VPN. Работа от разстояние

проф. д-р инж. Венета Алексиева,
проф. д-р инж. Христо Вълчанов

Основни моменти

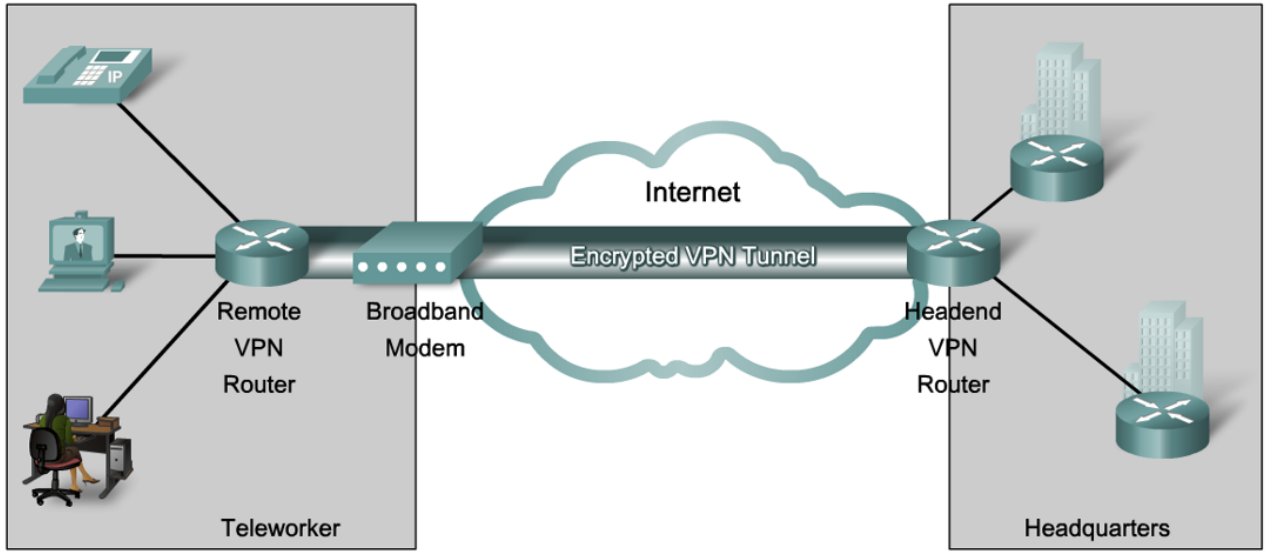
- Работа от разстояние (Teleworker)
- VPN
- GRE
- IPSec
- HMAC

Предимства на работа от разстояние

- За организациите:
  - Непрекъснатост на работата
  - Увеличава отговорността
  - По-сигурен, надежден и управляем достъп до информация
  - На добра цена интегрира данни, глас, видео, приложения
  - Увеличава продуктивността, удовлетвореността от услугата
- Социални предимства:
  - Нараства възможността за обединяване на групи
  - Намалява пътуването и свързания с това стрес

Изисквания

- Осигурява непрекъснатост на работата
- Грижи се за нарастващите нужди на бизнеса от комуникативност
- Secure & reliable достъп до информация
- Cost effective
- Скалируема



Недостатъци

- От гледна точка на работодателя :
  - Трудно следят работните постижения на служителите
  - Необходимо е да се въведе нов стил на управление
- От гледна точка на работниците :
  - Чувство на изолация
  - Бавни връзки
  - Отвличане на вниманието, разсейване

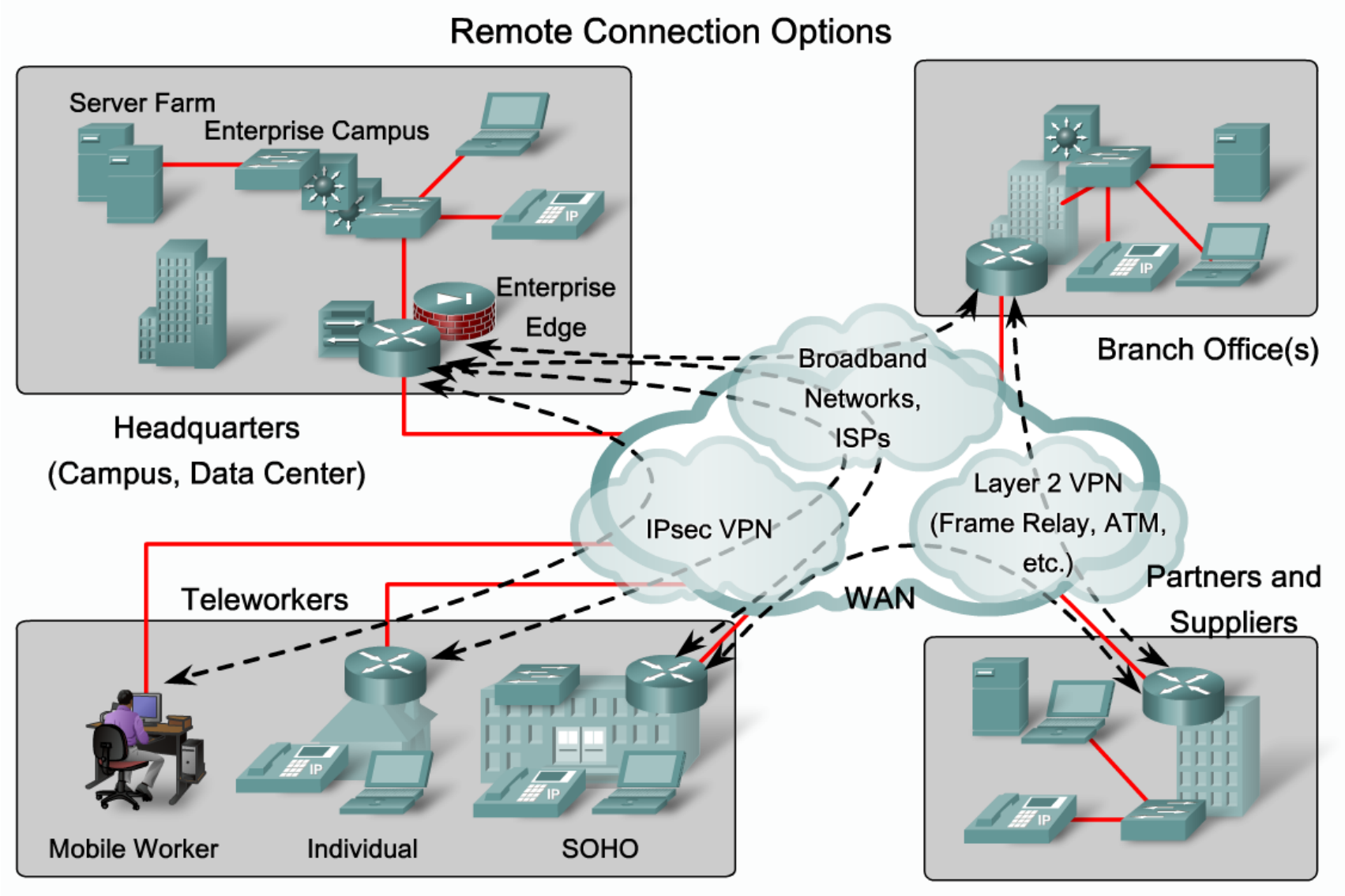
Технологии за работа от разстояние

- Broadband връзки - високоскоростен пренос на услуги: данни, глас и видео по Интернет и други мрежи.
- IPsec VPN мрежи
- Традиционните частни WAN Layer 2 технологии - Frame Relay, ATM и наети линии

