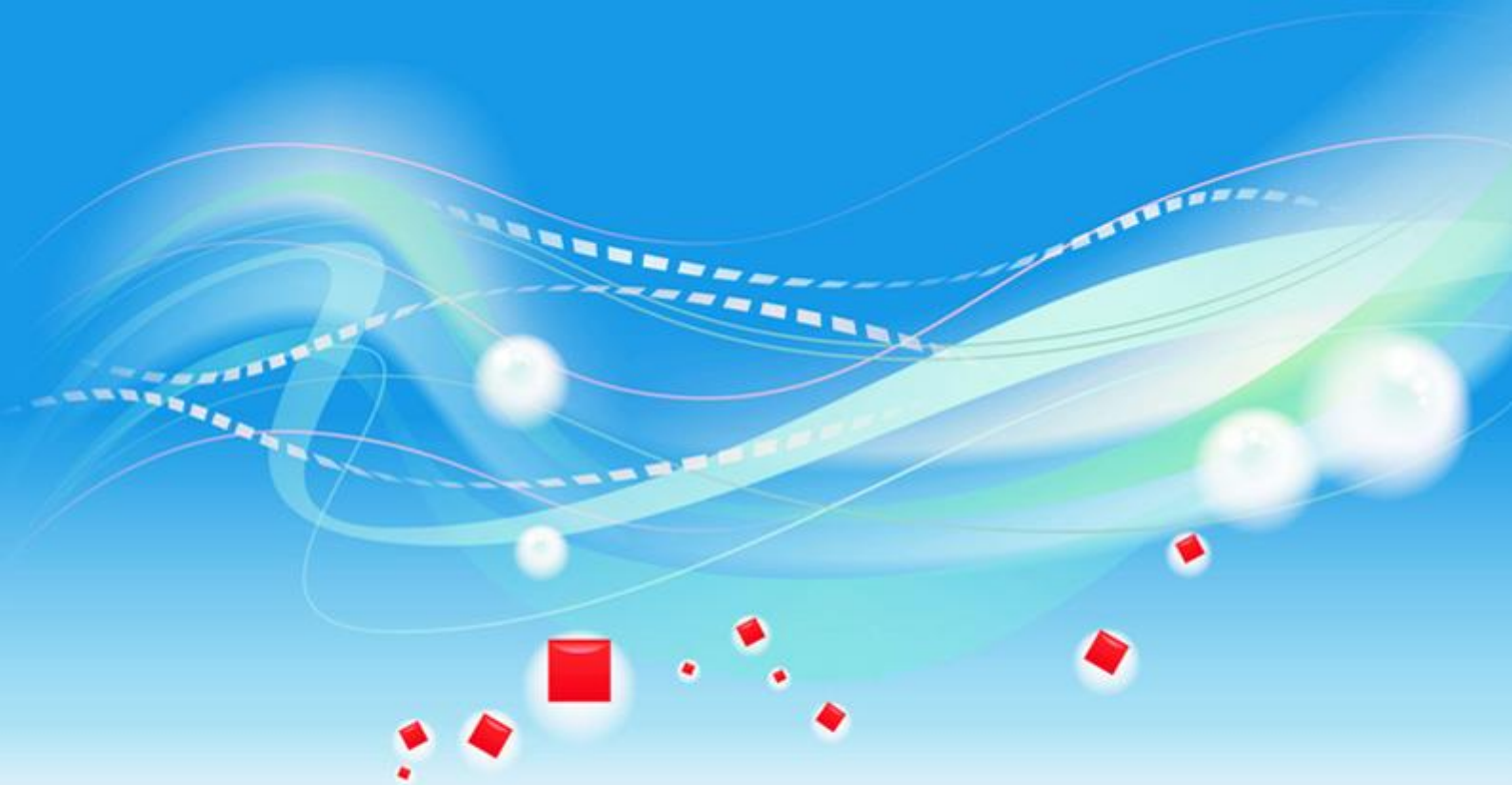

Principles of Establishing Connections in a ViPNet Network

General Information

ViPNet Virtual Private Network

infotecs

Version: 00121-02 90 04 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

This document describes the main principles of traffic routing and IP addresses translation which are applicable to ViPNet networks and ensure secure interaction of ViPNet hosts regardless of the network connection type.

