PROTOKOL IPSEC

Přehled vlastností protokolu IPSec

- IPSec – rámec otevřených standardů pro zajištění bezpečné komunikace přes sítě IP prostřednictvím využívání kryptografických bezpečnostních služeb
- Pracuje na síťové vrstvě referenčního modelu síťové architektury ISO/OSI
- Vyvinut primárně pro IPv6, kde bývala jeho podpora povinná každým uzlem – už není
- Implementován i pro IPv4
- Nelze použít pro přenos dat utajovaných dle zákona

Služby a složení protokolu IPSec

- IPSec poskytuje následující služby:
  - Integrita v prostředí nespojované komunikace
  - Ověřování původu dat
  - Ochrana proti opakovaným vysíláním téhož paketu
  - Důvěrnost (šifrování)
- Protokoly tvořící základ IPSec
  - Authentication Header (AH)
  - Encapsulated Security Payload (ESP)
  - Internet Key Exchange (IKE)

Historie

- První popis v RFC 1825, rok 1995
- První implementace v BSDI, rok 1995

- Současný stav
  - RFC 2401 – přehled architektury (1998)
  - RFC 2402 – popis protokolu AH (Authentication Header)
  - RFC 2406 – popis protokolu ESP (Encapsulation Security Payload)
  - RFC 2408 – popis protokolu IKE (Internet Key Exchange) – správa klíčů

Výhody a nevýhody IPSec

Výhody

- Transparentnost (netřeba modifikovat protokoly vyšších vrstev)
- Škálovatelnost (od jednotlivých PC po velké sítě)
- Aplikační nezávislost, lze zabezpečit libovolný protokol využívající protokol IP (telnet, ftp)
- Široká podpora mezi výrobci

Nevýhody

- Složitost – citlivost na některé útoky
- Větší režie, vadící u krátkých paketů (např. zvuk)

Protokol AH (Authentication Header)

- Protokol AH zajišťuje tyto funkce
  - Integritu dat
  - Autentizaci každého IP paketu
  - Ochranu před opakovaným vyslání téhož paketu
- Vlastnosti
  - Nešifruje data, ale nelze je změnit
  - IP záhlaví i data jsou podepsány
  - Zabraňuje útoku typu podvržení adresy sledováním pořadových čísel
  - Používá algoritmy HMAC (Hash Message Authentication Code)
  - Komunikující strany musí sdílet tajný klíč

Protokol ESP (Encapsulated Security Payload)

- Protokol ESP poskytuje
  - Důvěrnost dat
  - Určitá důvěrnost toku dat (maskování)
  - Volitelně podporu autentizace - AH
- Vlastnosti
  - Lze použít souběžně s AH
  - Podporuje řadu šifrovacích algoritmů, módů, atd.
    - DES, 3DES, RC5, IDEA, CAST a další

Protokol IKE (Internet Key Exchange)

- Protokol IKE
  - Kryptografická infrastruktura zajišťující vyjednávání o výměně klíčů
  - Ustaví Security Associations (SAs) mezi IPSec partnery
  - Autentizuje IPSec partnery
- Security Associations (SA) - *jednosměrný* vztah mezi odesílající a přijímající stranou; parametry
  - Security Parameters Index (metoda autentizace)
  - Cílová IP adresa
  - Identifikátor bezpečnostního protokolu (AH či ESP)

Použití protokolů IPSec

- Authentication Header
  - Požaduje se připojení k zaručenému adresátovi
  - Musí být ověřován zdroj dat
  - Data sama o sobě nejsou citlivá, riziko zachycení paketů a potenciální kompromitace je nízké
- Encapsulation Security Payload
  - Utajení přenášených informací
  - Pouze požaduje-li se ochrana dat
- Protokoly AH a ESP současně
  - Musí-li být data chráněna a je nutná autentizace
  - Pokud zvýšená bezpečnost kompenzuje pokles výkonnosti vyplývající z další režie