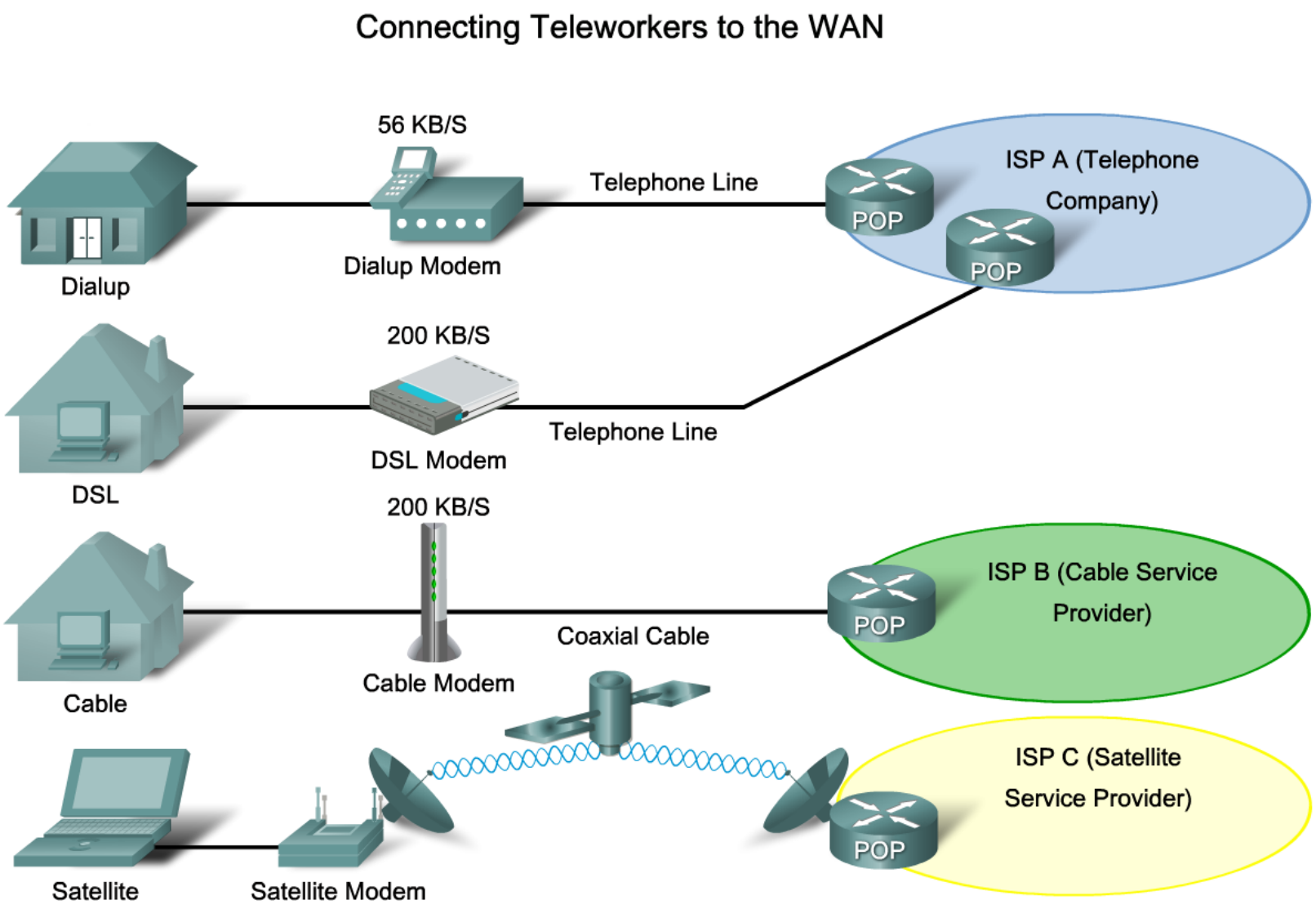
Компоненти

- Компоненти в дома - лаптоп или настолен компютър, широколентов достъп (кабел, DSL, WiFi) и VPN рутер или VPN клиентски софтуер, инсталиран на компютъра.
- Компоненти във фирмата - VPN рутери, VPN концентратори, устройства за сигурност, автентификация.