Prior to reading this document, we recommend you to read the document “ViPNet Technology. General Information”.

This document does not contain any information on network management, key structure, traffic filtering principles, or deploying an infrastructure for generating digital signatures.

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.
	**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 >	A hierarchical sequence of elements. For instance, menu items or sections

Command	in the navigation pane.
`Code`	A file name, path, text file (code) fragment or a command executed from the command line.

General Principles of Traffic Routing in a VPN Deployed Using the ViPNet Technology

Modern classic VPN systems are designed mainly for connecting local networks securely through the Internet and organizing remote access to their hosts. However, not all systems can be used to create a secure environment in a heterogeneous network infrastructure by establishing direct connections between the source and the destination of information.

The main task of a VPN deployed using the ViPNet technology is to protect traffic and access computers and other network devices while exchanging data in those network segments where it is required. Furthermore, it does not matter where the device is located (in the Internet, in a corporate network, in a local network, or its segment (see Network segment on page 19)).

If two computers with the ViPNet software installed (network hosts: clients and coordinators) communicate with each other through the ViPNet network, on these computers, IP traffic encryption and decryption is performed. Thus, their traffic can't be intercepted. This functionality is provided by a special protocol of dynamic VPN traffic routing in ViPNet networks, and by ViPNet coordinators.

Besides organizing “site-to-site” communication, a coordinator can perform the standard functions of a VPN gateway: tunnel the traffic from unprotected computers and devices located behind this coordinator within the local network to other coordinators or remote clients. In this case, in contrast to other VPN systems:

- the client can be registered on any VPN gateway (coordinator);
- additional configuring is not required;
- you can automatically establish a secure connection between any application on a computer and any ViPNet host.

Coordinator's Functions in a ViPNet Network

A VPN server in a protected network is called a coordinator.

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 (see Tunnel on page 20). 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 20) which operates on the application layer. The transport module (see Transport module (MFTP) on page 20) 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 (see Public address on page 19) 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.

Connecting Hosts to a ViPNet Network

Over the dynamic VPN traffic routing protocol used in ViPNet networks, you can quickly connect a new host to a VPN with minimum configuring. To add a new host to your network structure:

- create a new host in the ViPNet Network Manager program,
- link it with other ViPNet hosts,
- specify the access address, or the DNS name of the coordinator on which this new host is registered and choose the type of connection to the ViPNet network.

When the new host connects to the ViPNet network, the coordinator will immediately inform it about access parameters of the linked hosts.

There are several possible ways of connecting a host to a ViPNet network, which differ by firewall types:

- without a firewall,
- with a coordinator functioning as a firewall,
- with static address translation,
- with dynamic address translation.

Regardless of the ViPNet network connection type, a host can function both as a client and as a server. The choice of a connection type is determined by the host's place and purpose:

- If a host has a public IP address on the Internet, then you can use the **Without a firewall** connection type.
- If a host is located in a local network protected by a coordinator, then the **Coordinator** type firewall should be used.
- If a host has no address in the Internet and operates in the local network through a device where it is possible to configure static address translation rules, you should choose the **With static NAT** connection type.

- If a host operates through a device which has only dynamic address translation rules and it is not possible to specify the static address translation rules, you should choose the **With dynamic NAT** connection type. In this case, install at least one, the so called "main coordinator" with public access to this device in the network (the type of coordinator connection to the network should be set to **Without a firewall** or **With static NAT**).

However, connection types are not bound to any specific user scenarios.

