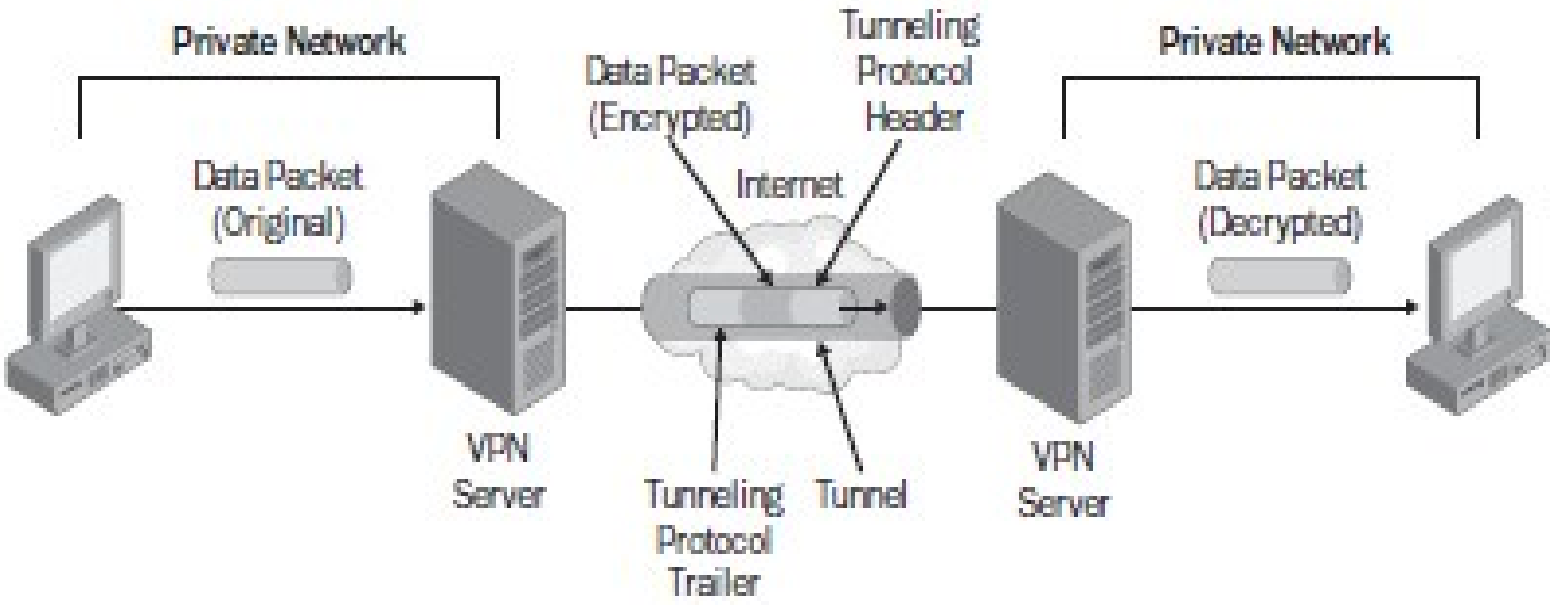
Virtual Private Networks (VPN)

Христо Вълчанов
Технически Университет - Варна

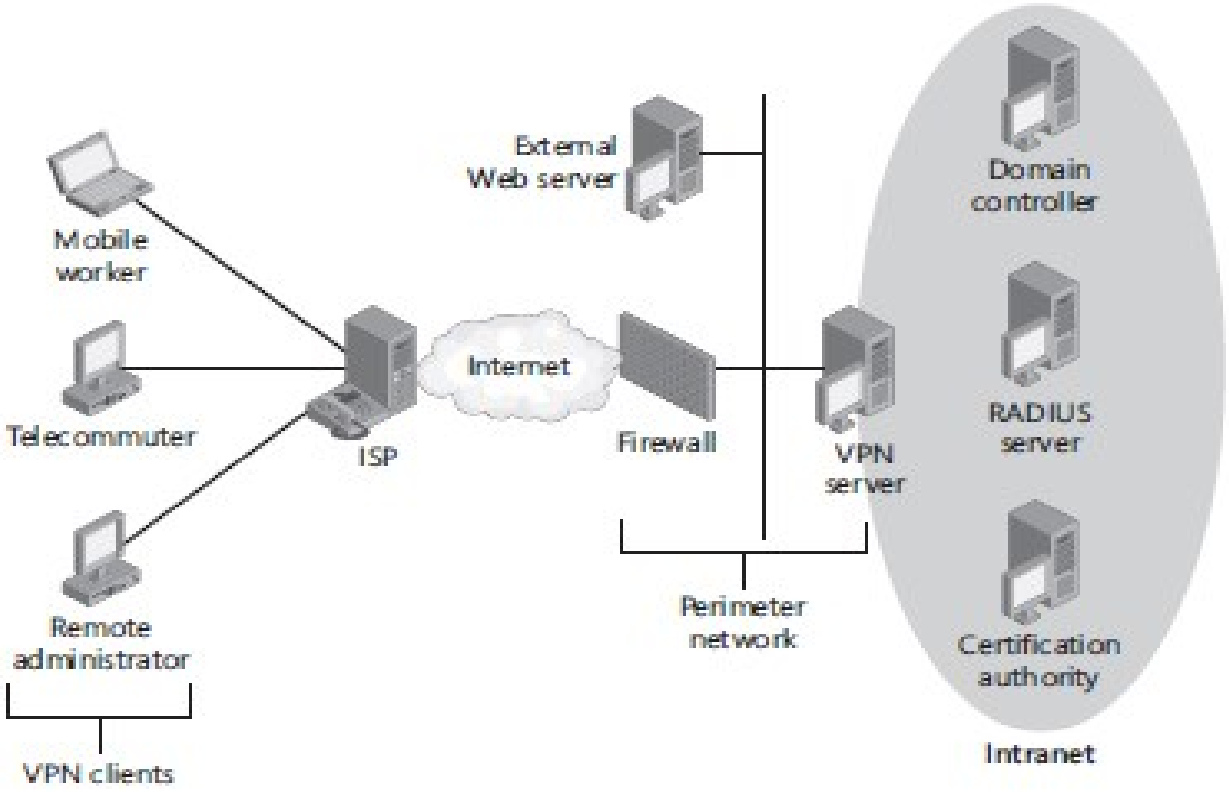
Предназначение на VPN

- Осигуряване на защитена криптирана връзка през Internet.
- VPN може да свързва както единичен компютър, така и мрежа към друга мрежа
- Обикновено потребителите се свързват към VPN, като
  - Първо се свързват към ISP
  - След това към VPN порт

VPN тунели


Private Network
Data Packet
(Original)
VPN
Server
Data Packet
(Encrypted)
Tunneling
Protocol
Header
Internet
Tunneling
Protocol
Trailer
Tunnel
VPN
Server
Private Network
Data Packet
(Decrypted)

Компоненти на отдалечен VPN достъп



VPN клиенти и сървъри

- VPN клиент – компютър стартиращ VPN връзка
- VPN сървър – компютър, отговорен за установяване на VPN връзка

Два типа VPN връзки:

- VPN връзка чрез отдалечен достъп – отдалечен потребител се свързва към корпоративен Intranet
- Router-to-router VPN връзка – отдалечена мрежа чрез рутер се свързва към корпоративен Intranet

Протоколи за виртуални частни мрежи

VPN протоколите капсулират данновите пакети в PPP пакети.

VPN се изграждат на базата на един от следните два протокола:

- Point-to-point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)

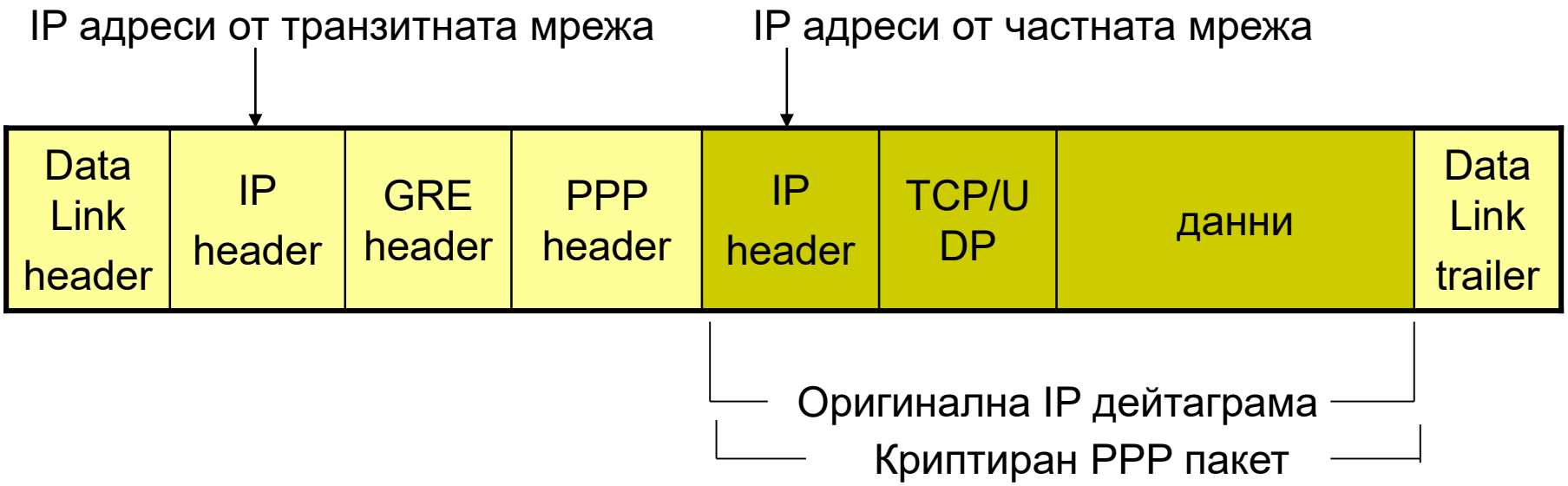
PPTP и L2TP

PPTP	L2TP
Междумрежовата комуникация трябва да е IP базирана	Междумрежовата комуникация може да бъде IP, Frame Relay, X.25, or ATM базирана
Без компресия на header	Компресиране header
Без автентикация на тунела	Автентикация на тунела
Изграден на базата на PPP криптиране	Използва IPSec криптиране

Протокол PPTP

- Капсулира PPP пакетите в IP пакети за предаване през IP базирани мрежи
- Използва TCP за връзка между VPN клиент и сървър

Структура на PPTP пакет



Протокол PPTP

Последователност на преобразуване на изходящите пакети:

- Капсулиране на оригиналната дейтаграма в PPP пакет
- Компресиране с MPPC
- Криптиране с MPPE
- Капсулиране с GRE header
- Формиране на нова IP дейтаграма с IP адресите на PPTP клиента и сървъра.

Протокол PPTP

General Routing Encapsulation (GRE) header включва полета за:

- Дължина на пакета
- Идентификатор на тунела, през който се предава пакета (Call ID)
- Поле за подтвърждение (Acknowledgment) за откриване на пропаднали пакети

Алгоритъмът за криптиране MPPE осигурява:

- Базова схема за кодиране – 40 битов ключ
- Силно кодиране – 56 битов ключ
- Много силно кодиране – 128 битов ключ

Протокол PPTP

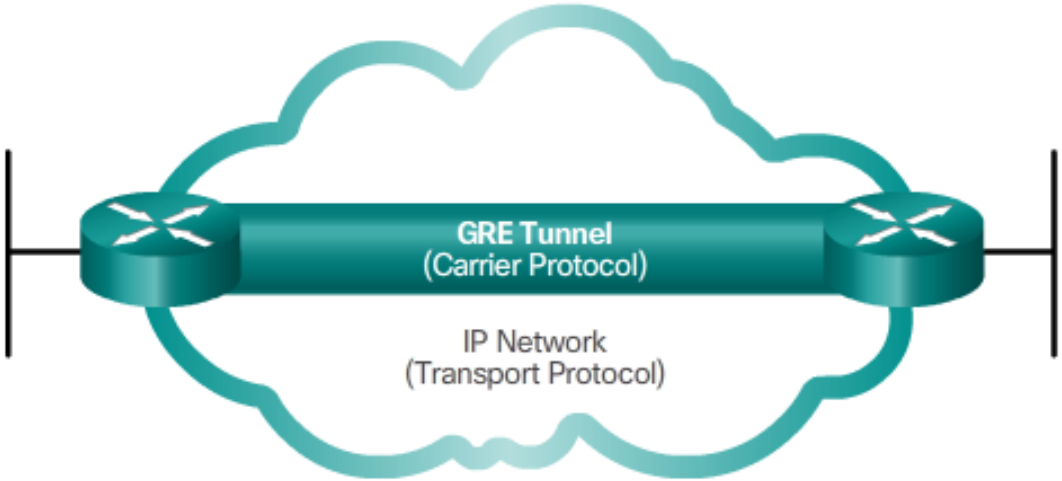
За управление на тунела между PPTP клиент и сървър се изгражда управляваща връзка, базирана на TCP:

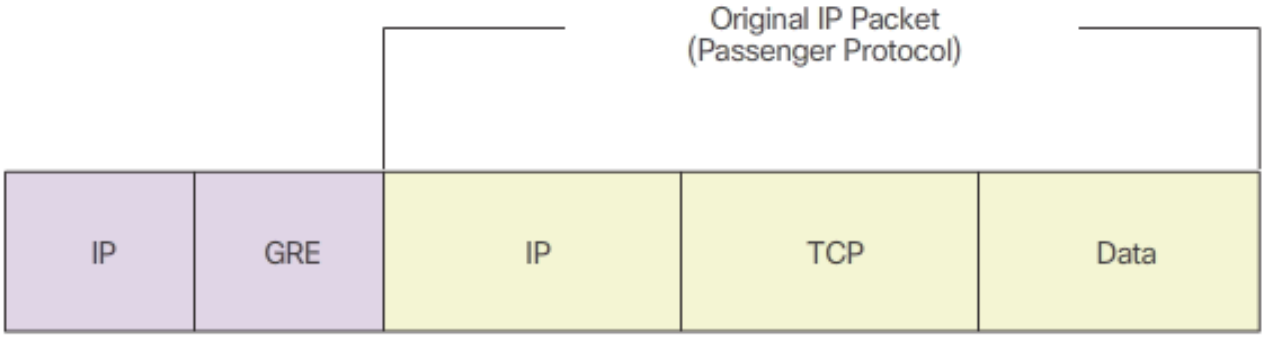
- Създаване на връзка чрез обмен на PPTP служебни съобщения. Клиентът и сървърът определят своите Call ID
- Следене на връзката – чрез чрез обмен на служебни съобщения Echo-Request и Echo-Reply.
- Закриване на връзката.