Технологии за отдалечен достъп

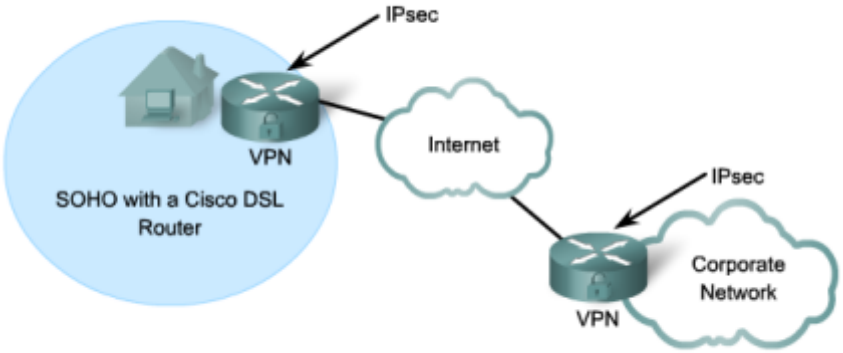


Broadband услуги

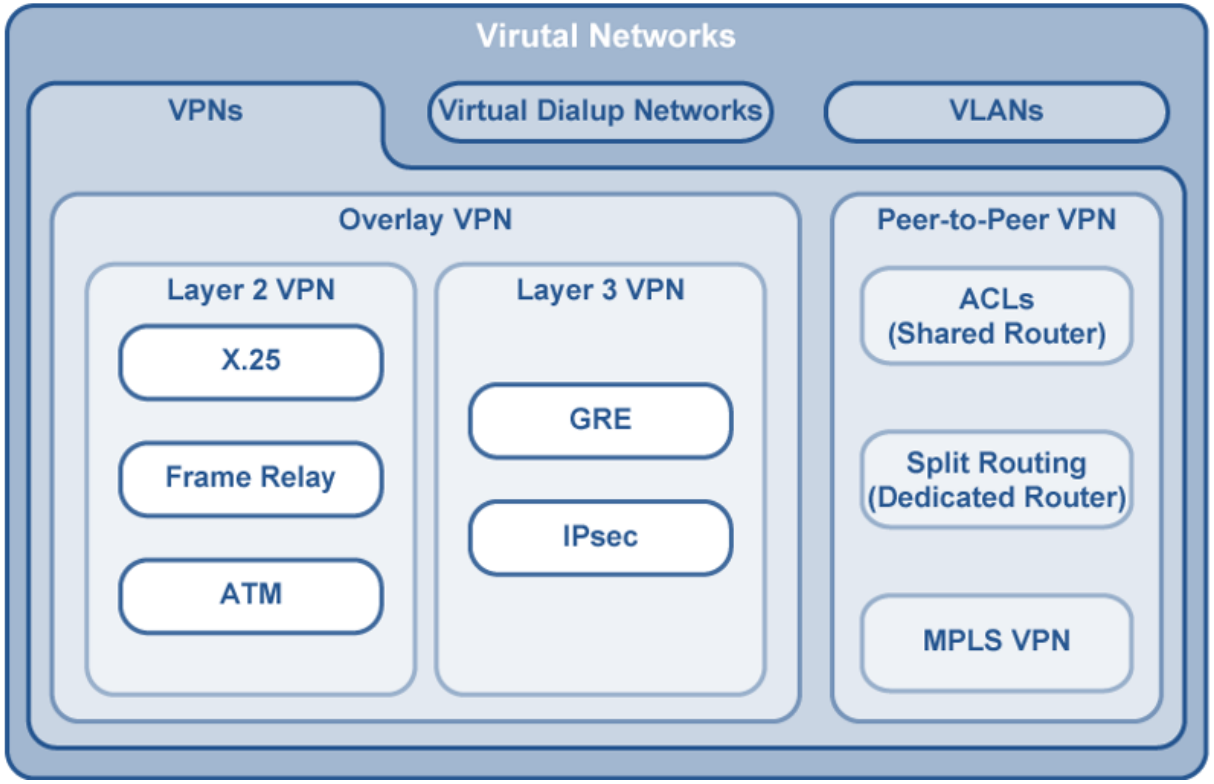


VPN

- Частна мрежа чрез публична мрежа
- Използва се вместо наета линия
- Ползи:
  - Съвместим с broadband технологиите
  - Намалява разходите
  - Сигурност
  - Скалируемост



Видове VPN



- Overlay VPNs: технологии като X.25, Frame Relay, ATM за Layer 2 Overlay VPN и Generic Routing Encapsulation (GRE) и IPsec за Layer 3 Overlay VPN.
- Peer-to-peer VPN: реализира се с отделни рутери за всеки клиент или с MPLS VPN технологията.

Overlay VPNs

- Layer 1 Overlay VPN
  - Остаряла и извън употреба.
- Layer 2 Overlay VPN
  - Традиционна комутирана WAN
  - Внедрено с X.25, Frame Relay, ATM и SMDS
  - ISP отговаря за транспортирането на фреймове от слой 2
  - Клиентът е отговорен за всички по-високи нива
- Layer 3 Overlay VPN
  - ISP мрежата е невидима за клиентските рутери
  - Използва IP тунелиране
  - ISP осигурява пренос на данни point-to-point между сайтовете на клиентите

VPN типове

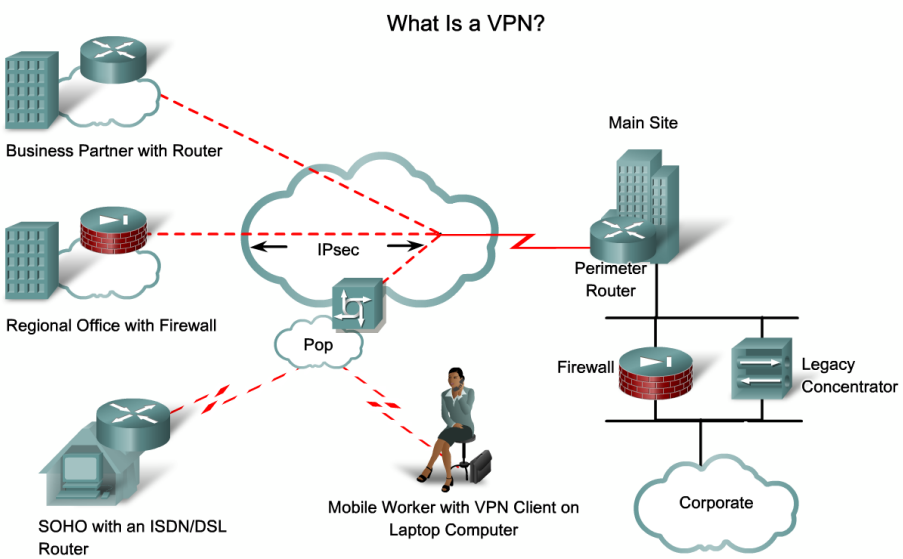
- Site-To-Site
- Remote-Access
- SSL VPNs

VPN Решения

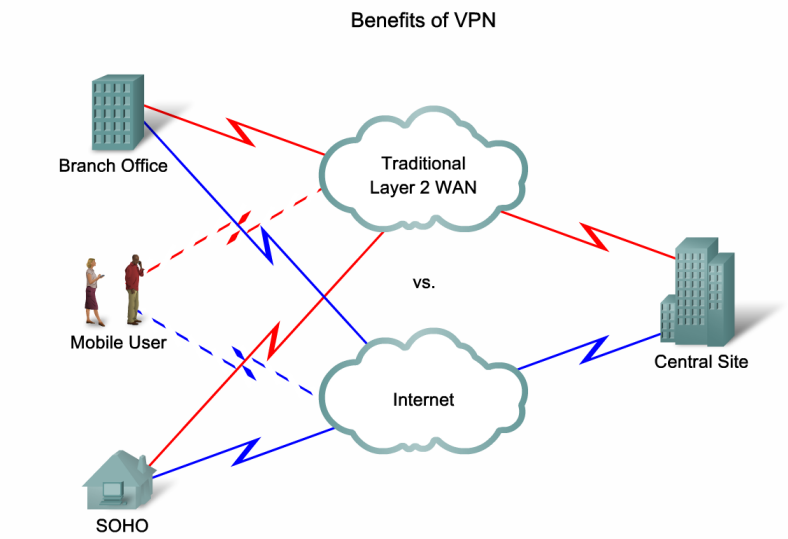
- Cisco VPN рутер
- Cisco PIX
- Cisco ASA
- Cisco VPN концентратор
- SOHO рутер

VPN на слой 3

- Generic Routing Encapsulation GRE (point-to-point)
- MPLS (any-to-any)
- IPSec (point-to-point)