Thus, the **With dynamic NAT** connection type is universal for a client and can be used almost anywhere. For mobile clients, it is reasonable to choose this connection type when creating a host. It enables a user to connect to a ViPNet network from his or her local network, or at home, or in a hotel, without re-configuring each time.

In some cases, it may be necessary to change a connection type for a mobile client. For example, if a mobile user moves from his or her local network (where his or her coordinator is located) to a company's branch office local network or to a network of a partner company with which the user is allowed to communicate, and this network is protected with another coordinator. In this case, on the mobile client, you should choose the **Coordinator** connection type and specify a coordinator of a new network. In order not to re-configure your host each time you move to another network, you may create several pre-set configurations on the mobile client, for example, "Alabama office" or "Washington office". Upon arrival to a particular office, you simply choose the required configuration and continue working.

When choosing a connection type on stationary ViPNet hosts, you should consider the following properties of connection types:

- From a technical point of view, the **Without a firewall** and **Coordinator** connection types differ from the other two types in the way remote hosts register information about access to this host.

  For the first two types, registration is performed on the basis of cryptographically protected service information transferred together with a VPN packet. For the **With static NAT** and **With dynamic NAT** connection types, information about access parameters is registered on the basis of the source address and port of a VPN packet which are transferred unencrypted. This does not affect the security of the connections. However, the **Without a firewall** and **Coordinator** connection types are more resistant to attempted violation of connections by various attacks, including spoofing an IP packet's address or a source port. Regardless of such spoofing, reply packets will always be transferred to the address and port which are specified in the body of a VPN packet and can't be substituted.

  Taking this into account, it is reasonable to use the **Without a firewall** connection type for a coordinator if there is a public IP address (see Public address on page 19) available on its network interface (a static or dynamic one (see Dynamic address on page 18)). If there is no such address and in other cases, you may use other connection types which are no less secure.

- If you need to create protected segments (see Network segment on page 19) within a corporate ViPNet network, and those segments must have access to an external network, or if you want to direct VPN traffic through a particular route, then you can place coordinators in a line (a cascade scheme) using the **Coordinator** connection type. In this case, the traffic from an internal segment will be transferred to an external network, from one coordinator to another without any additional routing configuration required, and will not be available to anyone in the corporate network where this protected segment is located. The cascade length is not limited.

When choosing a connection type for a stationary client, you should consider the following simple rules:

- If a client is located in a local network protected with a coordinator, you should choose the **Coordinator** connection type. In this case, all protected traffic from the client to an external network will be transferred through the specified coordinator, regardless of the routing settings on the computer.
- If a client is located at home, the best connection type is **With dynamic NAT**.
- If clients are located in a local network which is not protected with a coordinator, and it is possible to configure static address translation rules on the organization's firewall, the best connection type would be **With static NAT**. If it is not possible to configure static address translation rules on the organization's firewall, you may choose the **With dynamic NAT** connection type.

Main Principles of Host Communication in a ViPNet Network

As follows from the information above, ViPNet technology may help you organize a VPN network in any distributed IP network of any structure which represents a consolidation of global, regional and local networks and includes computers of local, remote, and mobile users. Local networks may include various dedicated network segments, both wired and wireless.

ViPNet hosts (clients and coordinators) may be located in any part of such a network and have private IP addresses which may be inconsistent and non-routable in global and local networks. In this case, clients and coordinators may establish permitted peer-to-peer connections between each other for any network applications.

A VPN based on the ViPNet technology is self-adjustable. ViPNet hosts automatically register information about access parameters of other hosts and transfer this information via the

network. A ViPNet network self-adjusts in cases of changing physical or virtual network parameters and ensures transparent traffic protection while transferring a message from its sender to its recipient, regardless of the connection's initiator.

The client or coordinator software is installed on each ViPNet host, providing traffic encryption using end hosts' paired association keys (in which case, each IP packet is encrypted by using a unique derived key, see the document "ViPNet Technology. Overview"). For further traffic routing, on coordinators, each IP packet is provided with unique IDs of its sender and recipient. These identifiers are not encrypted, but protected using message authentication code (MAC).