Протокол GRE

За управление на обмена на мултипротоколен и мултикаст трафик между две страни, имащи само IP връзка.

Протокол GRE





Протокол L2TP

- Работи на ниво 2 на OSI
- Създава тунел между L2TP клиент и L2TP сървър
- Използва UDP за създаване и управление на тунела и транспортиране на данните.
- Поради ненадеждността на UDP използва свой собствен механизъм за контролиране на реда на получаване на пакетите, базиран на номериране на пакетите.

Протокол L2TP

- L2TP работи съвместно с IPSec
- L2TP клиентът и сървърът трябва да поддържат и двата протокола
- Пакетите се криптират със средствата на IPSec
- При предаване на данните клиентът и сървърът използват IPSec за договаряне на защитена комуникация
- По подразбиране за автентикация се използват сертификати

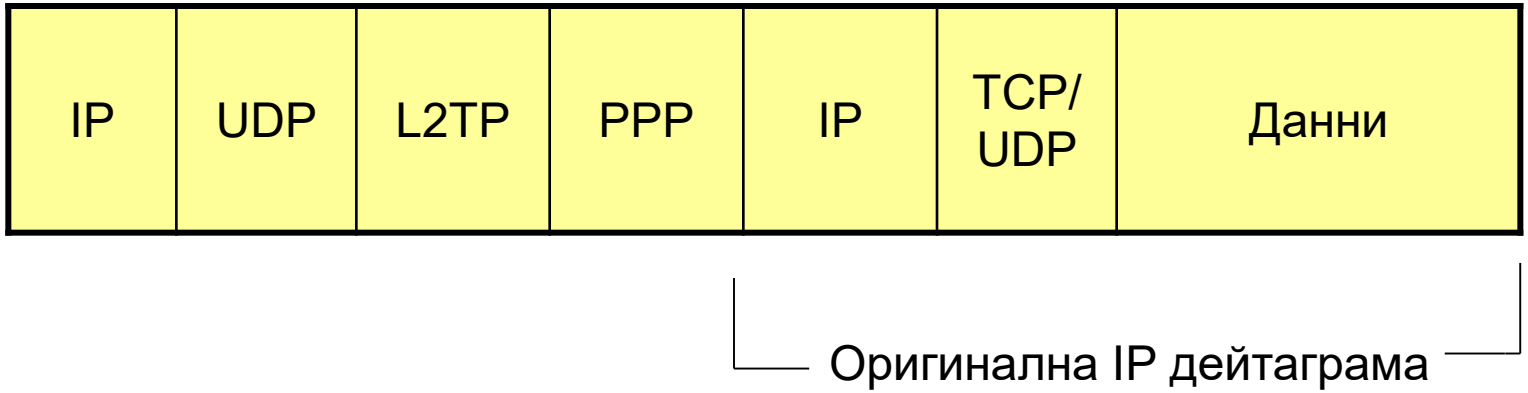
Протокол L2TP

Последователност на преобразуване на изходящите пакети:

- Капсулиране на оригиналната дейтаграма в PPP пакет
- Формиране на нова IP дейтаграма с IP адресите на L2TP клиента и сървъра, UDP header и L2TP header (UDP порт 1701)
- Изпращане на получената дейтаграма към компонентите на IPSec.

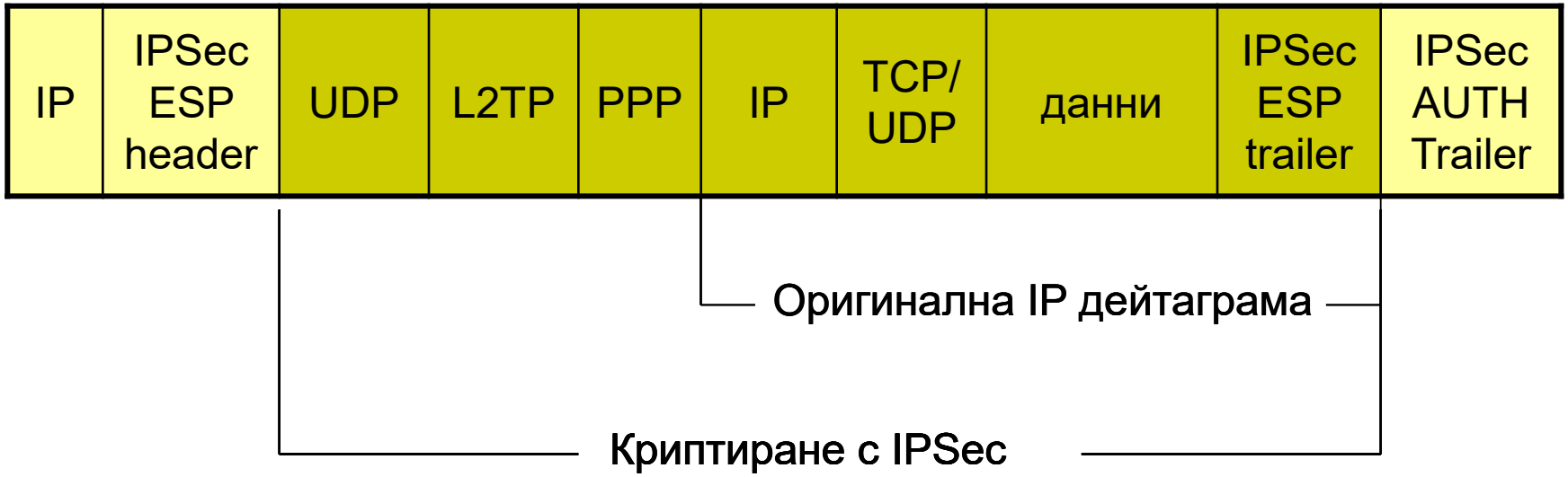
L2TP капсулиране

Некриптиран L2TP пакет



L2TP капсулиране

L2TP пакет, криптиран с IPSec



Предназначение на IPSec

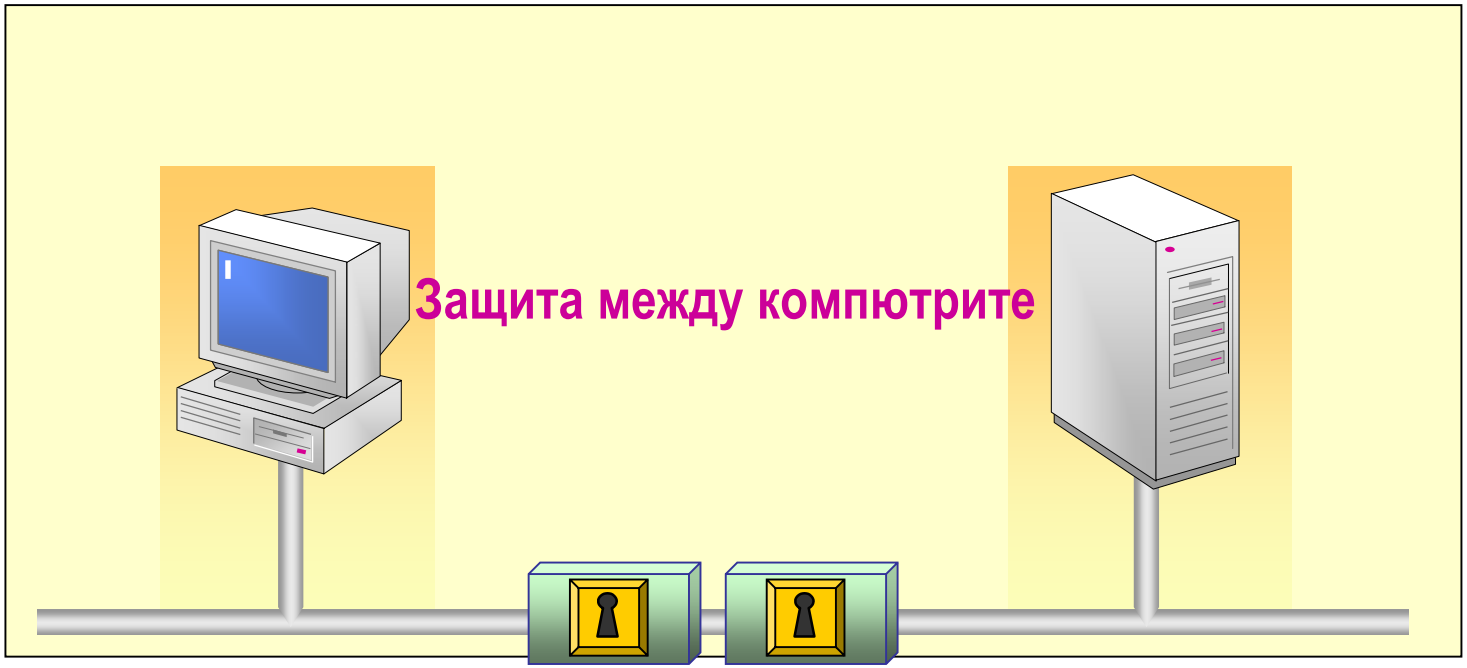
Цел: Осигуряване на защита на IP пакетите посредством използване на криптографски методи

Модел на защита: *от край до край (end-to-end)*:

- Изпращащият и приемащият хост управляват защитата от своя собствен край
- Предполага се, че комуникационната среда не е защитена
- Междинните рутери може да не поддържат IPSec
- Транспарентност за междинните рутери, поради използването на стандартен IP пакет.

IPSec за защита между компютри

- Използване на IPSec в транспортен режим
  - Това е режим по подразбиране за IPSec
  - Осигурява защита end-to-end
  - Установява IPSec политики за трафик между системи



IPSec за защита между компютри

- Използване на IPSec в тунелен режим
  - Задава тунел между два рутера
  - Защита end-to-end
  - Установява IPSec политики за целия Internet трафик