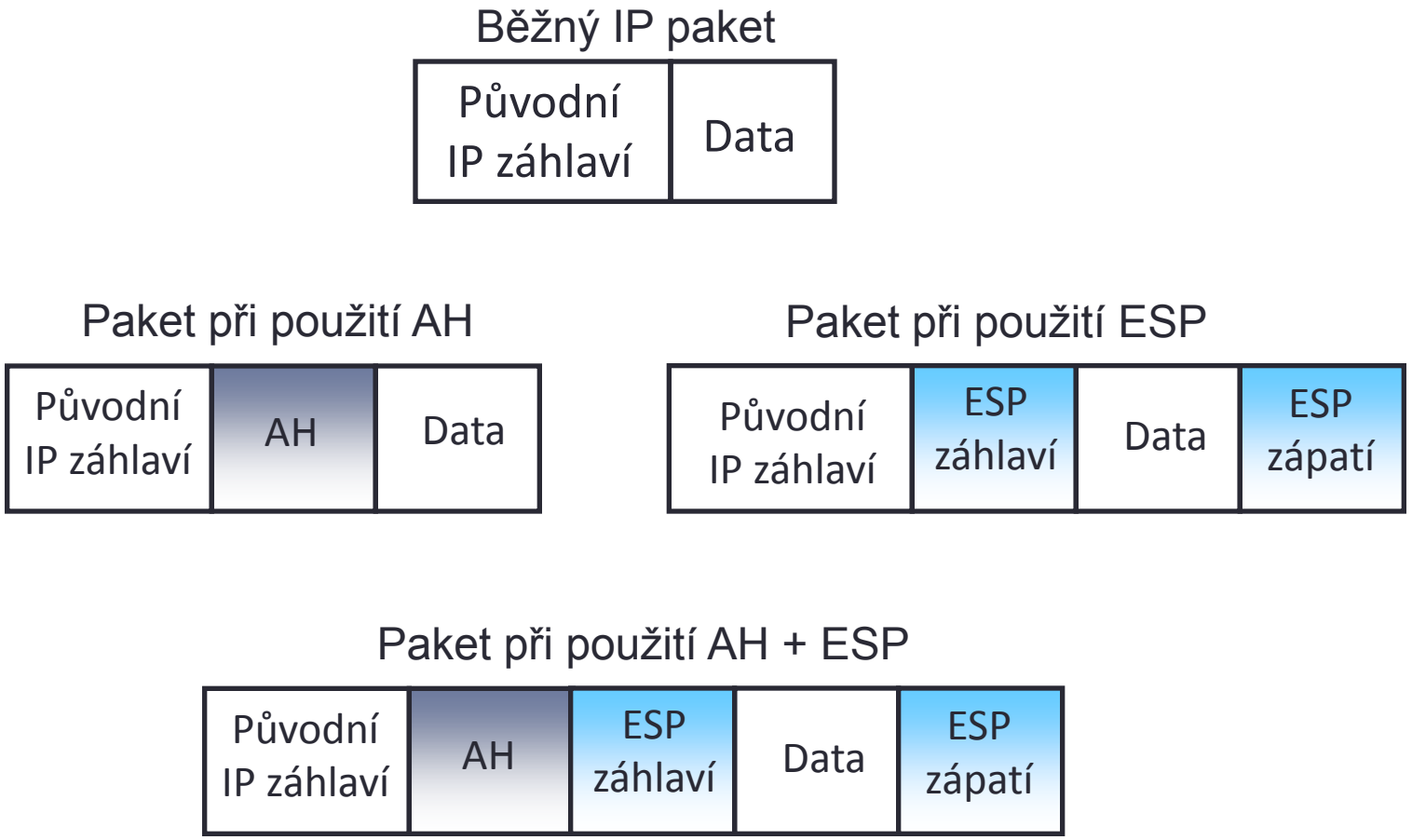
Scénáře nasazení IPSec

- IPSec může být nasazen takto

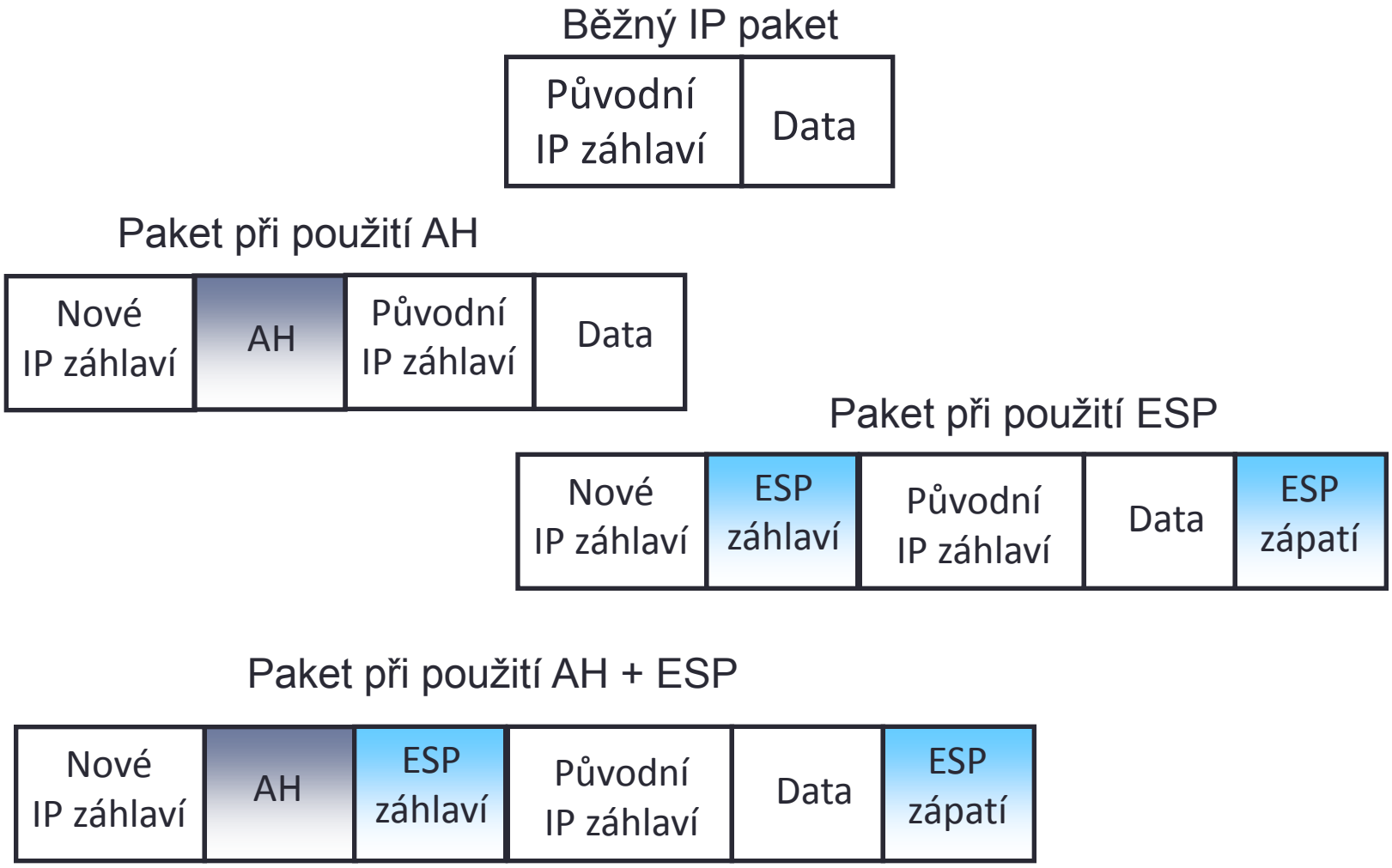
Transportní mód	Ochrana komunikace mezi dvěma koncovými počítači
Tunelovací mód	Ochrana komunikace mezi koncovým počítačem a sítí nebo mezi dvěma sítěmi

- Tři základní varianty konfigurace
  - Host to Host
  - Gateway to Gateway (propojení sítí - tunel)
  - Host to Gateway