Each ViPNet host receives information about other hosts, their access parameters, and status from its IP addresses server or from other coordinators (if the ViPNet host is a coordinator). Thus, the coordinator functioning as VPN server is responsible for collecting information about hosts and sending it to other hosts.

ViPNet hosts can be located inside any network that supports the IP protocol. The means of connection can be different: Ethernet, PPPoE via xDSL, PPP via dial-up or ISDN, mobile access such as GPRS or UMTS, Wi-Fi devices, MPLS or VLAN. The ViPNet software supports various protocols in the link layer. IP protocols of three types (IP/241, UDP, and TCP) are used to create VPN tunnels between ViPNet hosts and encapsulate traffic transferred over other IP protocols.

The IP/241 protocol (on page 19) is used when ViPNet hosts communicate with each other in the same LAN segment and when these hosts are accessible by broadcast addresses. The IP/241 protocol is more efficient because it does not have an 8-byte UDP header. When the original packet is encrypted, it is encapsulated into an IP packet with the 241 protocol number.

If the ViPNet hosts are in different network segments, the UDP protocol is chosen automatically, which allows IP packets to pass through firewalls. Upon encryption, the original packet is encapsulated in a UDP packet.

If there is a NAT device on the IP packet's route, dynamic or static address translation rules should be configured on this device. These rules allow UDP traffic exchange with ViPNet hosts. If you configure static NAT rules, you should specify the ViPNet host's port. The default port is 55777, but you can specify any other port if necessary. If packets pass directly through a coordinator, the port number of the hosts located behind this coordinator is of no importance. As they pass through a coordinator, packets acquire the coordinator's IP address and port number.

In some cases your ISP may have blocked UDP traffic and the ViPNet hosts can't communicate over the UDP protocol. For example, this may happen if you are connecting to a ViPNet VPN from a hotel or some other public place. Then you can redirect the whole IP traffic via a TCP tunnel, which has been configured on the connection coordinator of the host that initiates the connection. You may specify any port when configuring a TCP tunnel on a connection server. By default, port 443 is used.

On the connection server, the received IP packets are retrieved from the TCP tunnel and forwarded to the destination host over UDP.

Connection without a Firewall

This connection type is generally used on a coordinator with at least one public IP address. This address does not need to be static (see Static address on page 20): it may also be dynamic (see Dynamic address on page 18). In this case, you should use the dynamic DNS technology and specify the address in the ViPNet Network Manager program as the coordinator's DNS name.

Network hosts using this connection type always use the IP/241 protocol (on page 19) to connect with each other directly. Encrypted traffic from such clients to coordinators and other clients using coordinators as firewalls is always encapsulated into UDP packets.

We don't recommend you to use this connection type on clients since it may cause problems with access from external networks.

A coordinator routes VPN packets of ViPNet hosts in accordance with their destination hosts' IDs and forwards the packets further through the network; the IP address of the corresponding coordinator's network adapter and coordinator's port are assigned to these packets.

If a coordinator functions as a tunneling server (a VPN gateway), the unencrypted traffic of a specified group of computers within a local network (generally, traffic of any IP devices: IP phones, web cameras, and so on) is received on the coordinator's network adapter, encrypted and encapsulated into VPN packets. After that, these packets are forwarded to other coordinators for their tunneled devices or clients; the IP address of the coordinator's network adapter and coordinator's port are assigned to these VPN packets.

Connection via a Coordinator

If, on the edge of a local network, a ViPNet coordinator functioning as a gateway is installed, then we recommend that you choose this coordinator as a firewall for stationary clients in the local network. If a client uses a coordinator as a firewall, encrypted traffic between this client and other hosts will be transferred via this coordinator. In this case, the coordinator functions as a cryptographic gateway and a router for encrypted packets and performs address translation.