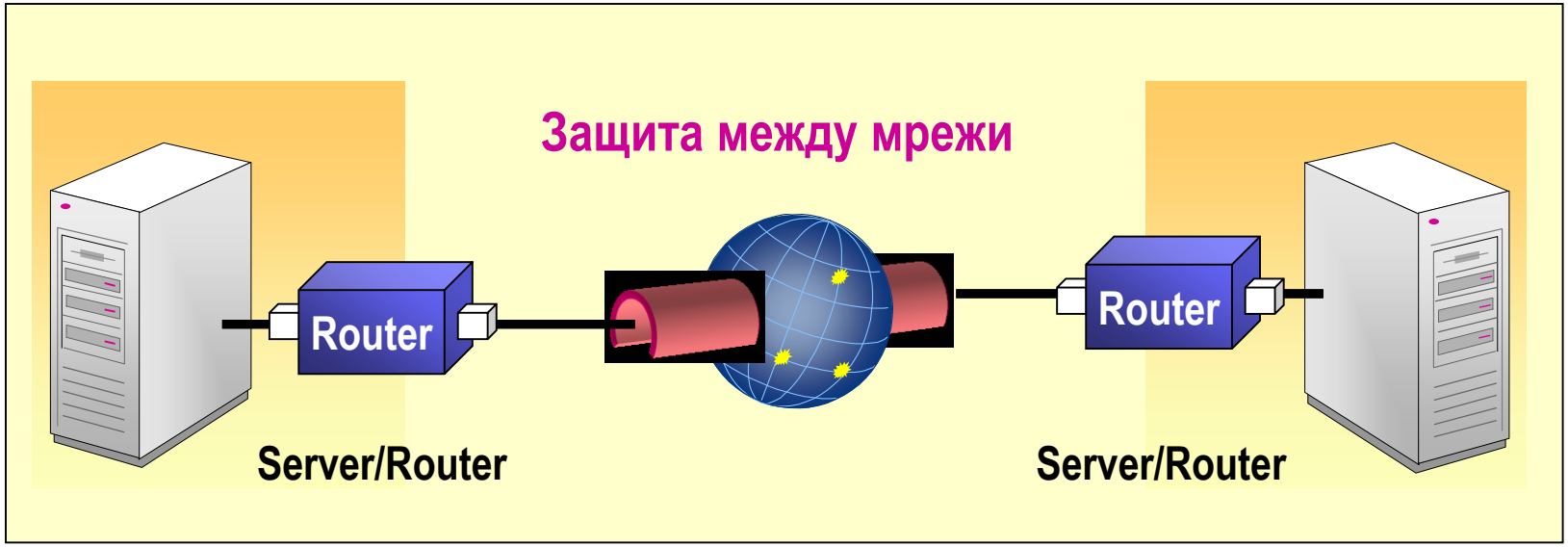


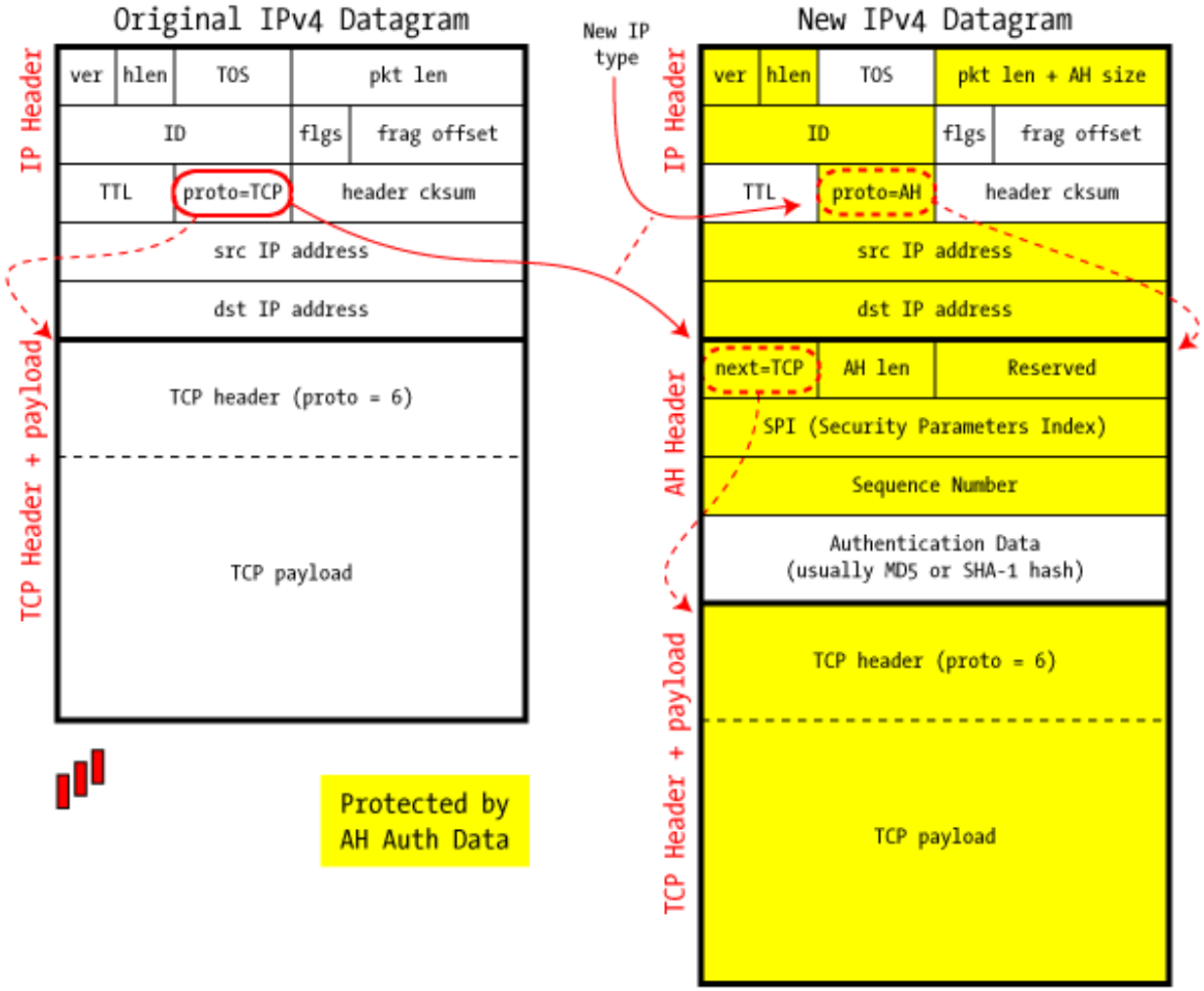
Схема за криптиране

- Криптиране на автентикацията
  - SHA – Secure Hash Algorithm – метод с висока сигурност, използващ 160 битов ключ
  - MD5 – Message Digest 5
- Криптиране на пакети
  - 56-bit DES – за приложения не изискващи висока сигурност.
  - 40-bit DES – метод, използван за Франция.
  - 3DES – по-сигурен метод. Използва три 56 битови ключа. Обработва всеки блок 3 пъти, като всеки път използва уникален ключ.
  - AES – препоръчван метод (256 битов ключ).

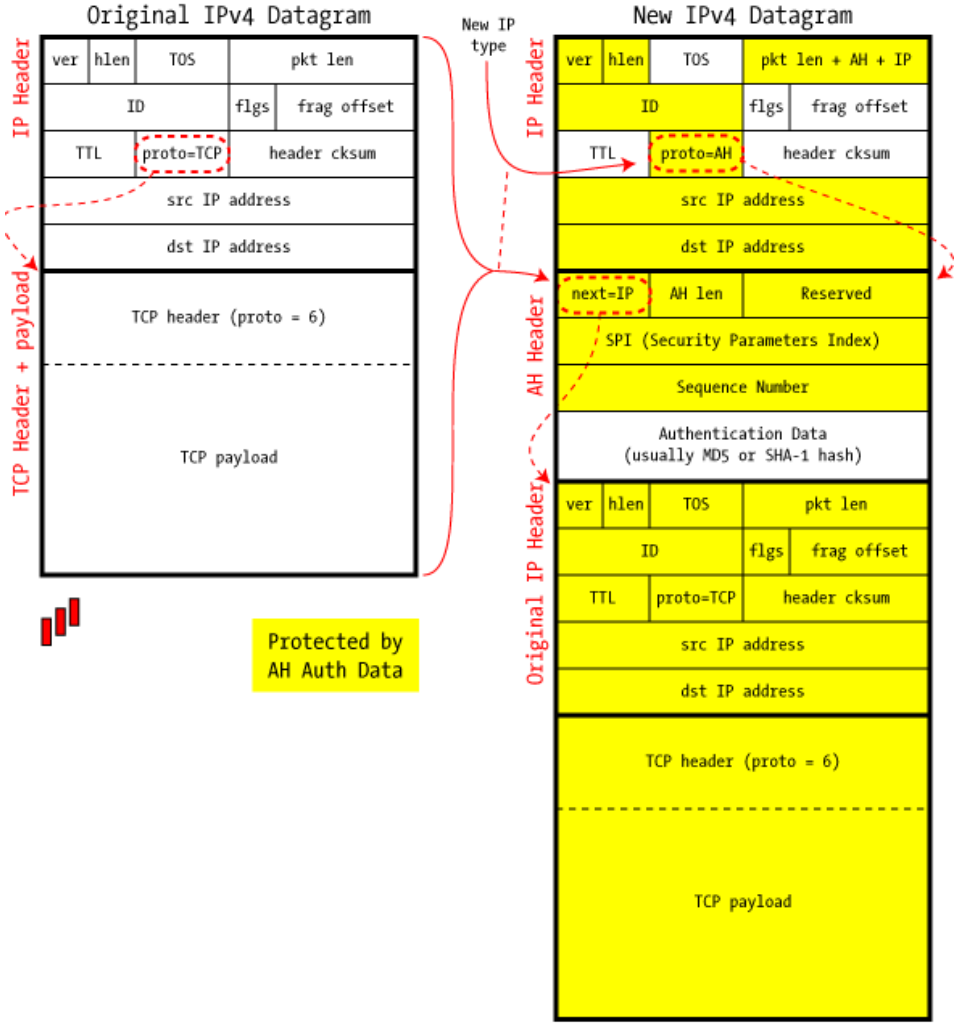
Типове IPSec протокол

- **Authentication Header (AH)** – осигурява автентикация и неделимост на целия пакет. Не криптира данните (не осигурява конфиденциалност), но ги защитава от модификация.
- **Encapsulating Security Payload (ESP)** – осигурява конфиденциалност, автентикация и неделимост. Може да се използва самостоятелно или в комбинация с AH.