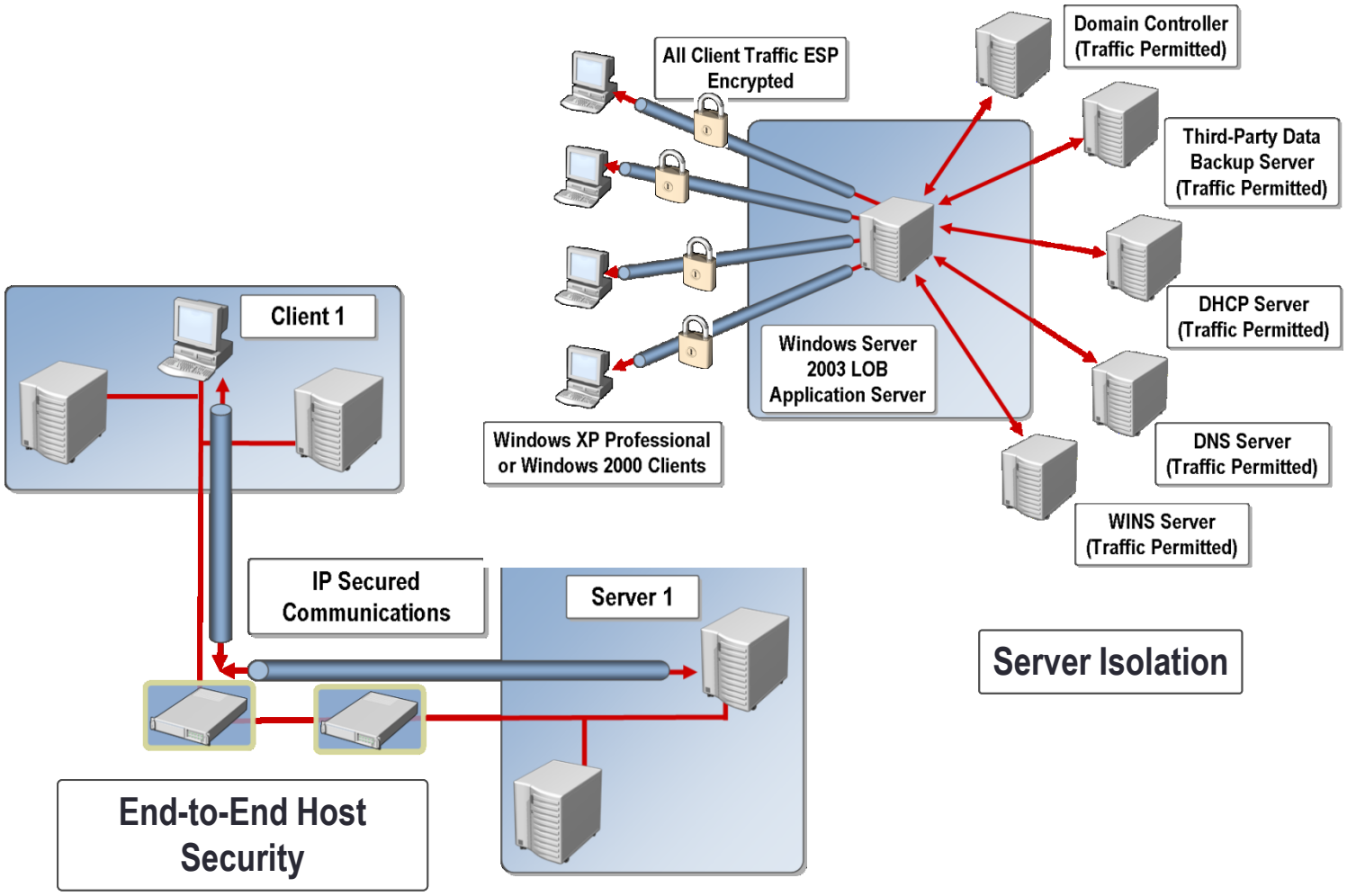
Transportní mód IPSec



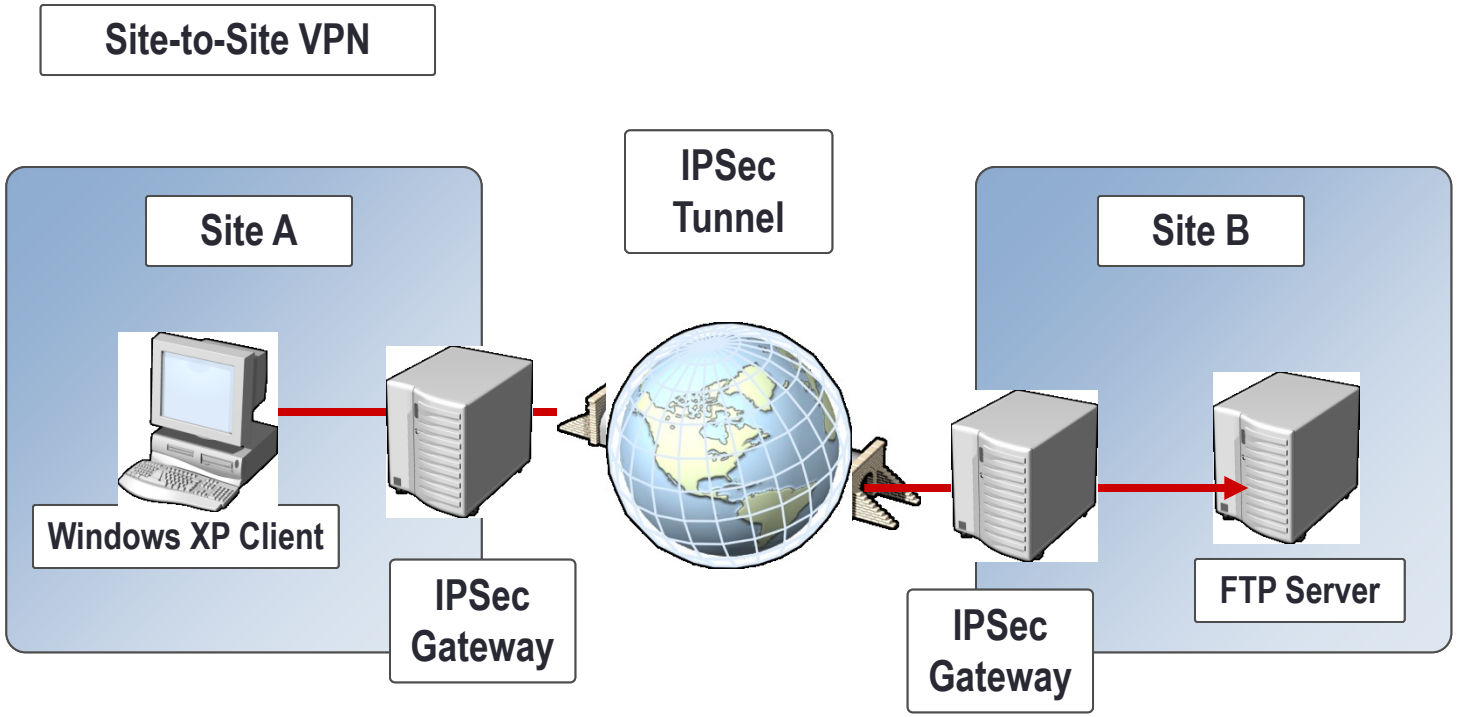
Tunelovací mód IPSec



Transportní mód



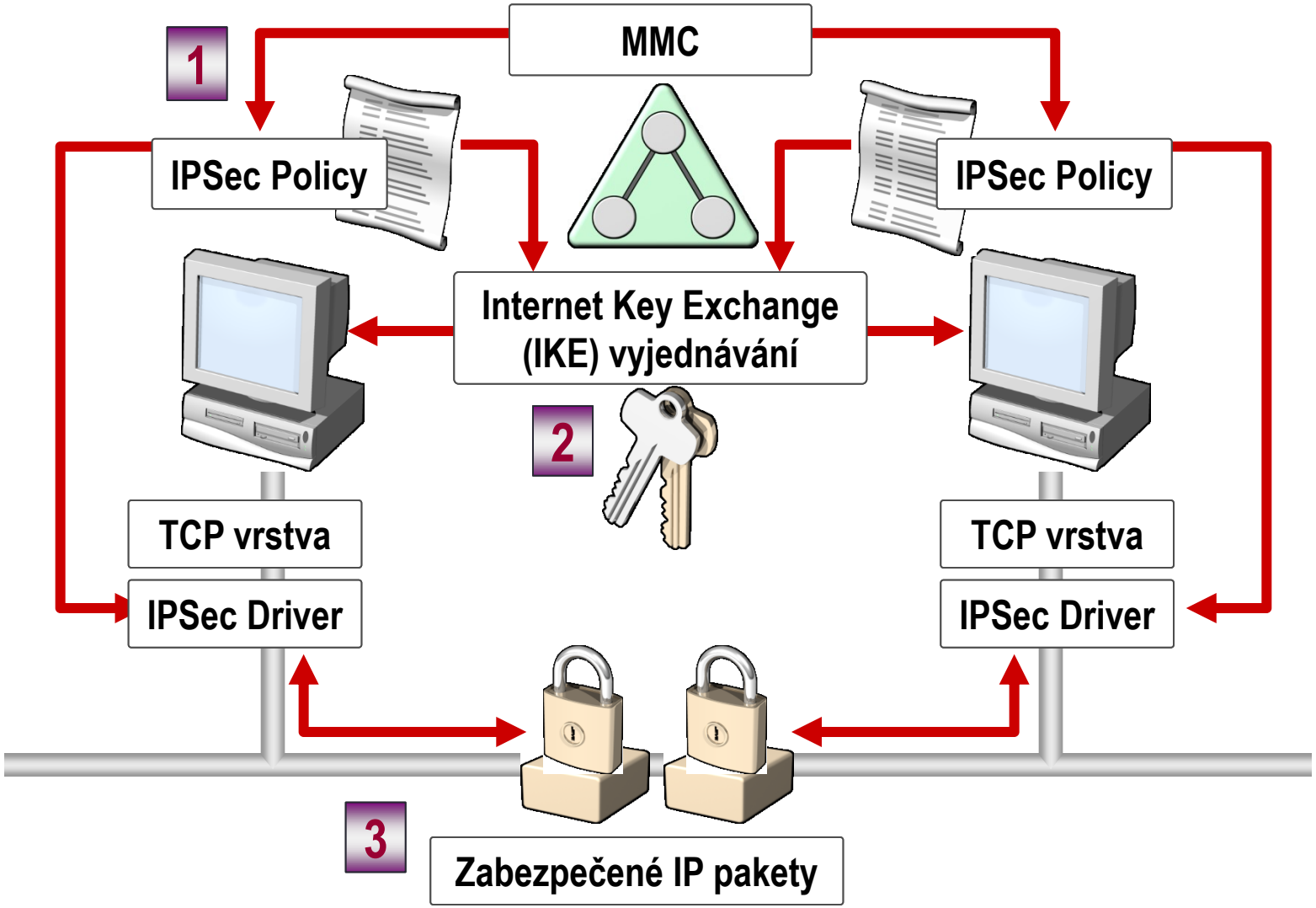
Tunelovací mód



Implementace IPSec

- Časté síťové prvky a operační systémy:
  - Zařízení Cisco
  - PC s MS Windows
- IPSec a MS Windows:
  - Podpora od Windows 2000
  - Flexibilní konfigurační možnosti (místní politika nebo Active Directory)
- MS Management Console (MMC):
  - Snap-in modul pro správu IP bezpečnosti
  - Nastavení obecných pravidel (IKE – doby platností, šifrovací algoritmy atd.)
  - Nastavení pravidel

Jak IPSec zabezpečuje datový provoz?



Konfigurace IPSec u MS Windows

- Filtr – definice parametrů
  - IP adresa
  - IP protokol
  - Zdrojový a cílový TCP a UDP port
- Akce filtru
  - Povolit přenos i nezabezpečených paketů
  - Nezabezpečené pakety blokovat (zahazovat)