Automatic routing of encrypted packets via the coordinator is implemented by the ViPNet driver without using routing tables (see Routing table on page 20) of the TCP/IP stack specified in the operating system. The default network gateway and other routes specified in the TCP/IP

stack are not changed after the ViPNet software installation. As a result, unencrypted packets routing is not changed.

On a client, in the ViPNet Client program, you may choose a coordinator that is not the client's VPN as a firewall.

This functionality can be useful for a mobile ViPNet user working in some other ViPNet network. When you are a mobile user working in a ViPNet network, you just need to set a coordinator located in this local network as a firewall.

In addition, coordinators are reserved in the network. You can install a second coordinator on the edge of a local network. If a coordinator is unreachable, you can choose another coordinator from the list and continue working.

Protecting a Local Network Segment

To protect the traffic of a particular LAN segment with a ViPNet coordinator installed on its edge which functions as a firewall for ViPNet clients of this local network, you can install a second ViPNet coordinator on the edge of such a segment; you can install clients behind this coordinator as well.

In this case, you should choose coordinator 1 (see the scheme above) as a firewall for coordinator 2. There should be no NAT devices between these two coordinators.

This type of coordinators' connection is called a cascade connection. The number of cascades is unlimited. As a result, for these coordinators, automatic routing of encrypted traffic from the internal network segment to both local and global networks will be performed.

Connection Type With Dynamic NAT

The dynamic NAT connection type is universal and may be used by mobile users both in offices and remotely, without the need to change program settings. You can use this connection type when you work at home, as well as when there is no coordinator in a local network and connection to an external network is established through a NAT device, on which it is difficult to configure static address translation rules.

To protect traffic of several hosts in a local network which interacts with an external network through a NAT device, and if it is difficult to configure static address translation rules on this device, then we recommend that you install a ViPNet coordinator in front of the NAT device and choose the dynamic NAT connection type on this coordinator. In this case, you should make all ViPNet clients in the LAN operate through this coordinator, and on tunneled devices,

you should specify the coordinator's private IP address (see Private address on page 19) as the default gateway address.

For a host, on which the dynamic NAT connection type is chosen, to be able to connect to external hosts through a NAT device, in the external network, you should install a coordinator accessible through a public IP address (connected to the network without a firewall or via static NAT). If a mobile client uses the dynamic NAT connection type and starts working in the same local network as that coordinator, the client connects following the same rules as when uses coordinator as a firewall.

The main purpose of the **With dynamic NAT** connection type is to provide reliable connection with other hosts through NAT devices, on which it is difficult or impossible to configure static address translation rules. Such a situation is typical when you use simple NAT devices, for example, DSL modems, wireless access points, as well as when you use ICS — Internet Connection Sharing — in OS Windows, on virtual machines. It is also difficult to configure the static address translation rules on providers' firewalls (in home networks, GPRS networks, 3G, 4G, public Wi-Fi and other networks, where providers assign private IP addresses).

By default, the UDP traffic transfer is enabled for most NAT devices, as they automatically create the so-called dynamic NAT rules for inbound traffic.

These rules are based on the parameters of incoming IP packets, allowed on the NAT device. The incoming IP packets whose parameters match this dynamic rule are allowed within the specified period of time (timeout) after receiving the last IP packet. When the timeout expires and if there is no IP traffic matching the defined rule, these dynamic rules are deleted and the NAT device starts blocking the incoming IP packets.

This means that an external source can't establish connection with a network host that uses a NAT device. A host working behind a NAT device will periodically send UDP packets to its inbound connections coordinator to keep the dynamic rule active. By default, the sending interval is 25 seconds. This allows any external ViPNet host to send IP packets to the ViPNet host that uses a NAT device, via the inbound connections coordinator at any time. In response, the ViPNet host will always send IP packets directly to the external host (if the external ViPNet host does not use the **With dynamic NAT** firewall type), without using the inbound connections coordinator. After receiving the first IP packet, the external host not using a firewall **With dynamic NAT** will transfer all the IP traffic directly to the ViPNet host working via a NAT device. Thus, ViPNet hosts exchange UDP traffic directly.