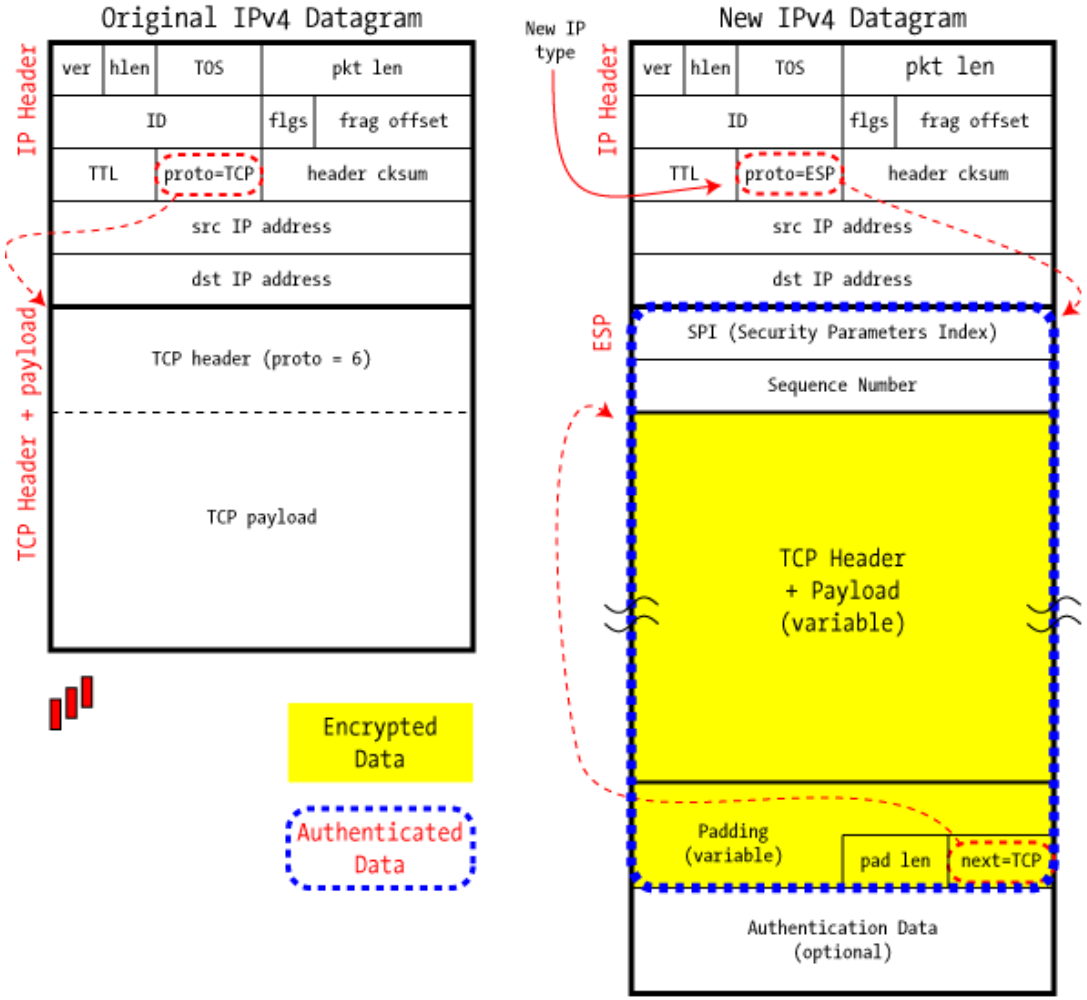
AH - транспортен режим



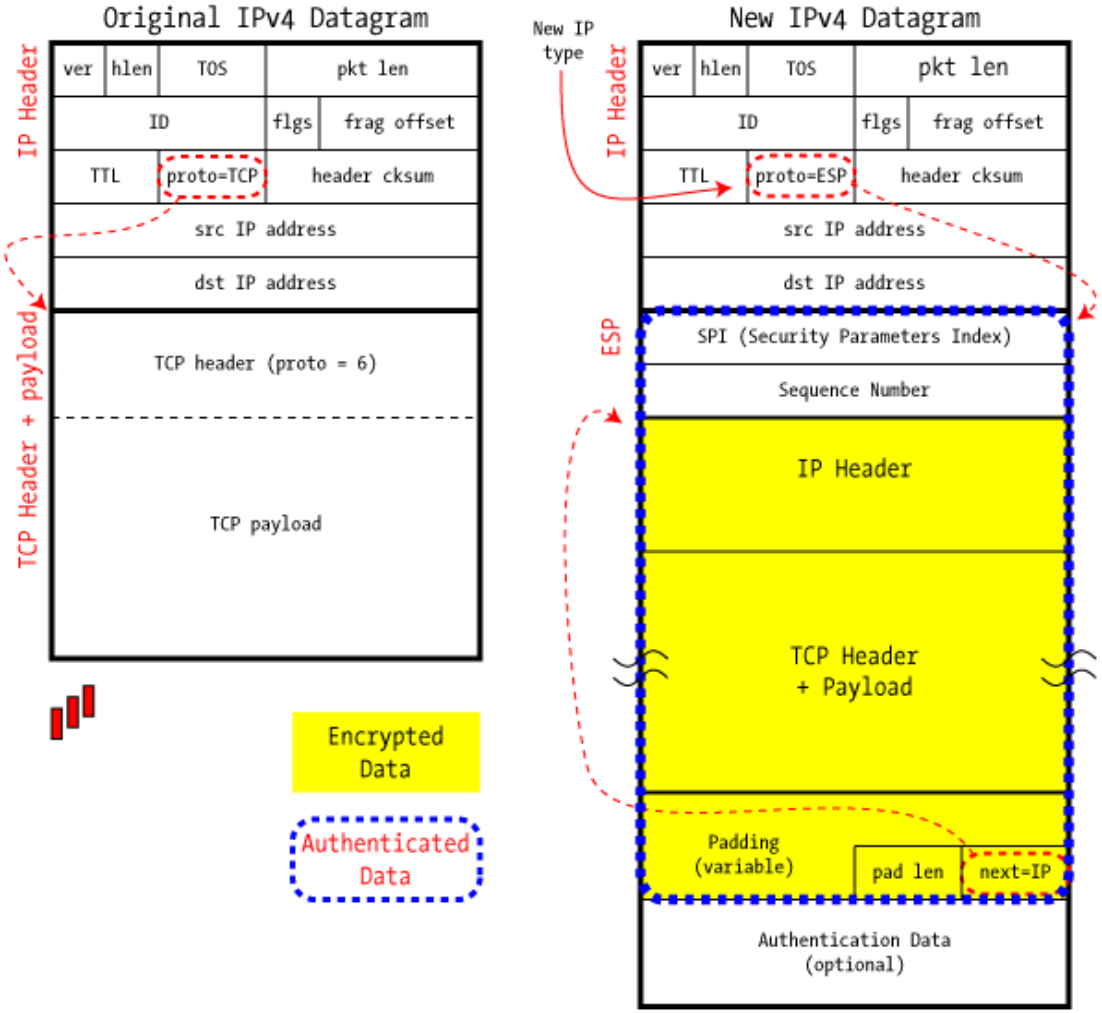
AH - тунелен режим



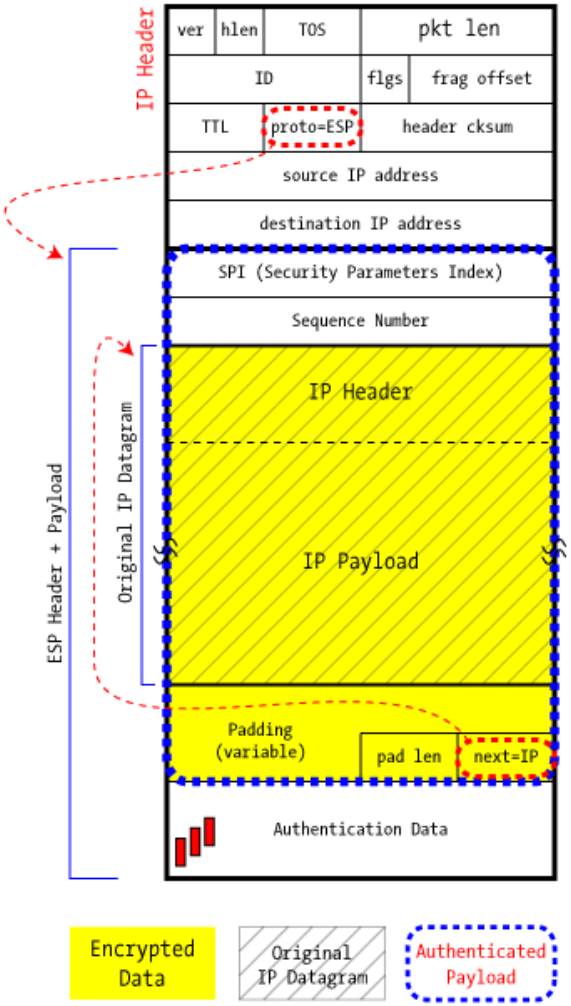
ESP – транспортен режим



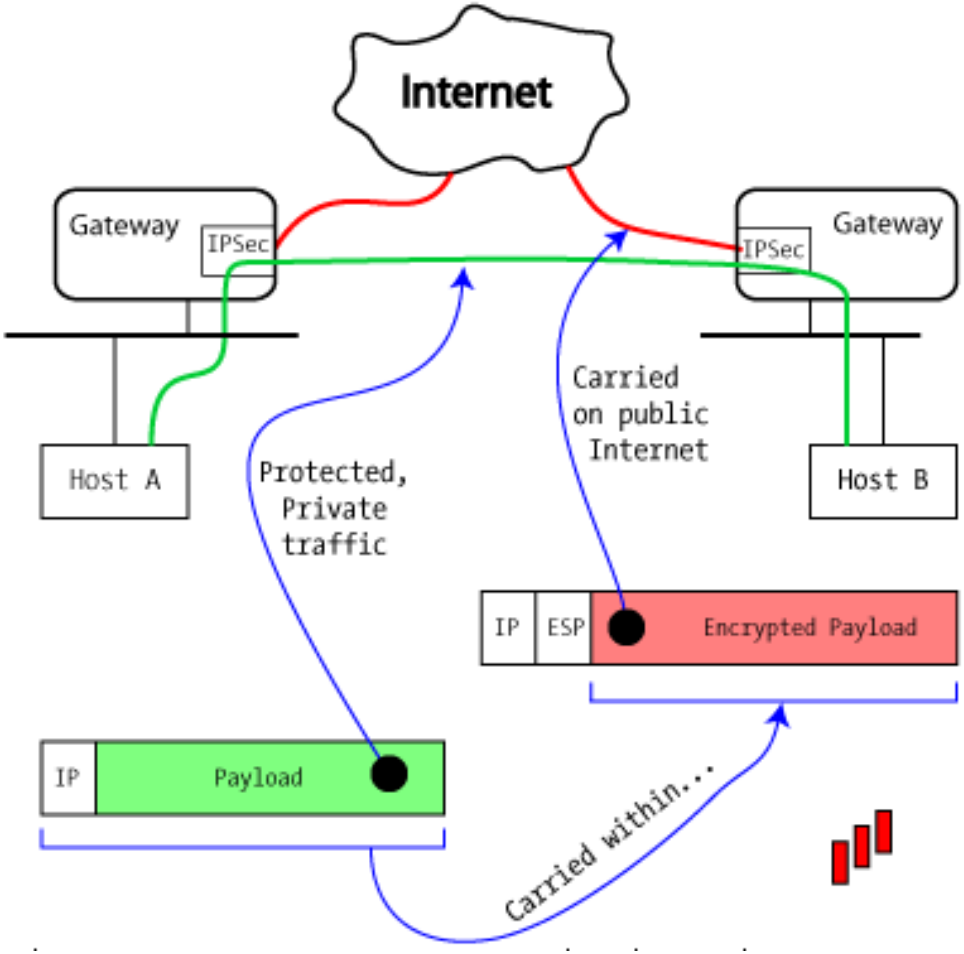
ESP – тунелен режим



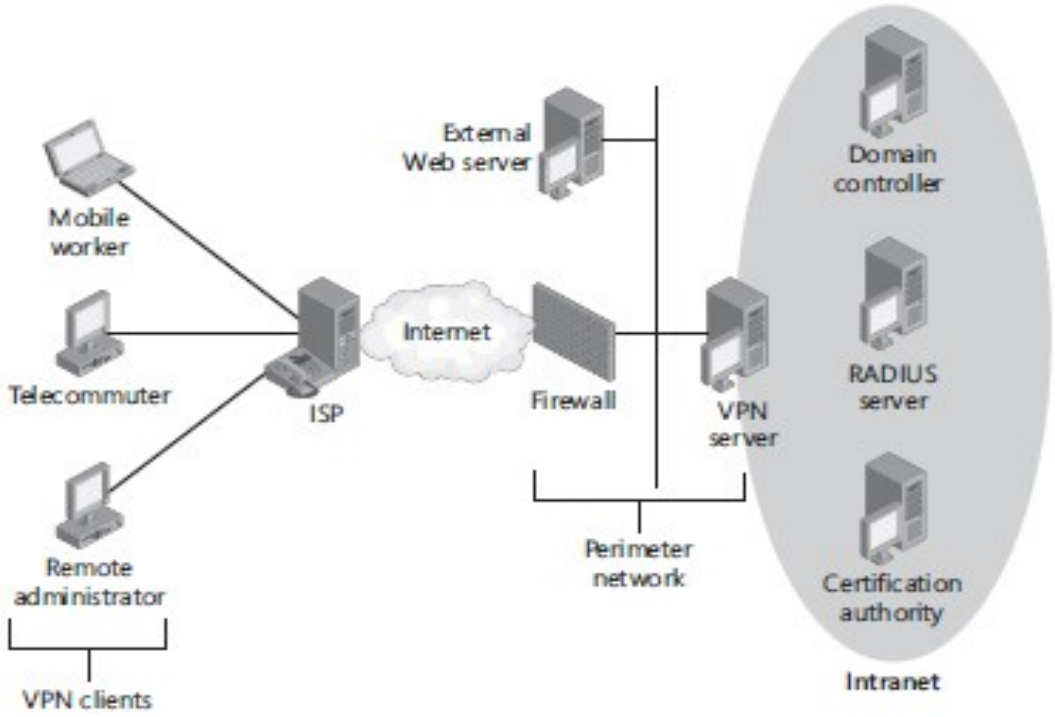
VPN капсулиране



VPN конекция

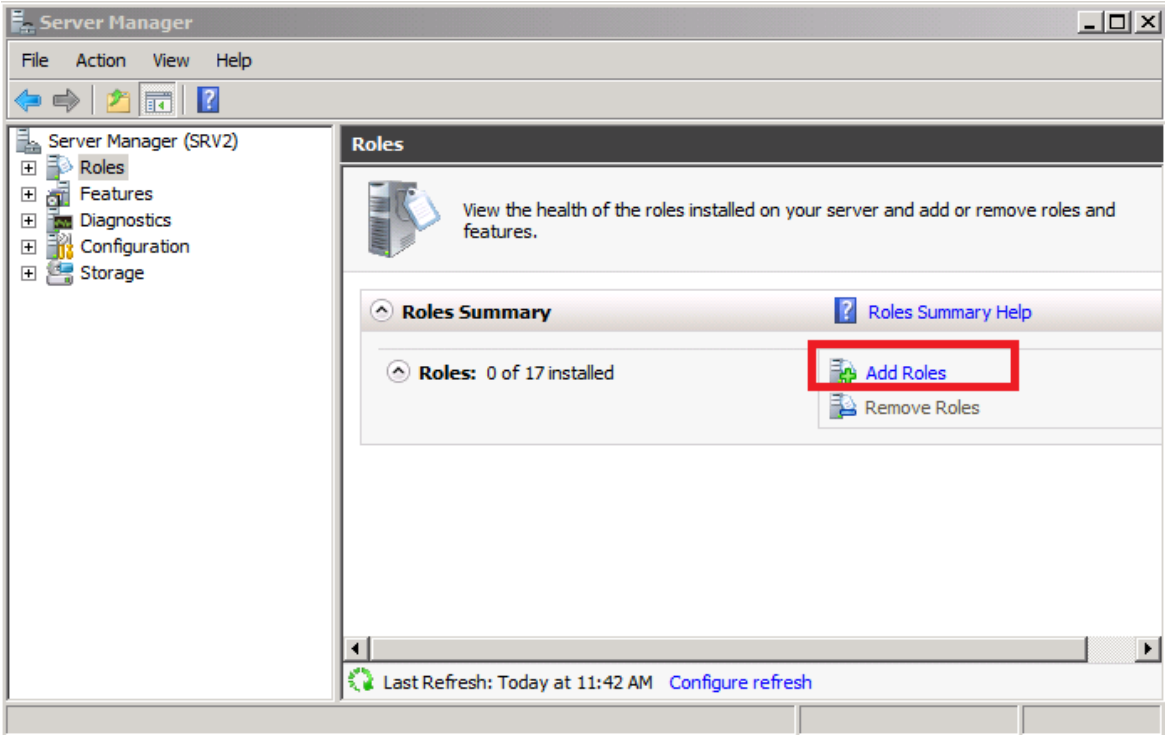