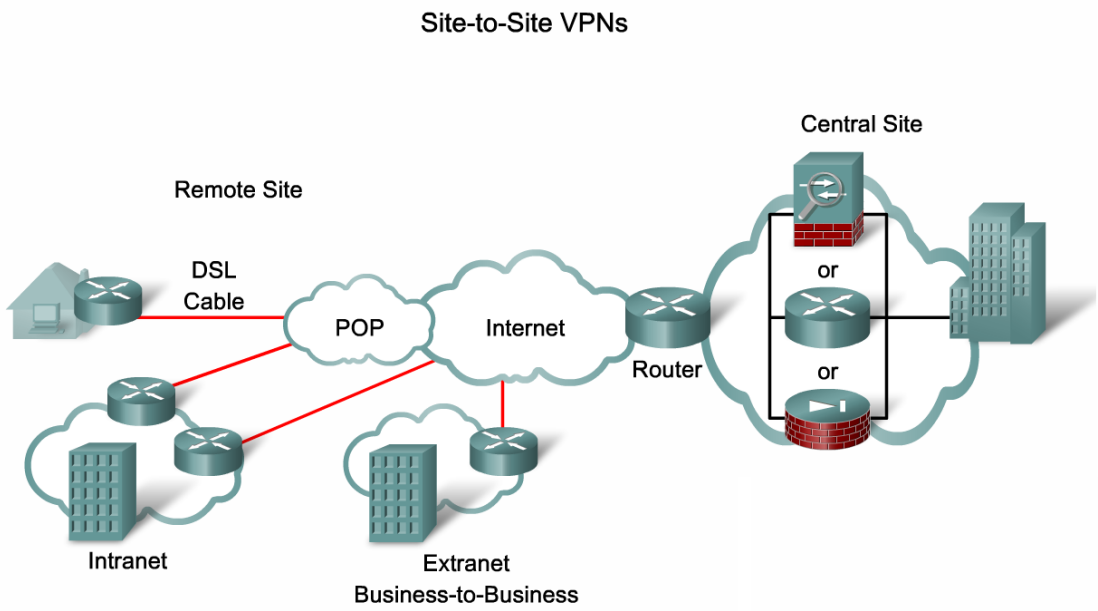


- Virtual: Information within a private network is transported over a public network.
- Private: The traffic is encrypted to keep the data confidential.

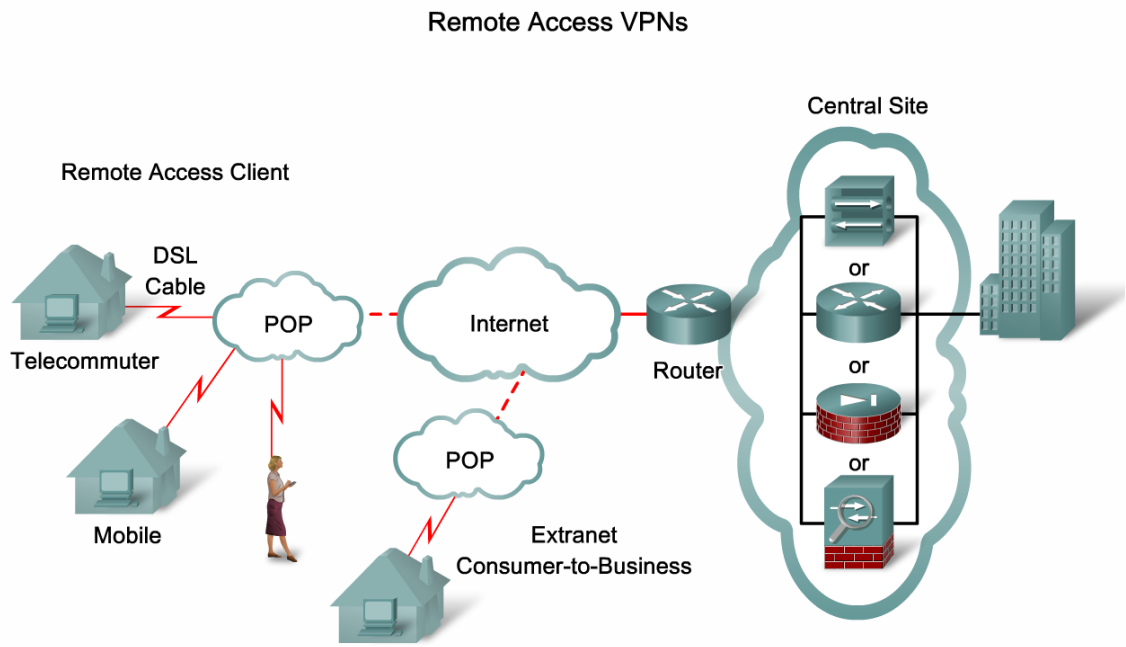


Compared to leased line options, VPN benefits include cost savings, added security, and increased scalability.

Site-to-site VPNs и remote-access VPNs

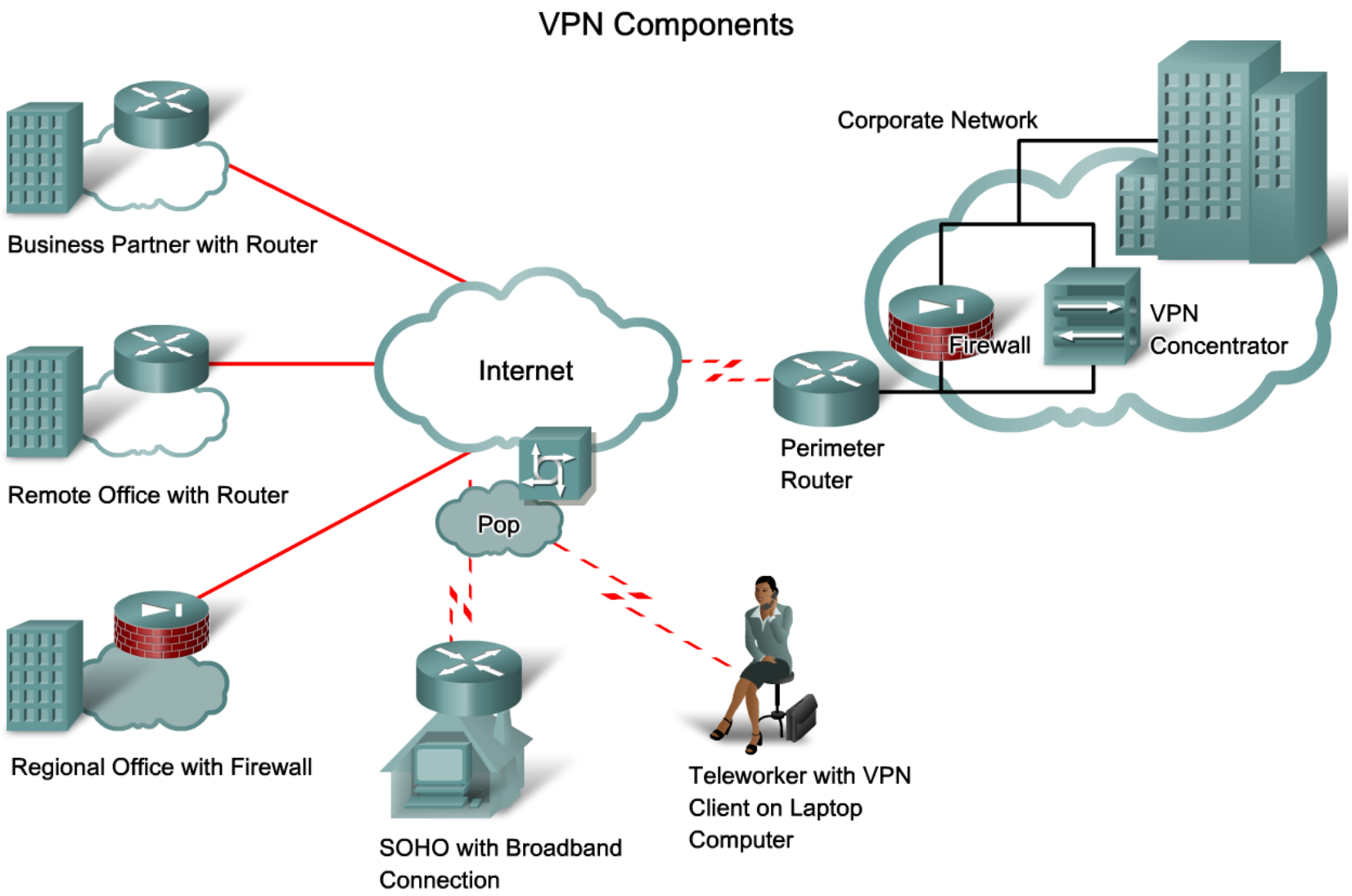


Site-to-site VPNs are extensions of the classic WAN.