This technology ensures stable failsafe access to ViPNet hosts working via NAT devices (because dynamic rules can't be deleted on a NAT device). Moreover, it provides a high speed of encrypted traffic exchange, since such an exchange uses inbound connections coordinators only at configuration setup and then all traffic is transmitted directly between ViPNet hosts (the scheme above). Note, that outbound traffic from a ViPNet host located behind a firewall with dynamic address translation to another host with the same settings always goes through the inbound connections coordinator of the other host.

Connection Type With Static NAT

This connection type is suitable if you need to protect the IP traffic of hosts in a local network, and on the edge of the local network there is a firewall that allows you to set static address translation rules. If the firewall has the NAT function and allows configuring static NAT rules, we recommend you to install a special coordinator in the corporate network to work directly with the firewall, so that corporate network traffic could be protected and access to an external network was organized.

You should choose this connection type for a client if there is no coordinator in a local network or you can't use a coordinator as a firewall for some reason, and it is difficult to configure static NAT rules on a firewall that you use to connect to an external network.

For the connection via a firewall **With static NAT** to work correctly, you should specify the address of the firewall you use as the default gateway in the OS settings of the ViPNet host. You should configure the following static address translation rules on the firewall:

- Allow and forward incoming UDP packets with a destination port specified in the ViPNet hosts' parameters;
- Allow outgoing UDP packets with addresses and ports of the ViPNet hosts behind the firewall (only in case outbound UDP traffic is blocked on the NAT device by default).

Warning: If there are several clients using the same firewall with static address translation, each client should have its own UDP port number. If several clients use one and the same port, there may be a conflict.

Virtual IP Addresses

When you connect remote users to local network resources and use the VPN technology to establish protected connections between local networks, you may face the challenge of IP address allocation and distribution. Addresses should be distributed to exclude potential conflicts — on a ViPNet host, all remote hosts' IP addresses should be unique.

In a classic VPN system, when you establish a partner network connection, you can solve this problem only by aligning address pools different from your partner network's pools to your local network. When you use multiple VPN technologies and want to organize remote access on a client host, you usually create a virtual adapter which is assigned with an address when a connection is established to a VPN gateway. In order to establish several VPN connections with several VPN gateways for access to various local networks, you should create several virtual adapters.

All these solutions have a number of disadvantages:

- It is not always possible to align address pools in various local networks.

  When the addresses are automatically assigned to virtual adapters, on a VPN gateway, there is a risk of conflict with a subnetwork where your computer is physically located. In this case, the network will become inoperative. When establishing connections to multiple gateways, it is also difficult to avoid address conflicts.

  In these cases, addresses are assigned from some private address space, which entails a high risk of potential intersection of IP addresses.

- Clients encrypt only the information received by their virtual adapters. Encryption is controlled using a highly insecure method — by editing a routing table in the TCP/IP stack (see Routing table on page 20).

The ViPNet technology uses a fundamentally different method to prevent conflicts and establish VPN connections.

The virtual IP addressing technology allows you to avoid all IP address conflicts. On each ViPNet host, each remote host's IP address and each tunneled IP address of remote coordinators are matched with their own virtual IP address, unique on this ViPNet host. Virtual IP addresses are assigned not to IP addresses, but to ViPNet host IDs. The number of virtual addresses assigned to each host equals the current number of its real addresses (see Real IP address on page 19). Each virtual IP address assigned to a tunneled static real IP address of a coordinator will exist as long as the real IP address exists. A range of virtual addresses is assigned to a range of tunneled real IP addresses. A range of virtual addresses will exist as long as the corresponding range of real tunneled addresses exists.