Конфигуриране на VPN сървър за отдалечен достъп



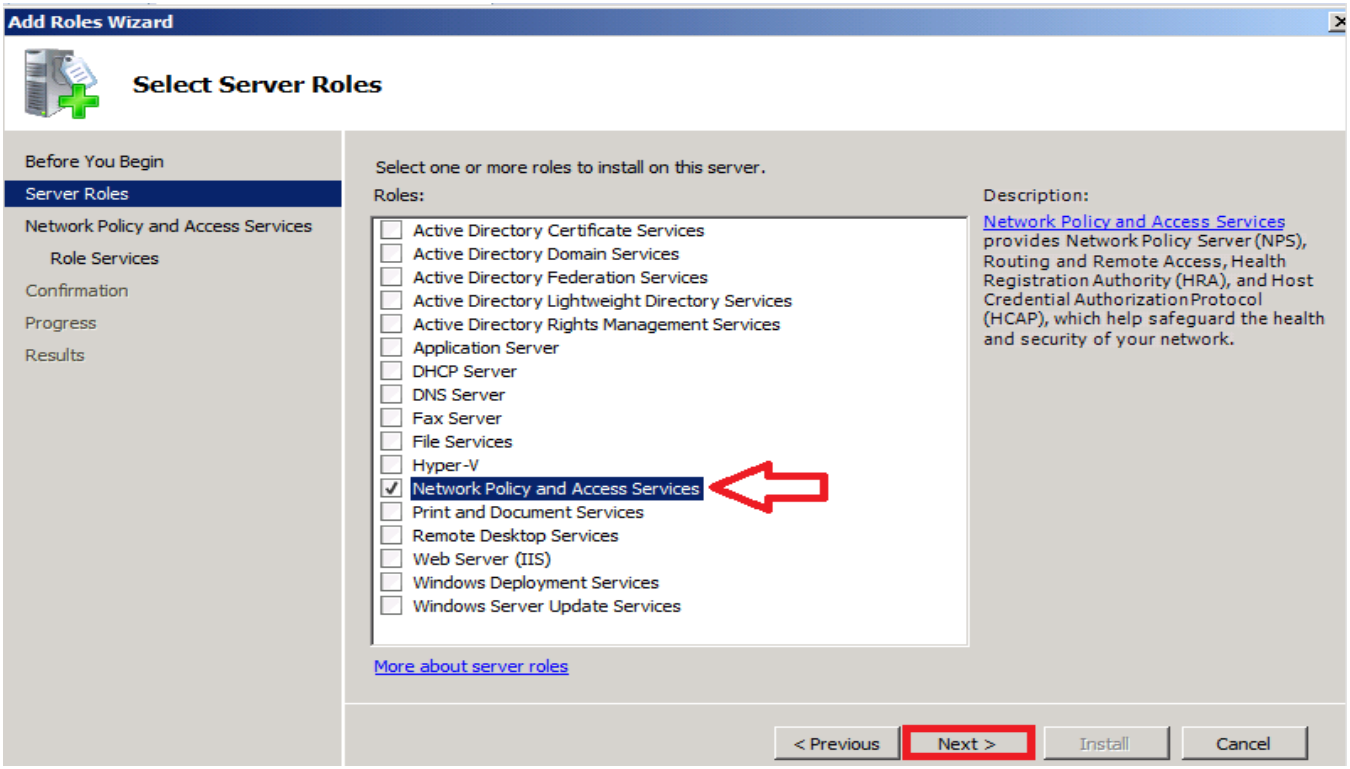
- VPN сървър
- VPN клиент

Инсталиране на роля



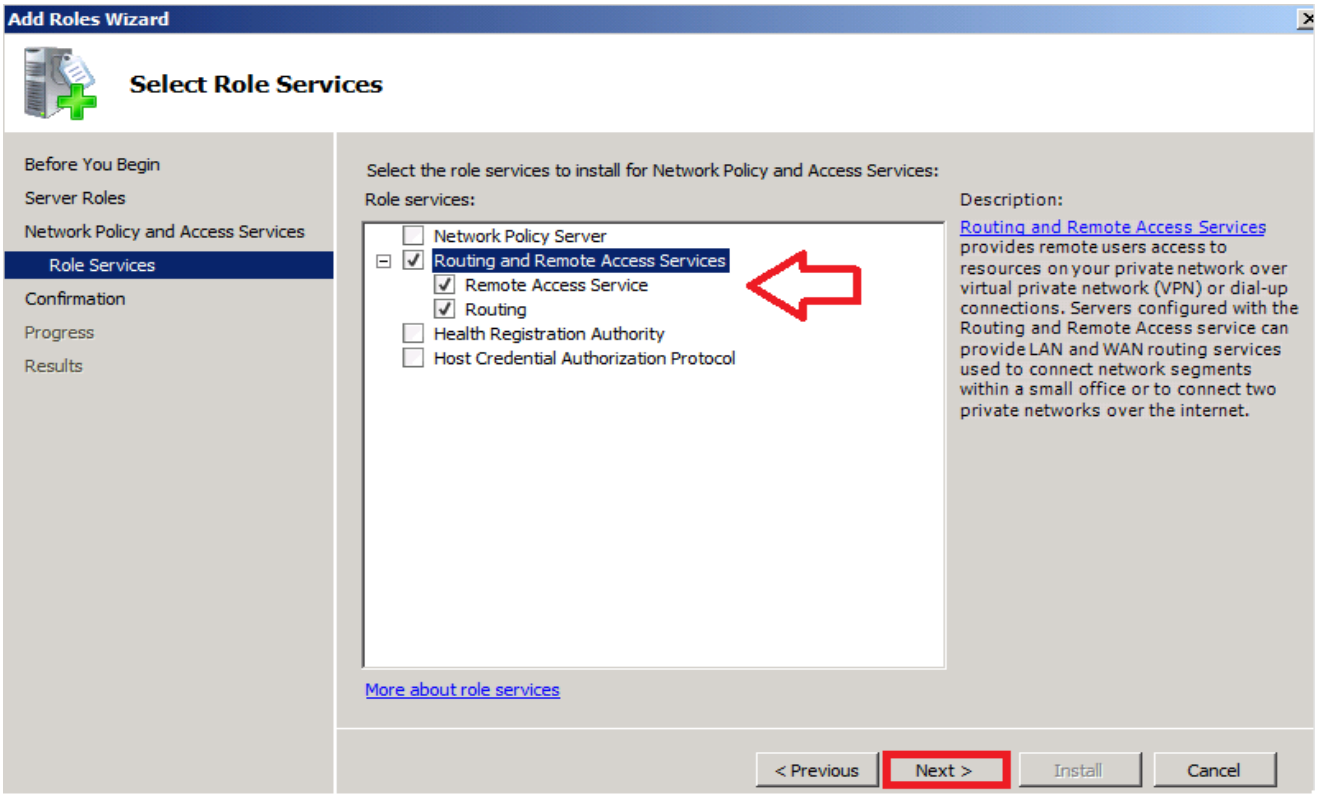
Инсталиране на роля

Network Policy and Access Services

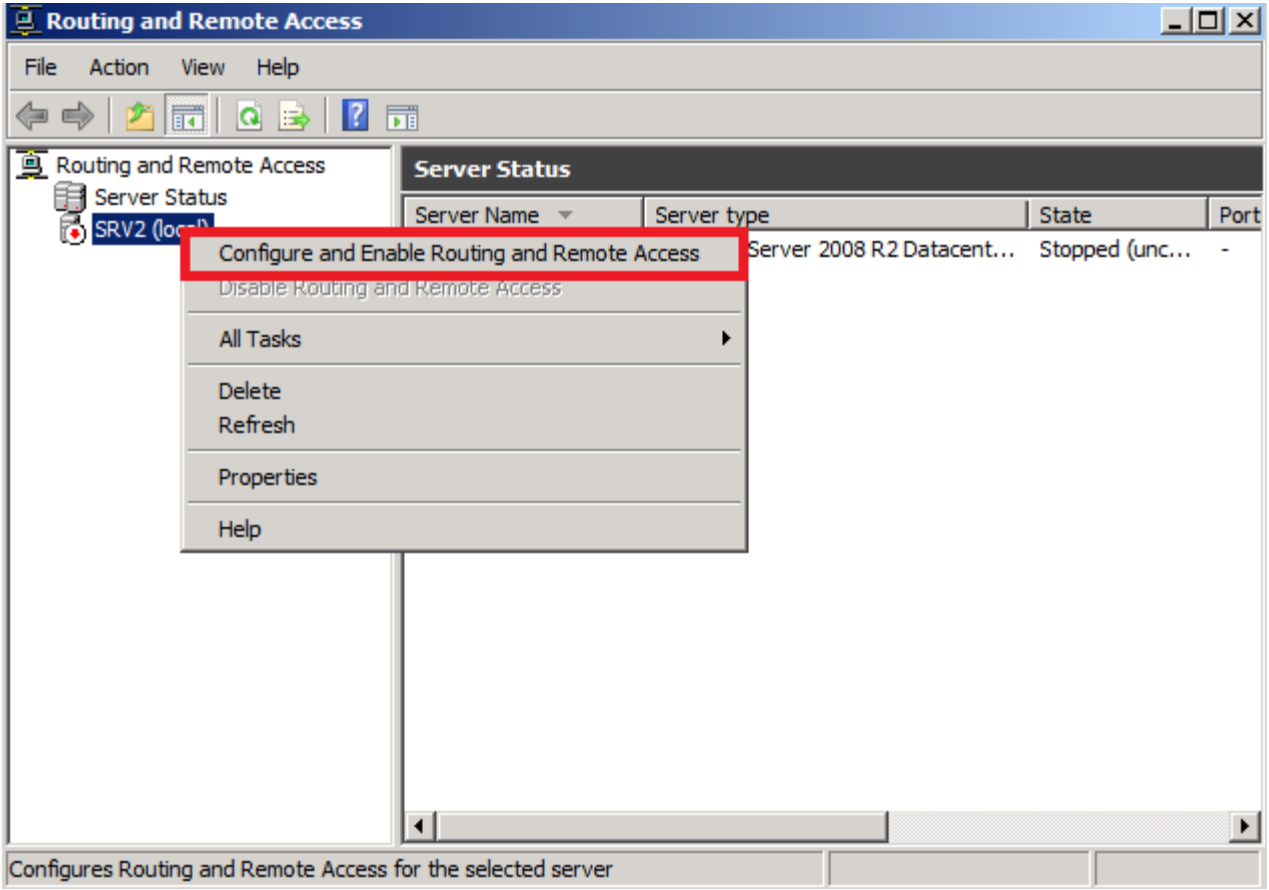


Услуги на ролята

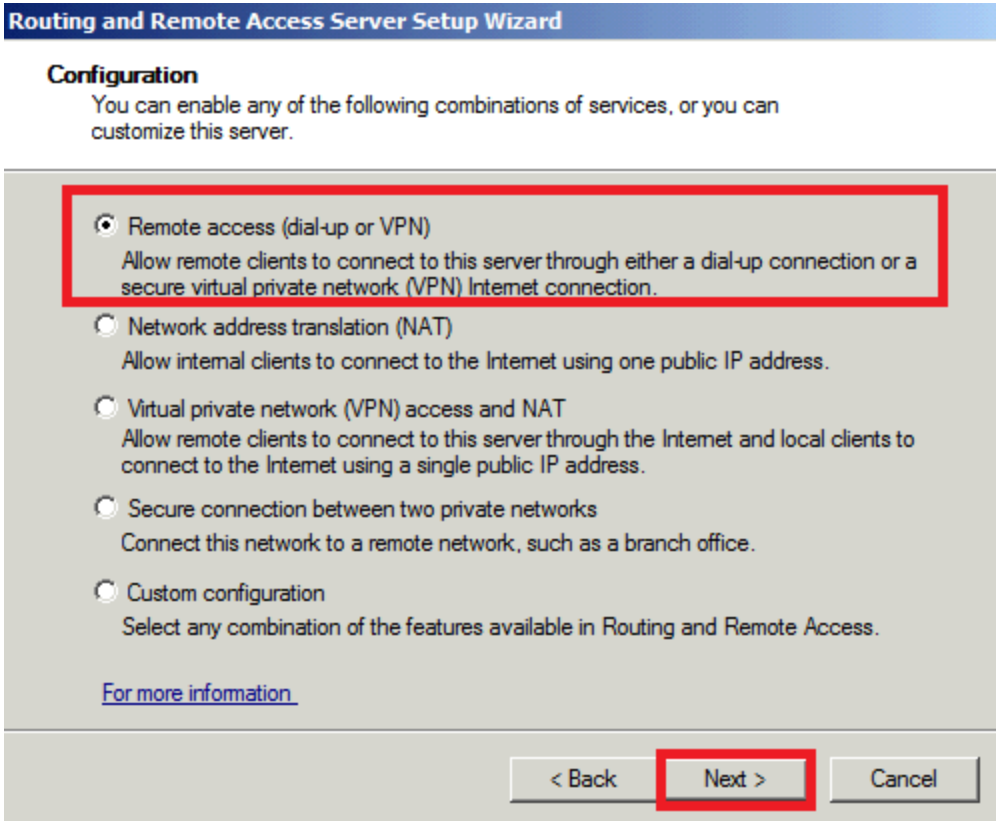