Remote Access VPNs mark an evolutionary step in dialup and ISDN networks.

Хардуерни и софтуерни компоненти за VPN



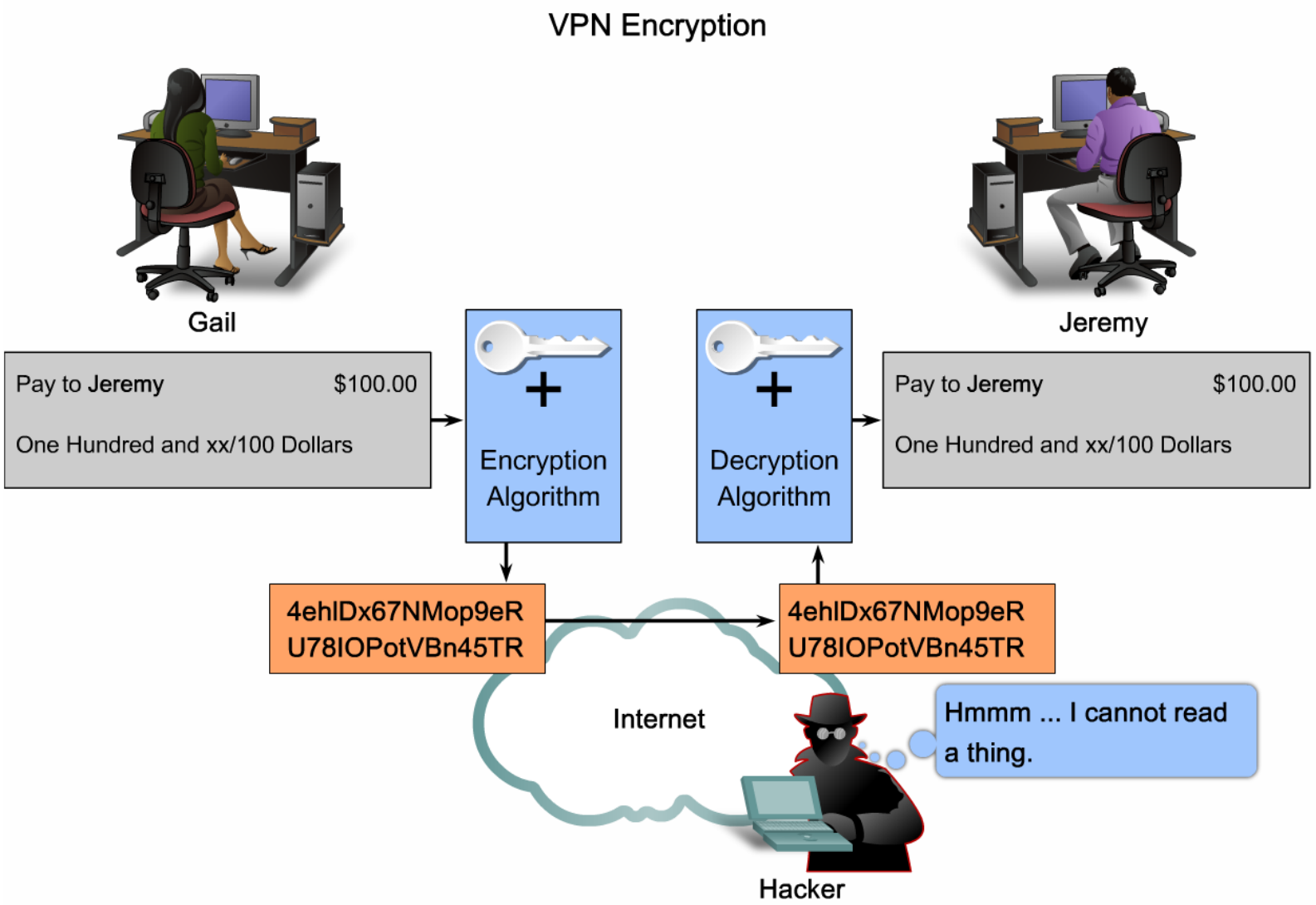
VPN осигуряват защитен отдалечен достъп

- Конфиденциалност на данните – защитава срещу spoofing
- Цялостност на данните- защитава срещу прекьсвания
- Автентикация

VPN тунел

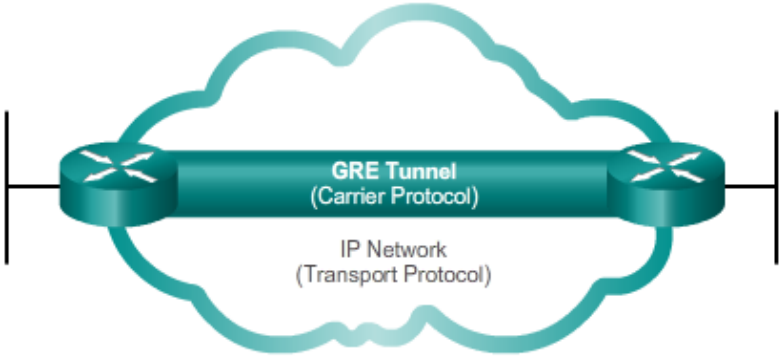
- Carrier protocol
  - Протоколът, по който се пренася информацията – Frame Relay, ATM, MPLS…
- Encapsulation protocol
  - Протоколът-обвивка на оригиналните данни – GRE, IPSec, L2F, PPTP,L2TP…
- Passenger protocol
  - Протоколът, който пренася оригиналните данни – IPv4, IPv6, IPX, Apple Talk