When conflicts occur within connections with remote hosts, the ViPNet driver forces its host's applications to use the assigned virtual IP addresses. As a result, there are no limitations to the address structure in different subnetworks, address alignment is not required, and a risk of conflicts is excluded for any remote user.

Besides, you don't need to create virtual adapters on your client. The TCP/IP stack operation parameters don't affect encryption procedures. The ViPNet driver intercepts all traffic, so the need to encrypt each IP packet and encryption keys are determined by the ViPNet driver based

on the information about IP addresses of all recipients. As a result, traffic going in any direction is automatically encrypted without any pre-configuration of your computer. For virtual IP addresses, the ViPNet driver also routes their traffic, forwarding it to the nearest access point's IP address.

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), Routing, ViPNet host.

D

Dynamic address

An IP address assigned to a host for one session by a DHCP service.

See also: DHCP service.

E

Edge of a local network

A conventional concept denoting a meeting point between a local network and a global network or another local one.

See also: Global network, Local area network (LAN).

External IP addresses

Addresses used in an external network.

See also: External network.

I

Internal IP addresses

Addresses of an internal network.

See also: Internal network.

IP addresses server

A feature of the ViPNet Coordinator software, providing collection and distribution of information about ViPNet host statuses (accessible, unavailable, last time of user activity).

See also: Coordinator (ViPNet coordinator), Protected host.

IP/241 protocol

An IP protocol 241 developed specially for ViPNet software.

N

Network segment

A portion of a computer network wherein devices communicate with each other using the same physical layer.

P

Private address

For the IP networks where direct connection to the Internet is not required, three IP addresses ranges can be used: 10.0.0.0-10.255.255.255; 172.16.0.0-172.31.255.255; 192.168.0.0-192.168.255.255. These addresses ranges can't be used on the Internet. If your IP address belongs to one of these ranges, you should use a firewall with the NAT function or a proxy to connect to the Internet.

Any organization may use any addresses sets from the above-mentioned ranges for its local network.

See also: Firewall, Network addresses translation (NAT).

Public address

An IP address that can be used on the Internet.

See also: Private address (on page 19).

R

Real IP address

An IP address assigned to a network interface of a computer in a local network or the Internet.

See also: IP address, Local area network (LAN), Network interface, Virtual IP address (on page 20).

Routing table

Table-like data used to discover a route to transfer data.

See also: Routing.

S

Static address

An IP address assigned to a computer permanently by fixed configuration of its hardware or software.

See also: IP address.

T

Transport module (MFTP)

A program intended to transfer data in a ViPNet network.

Tunnel

A virtual communications channel, connecting endpoints of one or several networks. It is created by means of the tunneling technology.

See also: Tunneling.

Tunneling coordinator

A feature of ViPNet Coordinator software, defined in Network Control Center or ViPNet Network Manager, providing traffic tunneling from specified local hosts where no ViPNet software with network layer traffic encryption is installed. The traffic is unencrypted only between the tunneled host and the tunneling coordinator; in other network sections the traffic is encrypted.

See also: Coordinator (ViPNet coordinator), Tunneled host, Tunneling, Unprotected IP traffic.

V

Virtual IP address

An IP address that is used by ViPNet host A to provide access to resources or tunneled resources of ViPNet host B instead of its real IP address. Virtual IP addresses for ViPNet host B are specified on ViPNet host A. On other hosts, other virtual addresses may be specified for ViPNet host B. ViPNet host B may be allocated as many virtual addresses, as many real addresses it has. When real addresses of ViPNet host B are changed, its virtual addresses specified on other hosts remain the same. Virtual IP addresses of tunneled hosts are mapped to real IP addresses of these hosts. They exist as long as the corresponding real IP addresses exist. Use of virtual IP addresses allows you to avoid conflicts of real IP addresses in case addresses ranges in local networks overlap. Also, you can use these IP addresses to authenticate remote hosts in ViPNet software.

See also: IP address, Real IP address (on page 19).