Routing and Remote Access Services



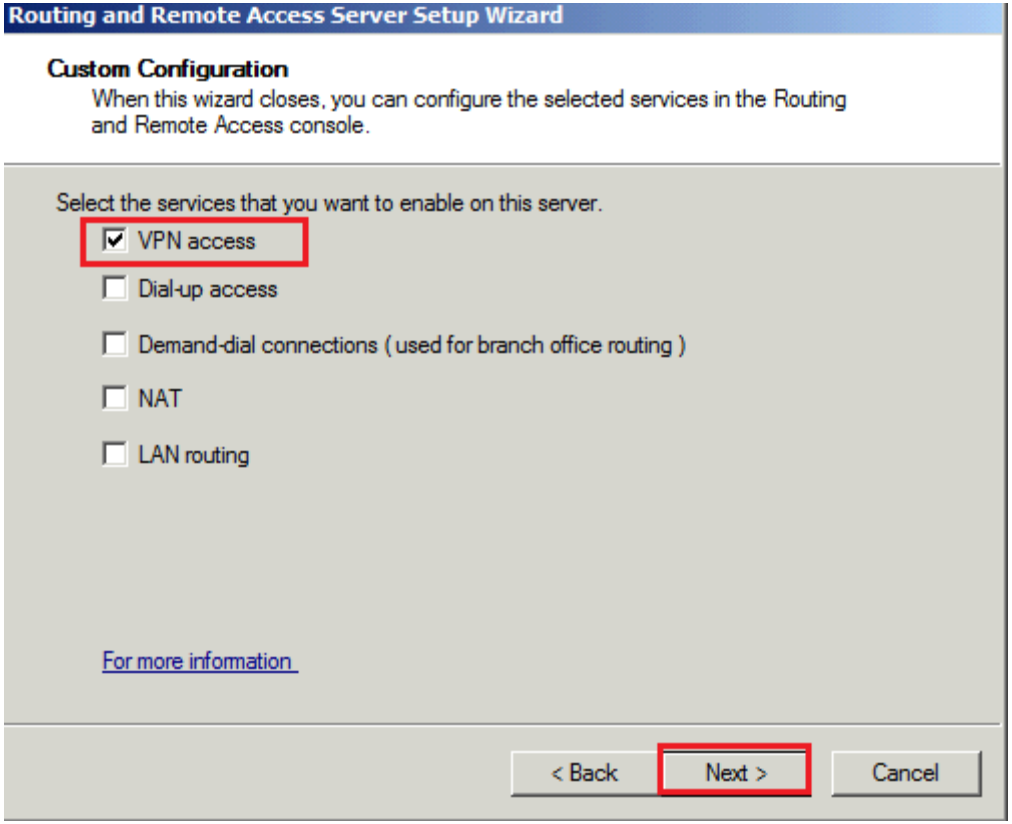
Конфигуриране на RRAS



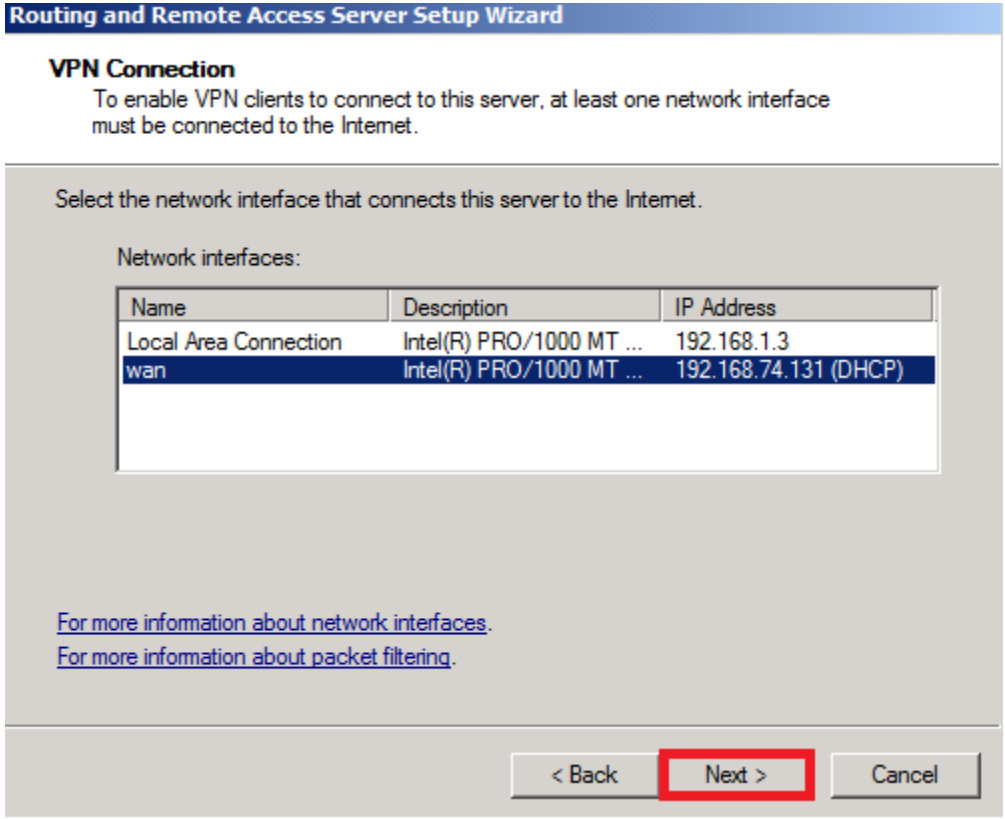
Конфигуриране на RRAS



Конфигуриране за VPN достъп

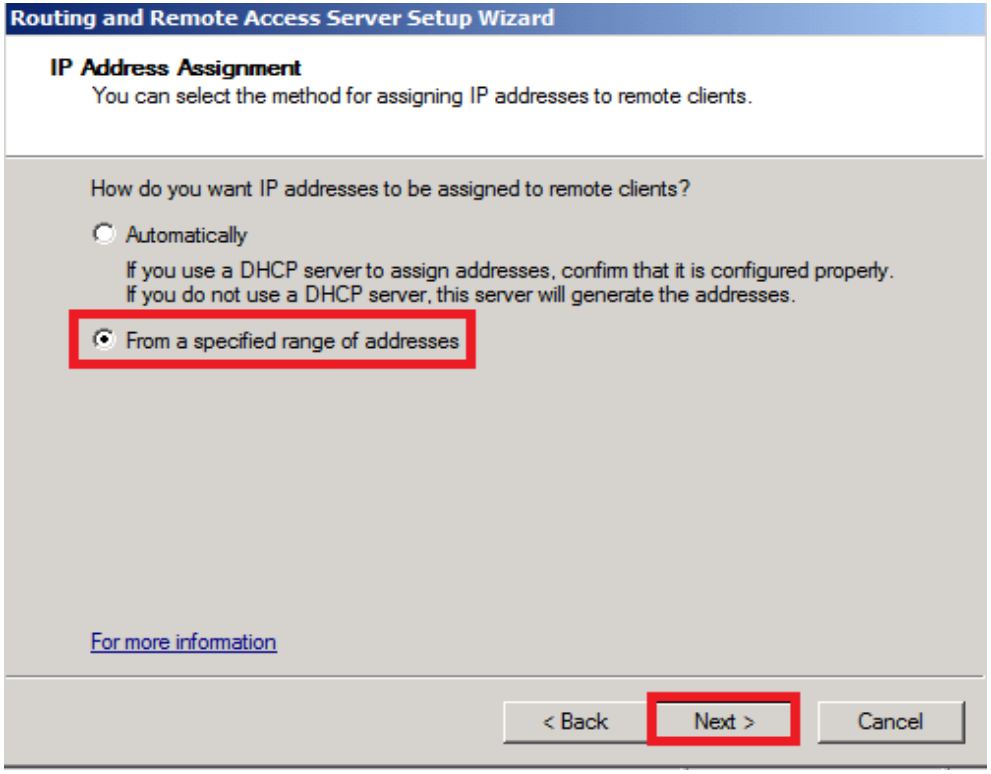


Определяне на външния интерфейс



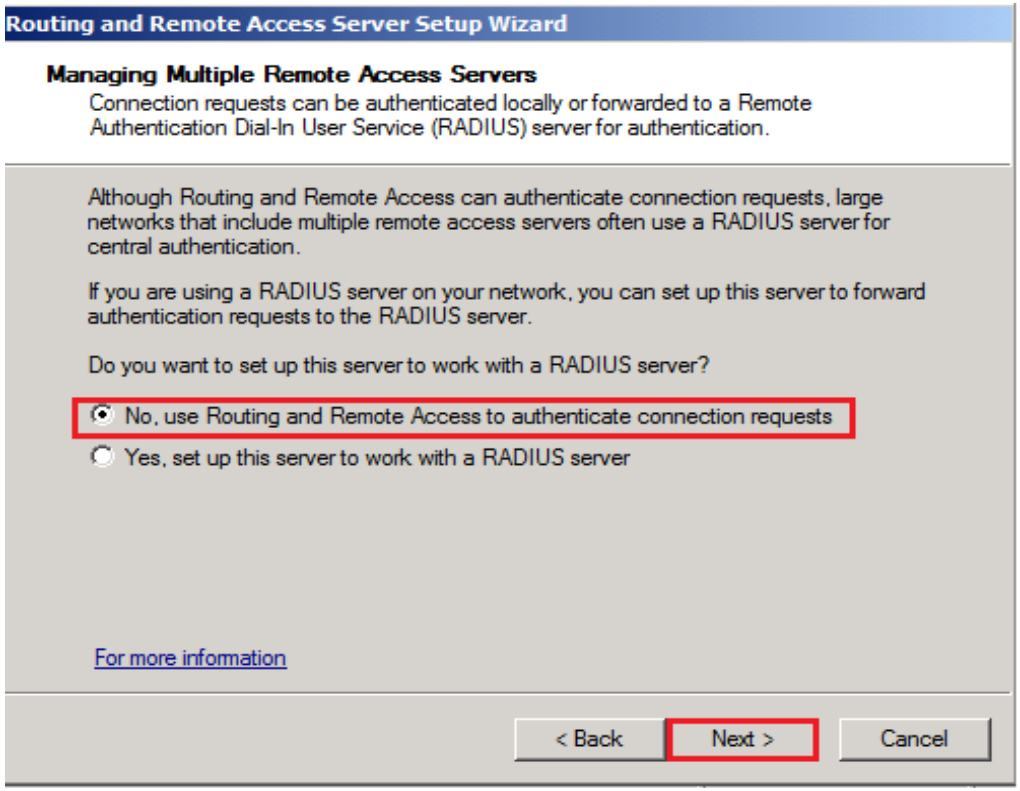
Определяне на начина на адресиране на клиентите