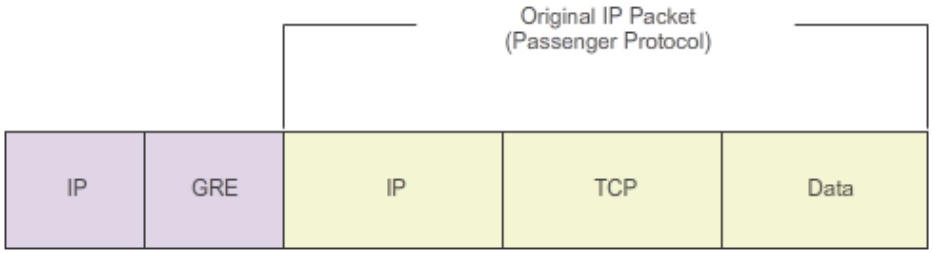
VPN криптиране



Site-to-Site тунел с GRE

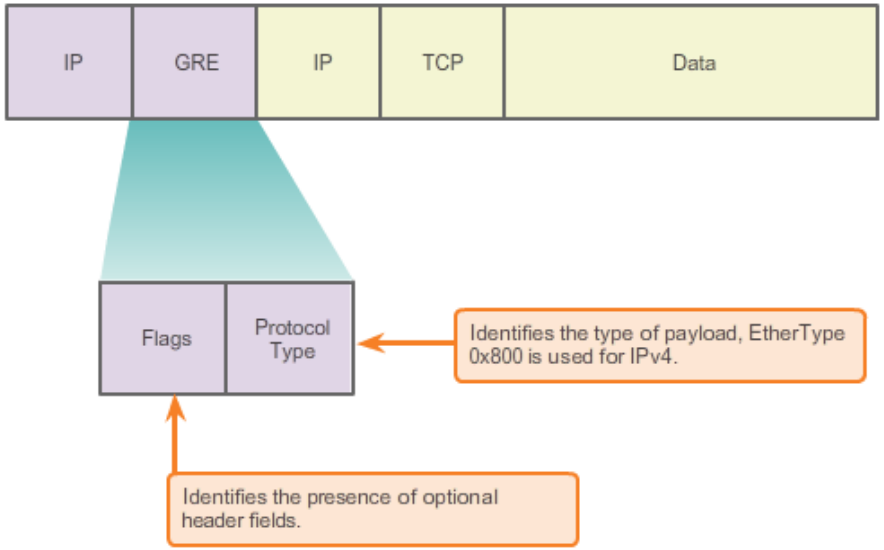
- Generic Routing Encapsulation (GRE)
- Основен, несигурен
- Протокол за site-to-site VPN
- Пренася IPv4, IPv6, AppleTalk, DECnet, IPX
- Създаден от Cisco



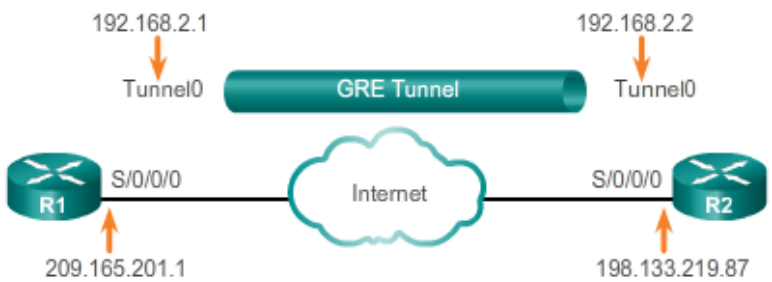


Характеристики на GRE

- По стандарт - RFC 2784
- Типовете протоколи, които може да пренася са в RFC 1700 - "EtherTypes".
- GRE няма механизми за flow-control.
- GRE няма механизъм за security.



Конфигуриране на GRE



R1 configuration:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

1. **interface tunnel** *number*
2. Посочва се IP адрес на сорса на тунела.
3. Посочва се IP адрес на дестинацията на тунела.
4. Конфигурира се IP адрес за tunnel интерфейса.
5. (Optional) Посочва се режим за тунела - GRE е по default за Cisco.

Internet Protocol Security (IPsec)

- Всички реализации на IPsec имат хедър на 3 слой в чист текст, за да няма проблеми с маршрутизацията.
- IPsec е комплект от отворени стандарти, който е алгоритмично-независим.
- IPsec осигурява конфиденциалността на данните, целостта на данните и удостоверяване на произхода.
- IPsec действа в мрежовия слой, защитавайки и удостоверявайки IP пакети.

IPsec функции

- Конфиденциалност
- Интегритет
- Автентикация
- Защита срещу отговор

Confidentiality

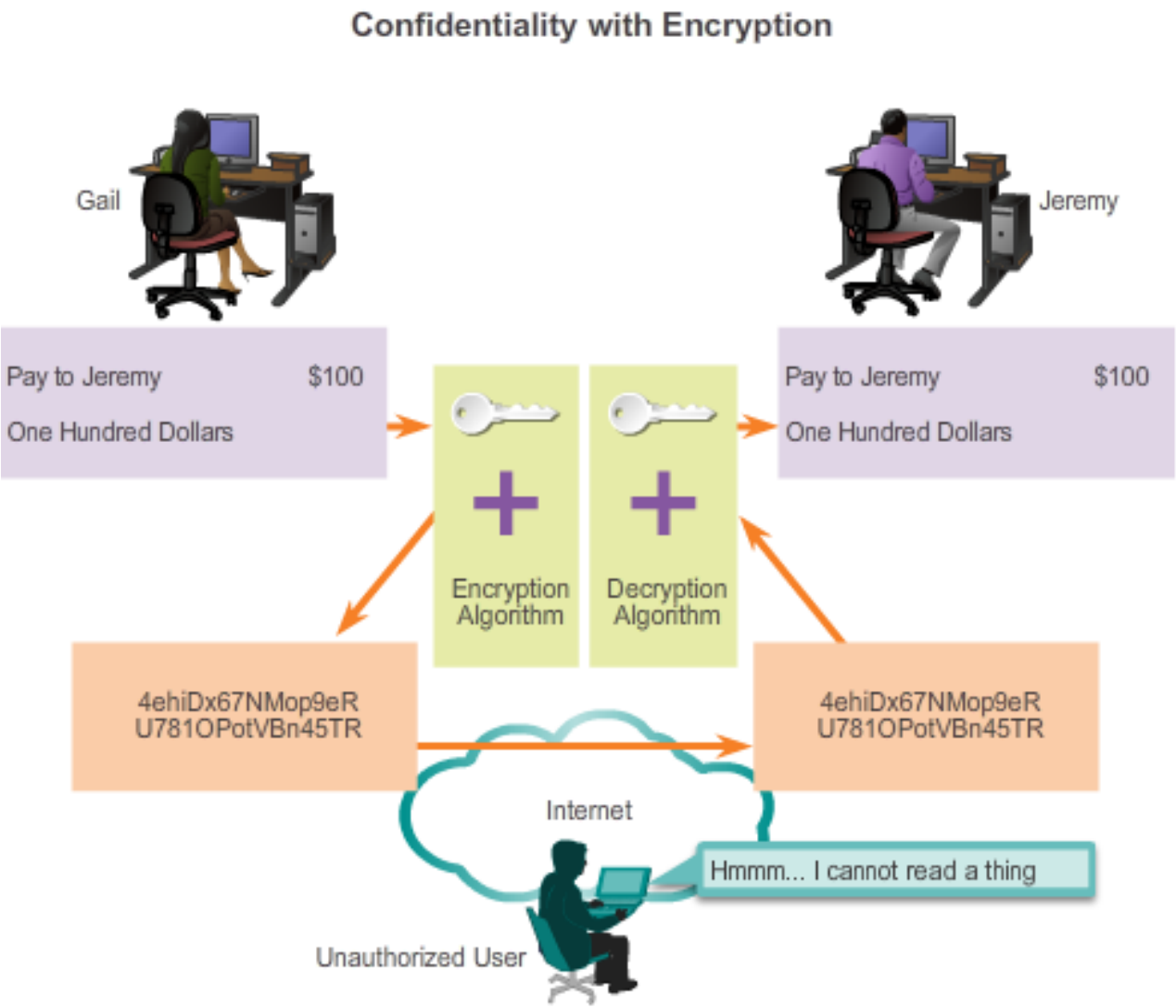
Data Integrity

Authentication

16	24	32 bit
Security Association Identifier (SPI)		
Sequence Number		
Payload Data (Variable Length)		
Padding (0-255 Bytes)		
	Pad Length	Next Header
Authentication Data (Variable)		