  - Aktivovat zabezpečený režim
- Autentizace
  - Kerberos
  - Předsdílený key
  - Certifikáty

Možnosti autentizace

- Kerberos
  - Integrován do Active directory
- Předsdílený key
  - Textový řetězec
  - Neexistuje spolehlivý a jednoduchý mechanismus zneplatnění
  - Použití pouze pro testovací účely
- Certifikáty
  - Nutná přítomnost certifikační autority
  - Kompromitované údaje lze zneplatnit (revocation)

Testování konfigurace IPSec

- Konfigurace:
  - Host to Host
  - AH, ESP
- Autentizace:
  - Předsdílený klíč
  - Certifikát (vlastní CA)
- Nástroje:
  - IPSec monitor
  - Network monitor
  - Wireshark apod.

Konfigurace IPSec u směrovačů Cisco

1. Konfigurace ISAKMP
   - Internet Security Association and Key Management Protocol (zabývá se všemi aspekty SA a zajišťuje výměnu kryptografických klíčů)
2. Konfigurace transformační sady IPSec
3. Konfigurace krypto ACL
   - Access Control List – rozhoduje o použití IPSEc pro každý paket
4. Konfigurace krypto mapy
5. Aplikace krypto mapy na rozhraní

Konfigurace ISAKMP

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 192.1.1.20
```

Konfigurace transformační sady IPSec

```
crypto ipsec transform-set MUJTRANS
 ah-sha-hmac esp-aes 256 esp-sha-hmac
```

(jeden dlouhý řádek, nově se někdy výstižněji označuje „IPSec Proposals“)

Konfigurace krypto ACL

```
access-list 101 permit gre host
     192.1.1.40 host 192.1.1.20
```

(jeden dlouhý řádek, protokol dle potřeby – zde GRE, ale třeba IP, ...)

Konfigurace krypto mapy

```
crypto map MYMAP 10 ipsec-isakmp
 set peer 192.1.1.20
 set transform-set MUJTRANS
 match address 101
```

Aplikace krypto mapy na rozhraní

```
interface serial0/0/1
R3(config-if)# crypto map MYMAP
```

Děkuji za pozornost