При отсъствие на DHCP сървър



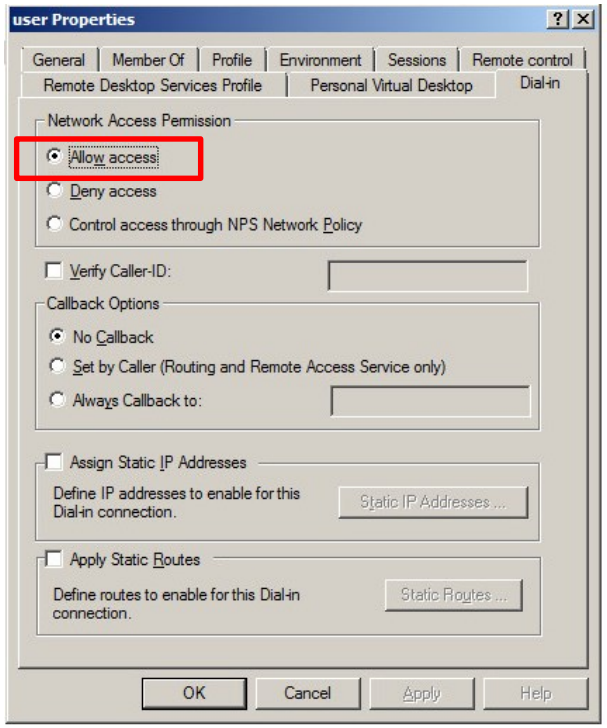
Определяне на начина на автентикацията

При отсъствие на RADIUS сървър

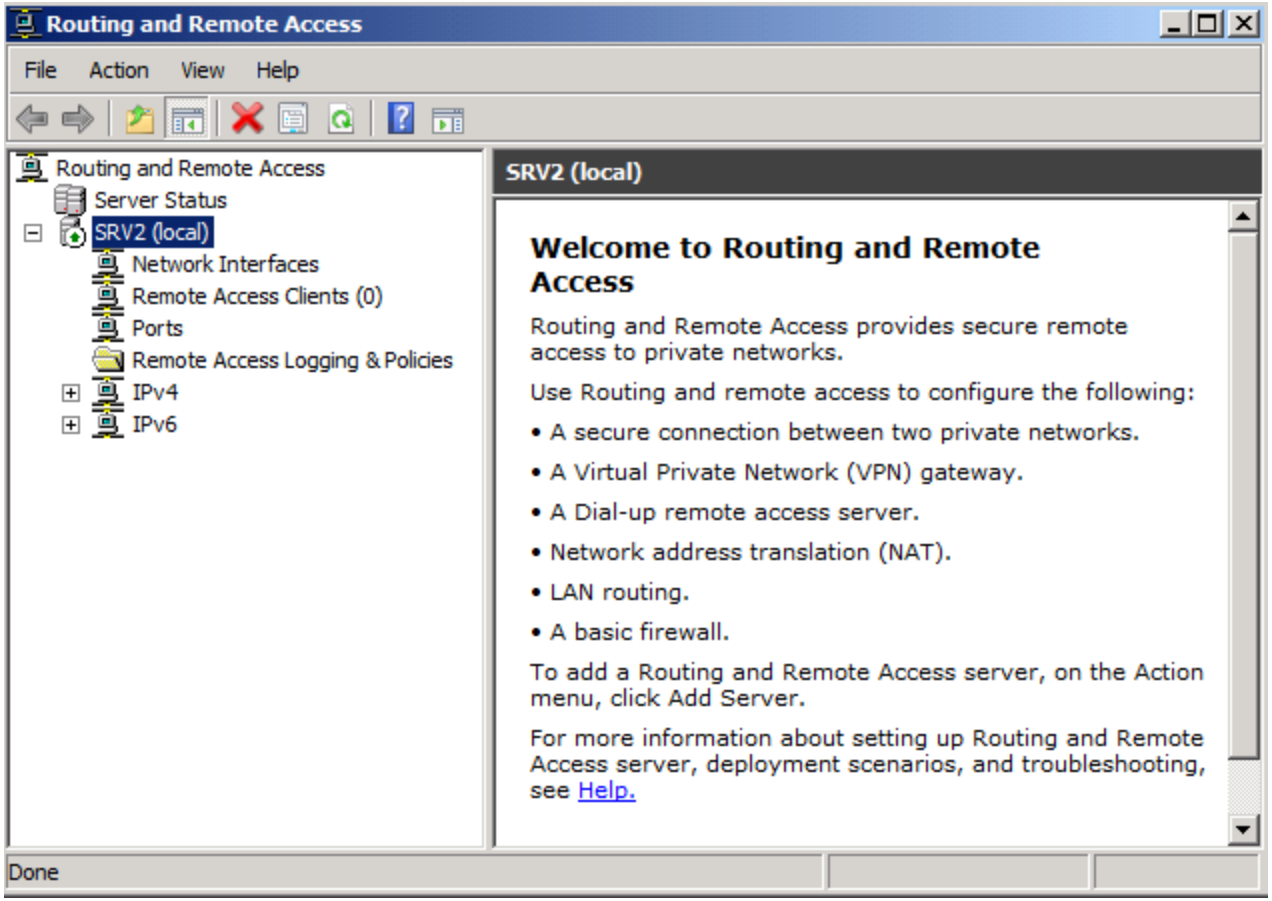


Конфигуриране на достъпа за потребител

От Admin Tools -> Computer Management -> Users

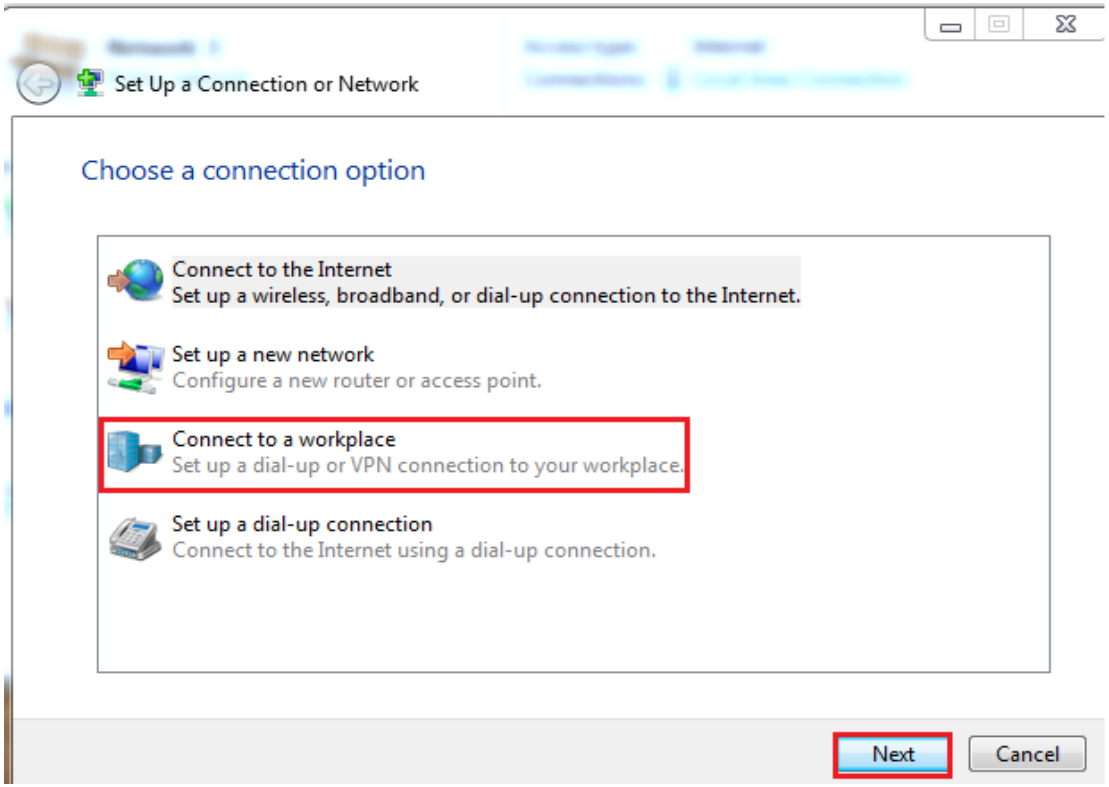


Крайна конфигурация

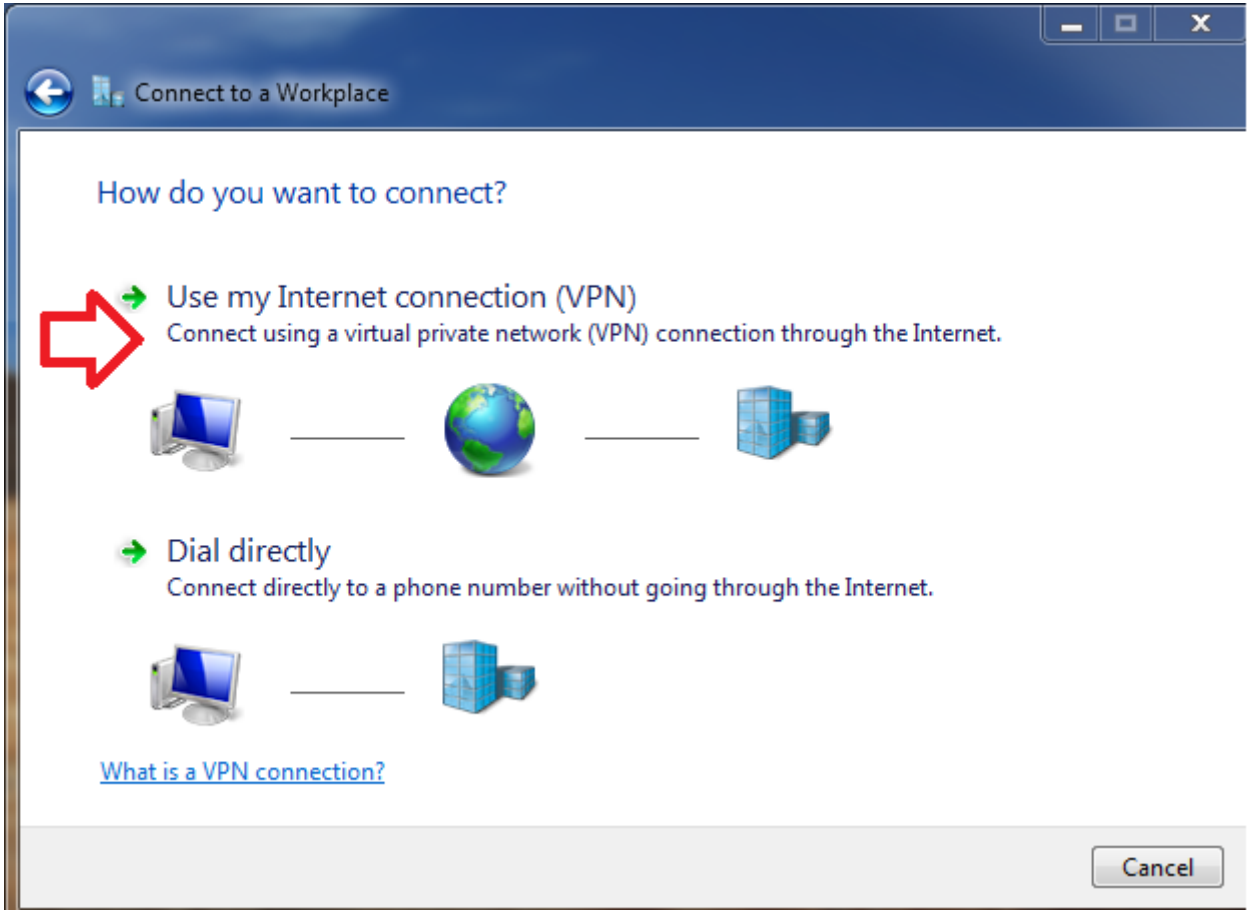


Конфигуриране на Windows 7 клиент за VPN

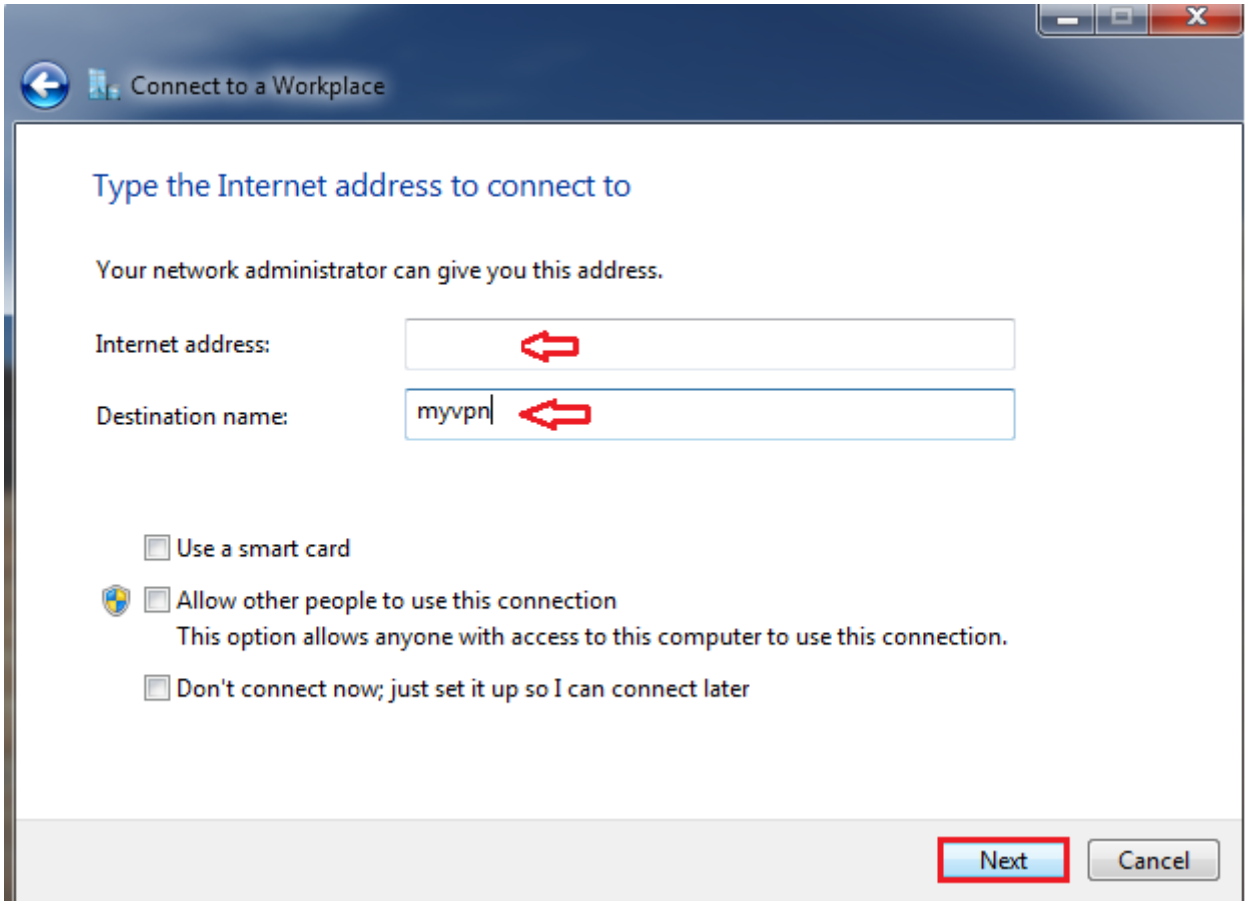
Network and Sharing Center -> Set up a Connection