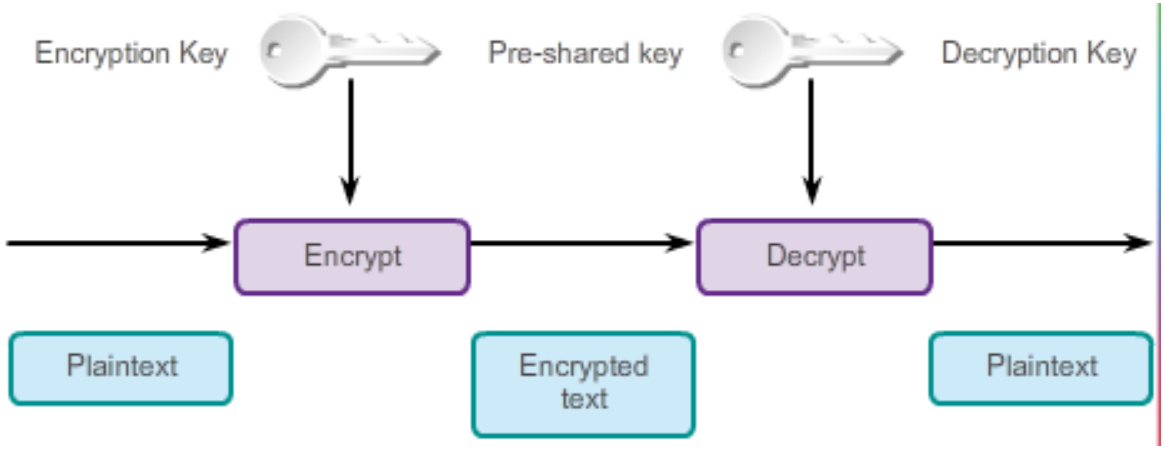
Anti-Replay Protection

Конфиденциалност

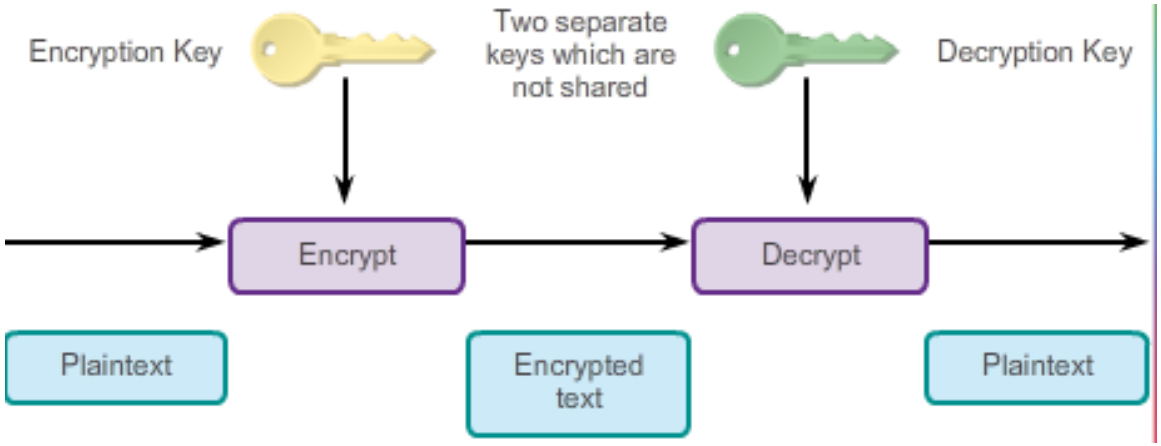


Симетрично и асиметрично криптиране

- Симетричен

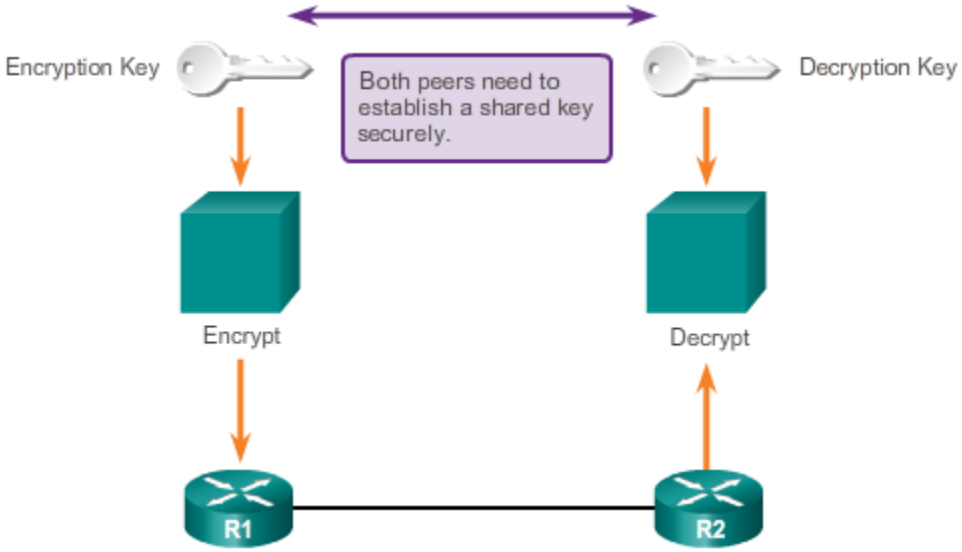


- Асиметричен



Интегритет

- Diffie-Hellman (DH) не е механизъм за криптиране и обикновено не се използва за криптиране на данните.
- Това е метод за сигурно обменяне на ключовете за криптиране на данните.
- (DH) алгоритмите позволяват двете страни да създадат общ таен ключ, който се използва от криптиращите и хеш алгоритми.
- Създаден от Whitfield Diffie и Martin Hellman през 1976г.



Симетричен и асиметричен ключ

- DH е първата система за използване на публичен ключ или асиметрични криптографски ключове. Днес DH е част от стандарта IPsec.
- Протоколът OAKLEY използва алгоритъм DH. OAKLEY се използва от протокола IKE, който е част от Internet Security Association и протокола за управление на ключове.
- Алгоритми за криптиране, като например DES, 3DES и AES, както и MD5 и SHA-1 хеш алгоритми изискват симетричен, споделен таен ключ за извършване на криптиране и декриптиране.