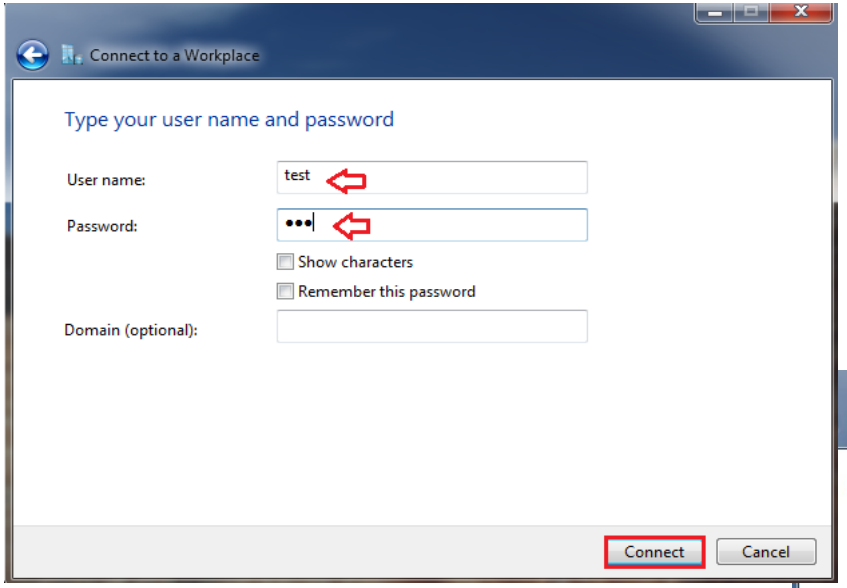
Конфигуриране на Windows 7 клиент за VPN

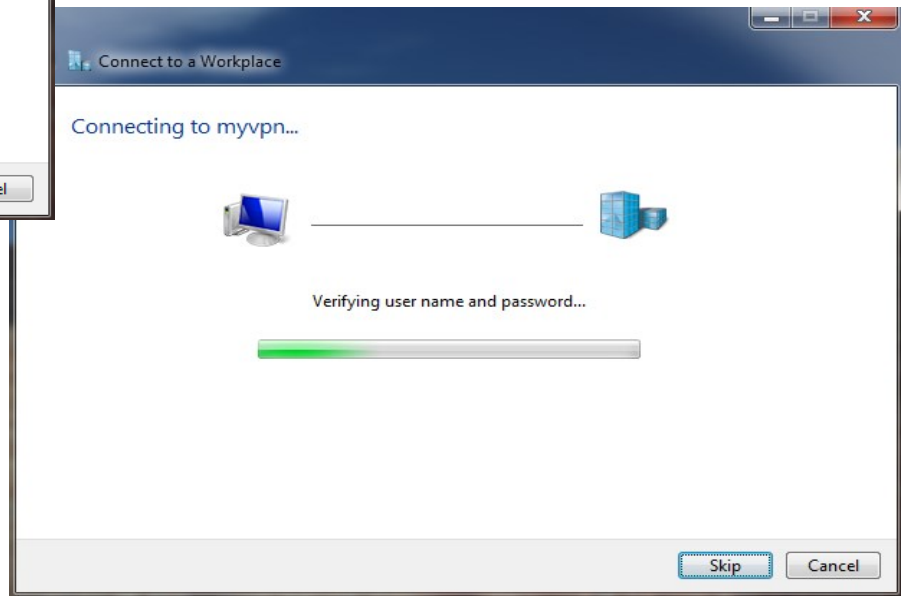


Задаване на параметри



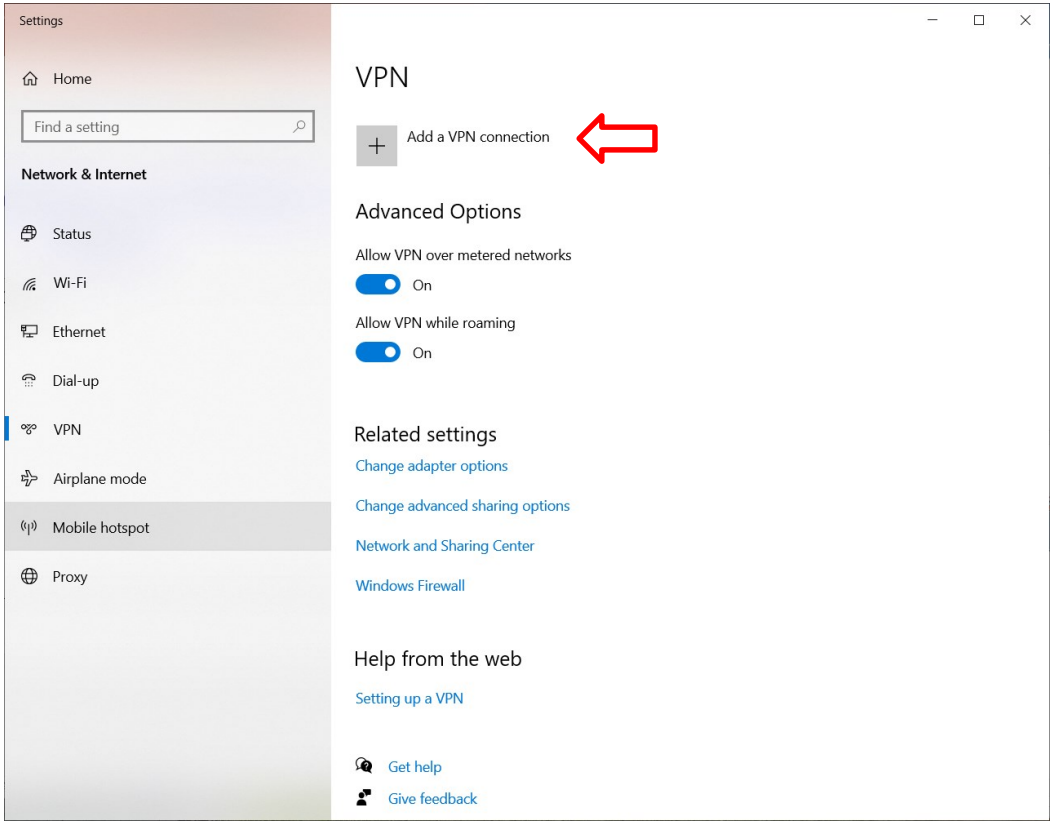
Задаване на кредениціали



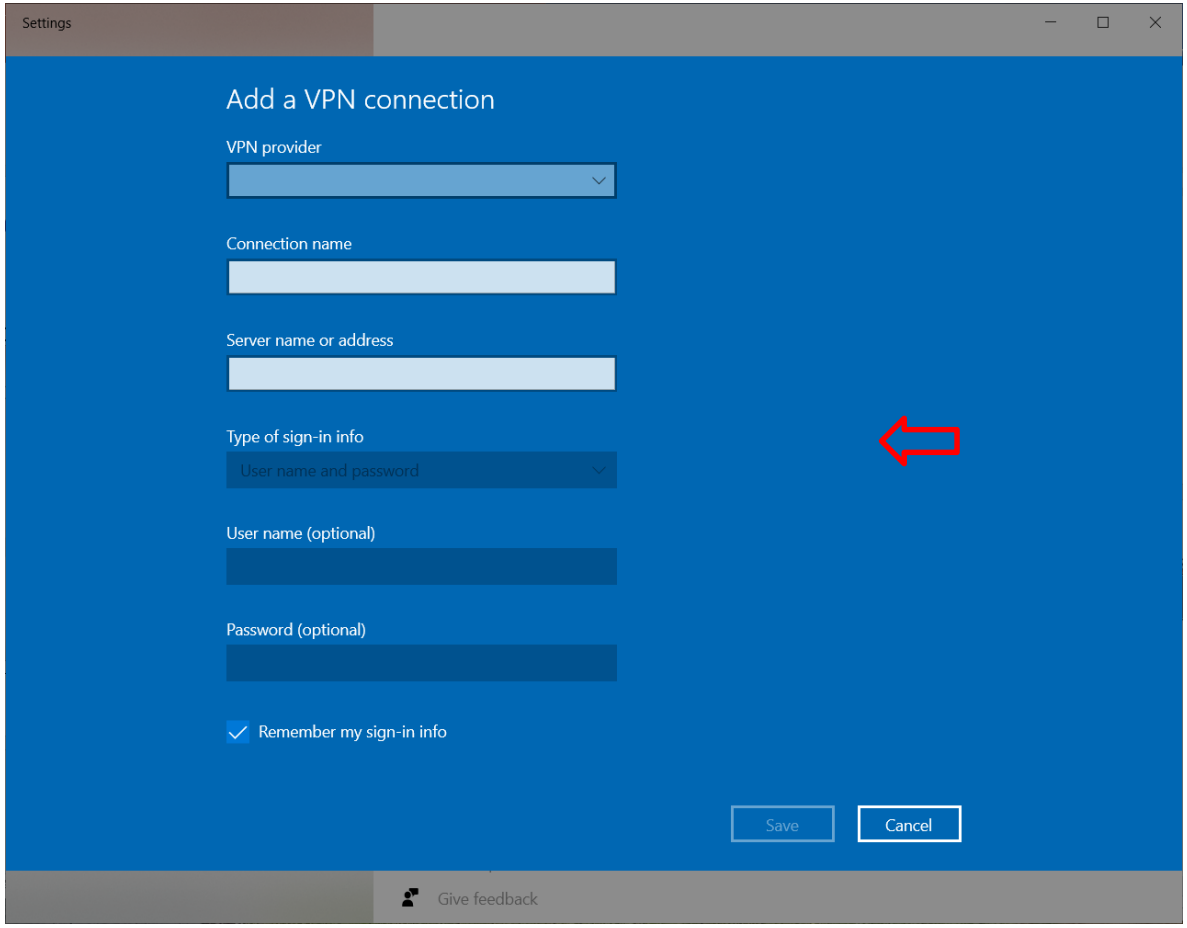


Конфигуриране на Windows 10 клиент

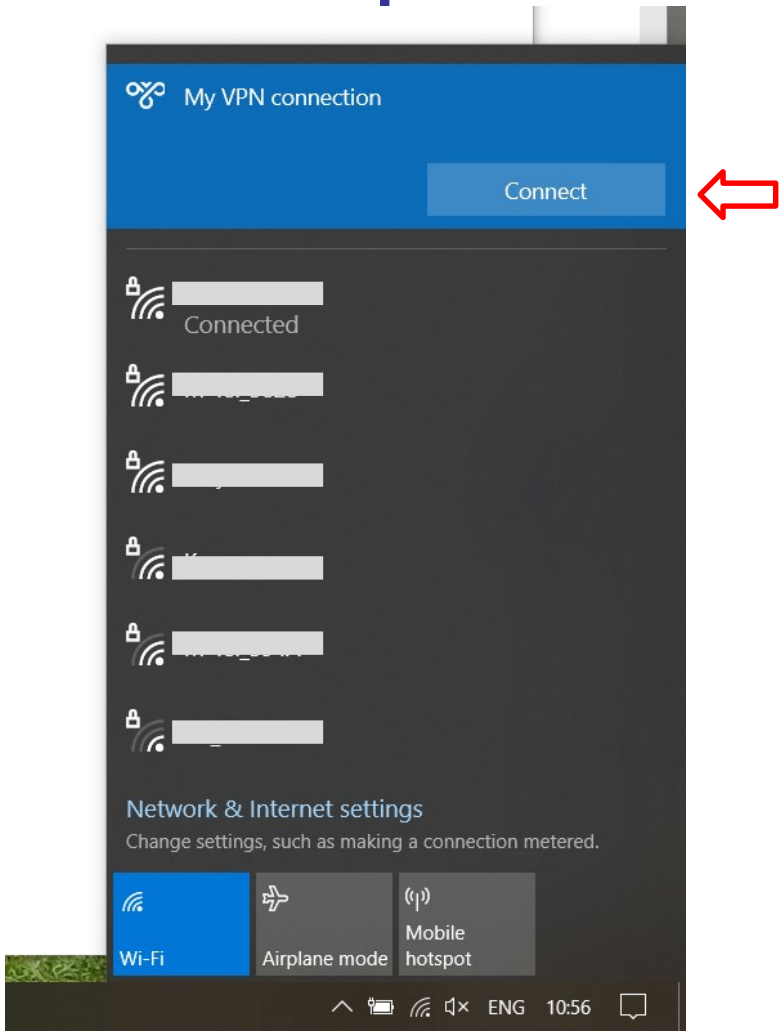
Search - > VPN settings



Задаване на кредениции



Свързване


My VPN connection
Connect
Connected
Network & Internet settings
Change settings, such as making a connection metered.
Wi-Fi
Airplane mode
Mobile hotspot
ENG
10:56

Въпроси?