Интегритет с Hash алгоритъм

- Целостта и автентичността на VPN трафика се обработват от хеш алгоритми.
- Hash също се именова message digest.
- Хеш е число, което се генерира от текстов низ. Генерира се с помощта на формула така, че е малко вероятно друг текст да произведе същата хеш стойност.
- Хеш-ът е по-малък от самия текст.

Принцип на работа на Hash-а

- Оригиналният подател генерира хеш на съобщението и го изпраща със самото съобщение.
- Получателят анализира съобщението и хеш-а, изчислява друг хеш от полученото съобщение и сравнява двата хеш-а. Ако те са едни и същи, получателят може да бъде сигурен в цялостта на оригиналното съобщение.

HMAC

- VPNs използват код за удостоверяване на съобщение за проверка на целостта и автентичността на съобщението, без да използват каквито и да било допълнителни механизми.
- **Hash-based Message Authentication Code (HMAC)** има два параметъра - за въвеждане на съобщение и таен ключ, който е известен само на подателя на съобщението и предварително известни получатели.

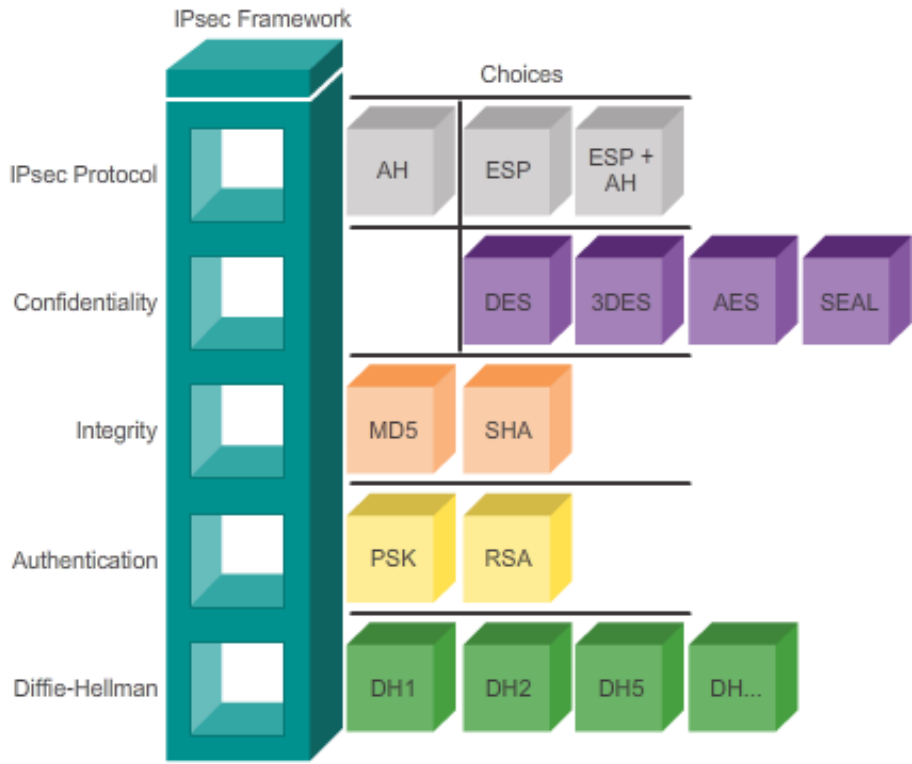
Алгоритми HMAC

- MD5 - Използва 128-битов споделен таен ключ . Съобщението и ключът се комбинират чрез Hash алгоритъм HMAC-MD5. Резултатът е 128-битов Hash. Hash е приложен към оригиналното съобщение и се изпраща до отдалечения край.
- SHA - SHA - 1 използва 160-битов секретен ключ. Съобщението с променлива дължина и 160-битовия споделен таен ключ се комбинират чрез Hash алгоритъм HMAC-SHA1. Резултатът е 160-битов Hash. Hash е приложен към оригиналното съобщение и се изпраща до дестинацията.
- Cisco IOS поддържа също и 256-битови, 384-битови и 512-битови SHA реализации.

Автентикация

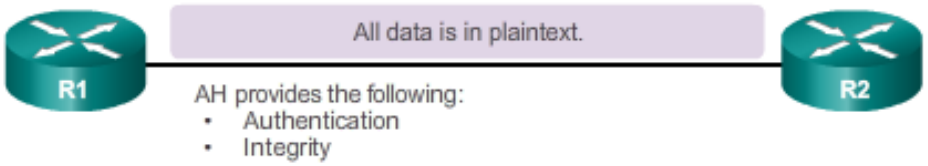
- PSK - таен ключ , който се поделя между двете страни с помощта на сигурен канал, преди да трябва да се използва. PSKs използват симетрични криптографски алгоритми.
- RSA подписи - Цифровите сертификати се разменят за удостоверяване на пиъри. Локалното устройство хешира и криптира с неговия личен ключ. В отдалечения край криптирания хеш е разшифрован с помощта на публичния ключ. Ако разшифрования хеш съвпада с преизчисления хеш, подписът е истински.

IPSec

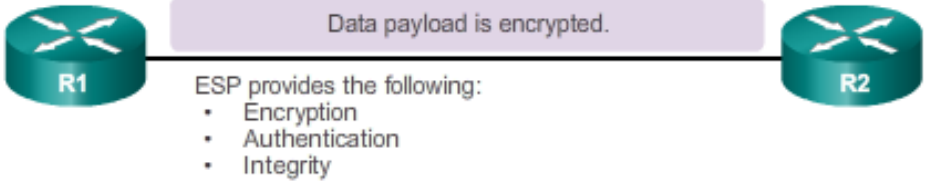


IPsec Protocol Framework

Authentication Header



Encapsulating Security Payload



Remote-access VPNs

Използват се:

- Secure Sockets Layer (SSL)
- IP Security (IPsec)

И двете (IPsec и SSL) VPN технологии предлагат достъп до почти всяко приложение, мрежа или ресурс.

SSL VPN предлагат лесна връзка от не-фирмени настолни компютри, малко или никаква поддръжка на десктоп софтуер и потребителски-персонализирани уеб портали при влизане.

Сравнение на IPSec и SSL

	SSL	IPSec
Приложения	Web приложения, споделяне на файлове, e-mail	Всички IP-базирани приложения
Криптиране	Средно до силно Ключ:40-256 bits	силно Ключ:56-256 bits
Автентикация	Средна One-way/two way автентикация	Силна two way автентикация със споделен ключ или цифров сертификат
Сложност	Ниска само web браузър	Средна
Опции за връзка	Свързва всякакви устройства	Свързва само устройства със специфична конфигурация

Конфигуриране на Site-to-Site VPNs

- Да се позволи VPN traffic с ACL , който позволява ESP (50), AHP (51), ISAKMP (UDP 500) трафик
- Да се опишат ISAKMP политиките - encryption, hash, Diffie-Hellman
- Да се избере платформа - ESP или AH
- Да се създаде ACL стандартен или разширен, за да се защити трафика
- Да се създаде crypto map

Въпроси ?

Благодаря за вниманието !