VPN siete, Broadband technológie, Filtre sieťovej prevádzky

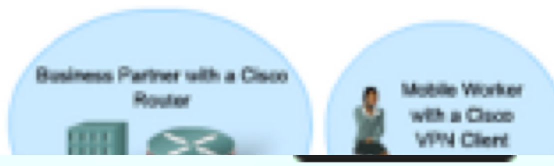
Module 9

Obsah

- Úvod do VPN technológií
- IPSec VPN
- Konfigurácia site-to-site VPN (CLI)
- Remote-access VPN
- Broadbandové technológie (DSL)
- Filtre sieťovej prevádzky

Virtuálne privátne siete (VPN)

- VPN poskytuje prostriedok pre rozšírenie produkčných infraštruktúr o možnosti bezpečného vzdialeného prístupu



- VPN sieť je vytváraná prostredníctvom techniky zapúzdrenia (tunnelingu) IP packetov do transportného protokolu. Za týmto účelom sa využíva GRE, ktorý je sám o sebe nešifrovaný.

Virtuálne privátne siete (VPN)

Výhody VPN:

- Lacný prostriedok na rozšírenie infraštruktúry

  Takmer beznákladové využitie prostredia ISP eliminuje požiadavku na prenajaté okruhy. Softvérové VPN systémy eliminujú potrebu špeciálnych zariadení u klienta.

- Bezpečnosť

  VPN prostredníctvom mechanizmov šifrovania poskytuje vysokú úroveň zabezpečenia. Zvyšuje bezpečnosť klasického pripojenia end-to-end šifrovaním.

- Škálovateľnosť

  S využitím providerských sietí (sieť Internetu) je možné jednoducho pridávať používateľov prostredníctvom VPN a tak rozšíriť firemnú infraštruktúru.

- Kompatibilita s broadbandovými technológiami

  Keďže ide o techniku tunelovania, je možné využiť ľubovoľnú IP sieť.

Virtuálne privátne siete (VPN)

- V najjednoduchšom prípade je VPN sieť tvorená medzi dvoma bodmi cez sieť ISP formujúca logické spojenie

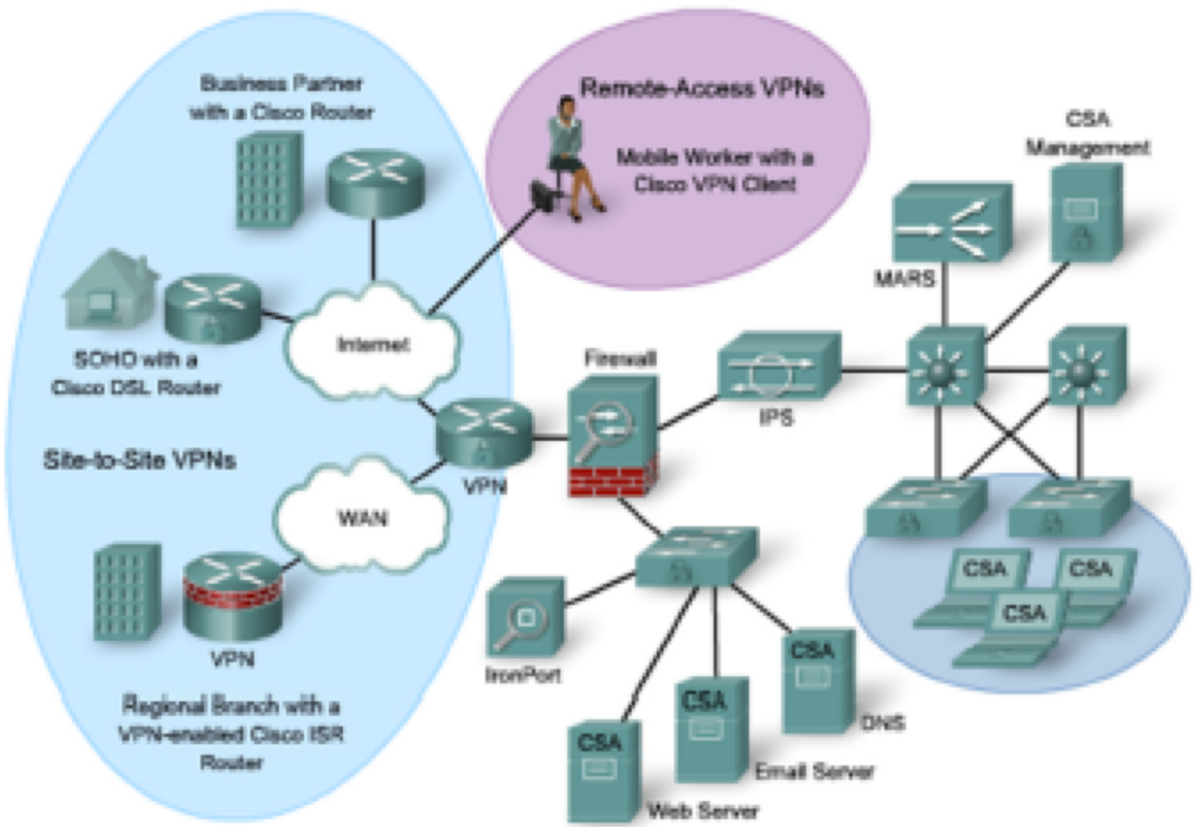
- Logické spojenia môžu byť na rôznych vrstvách ISO/OSI modelu

- Rozlišujeme VPN siete:
  - Layer 2 VPN
  - Layer 3 VPN

Kategorizácia VPN

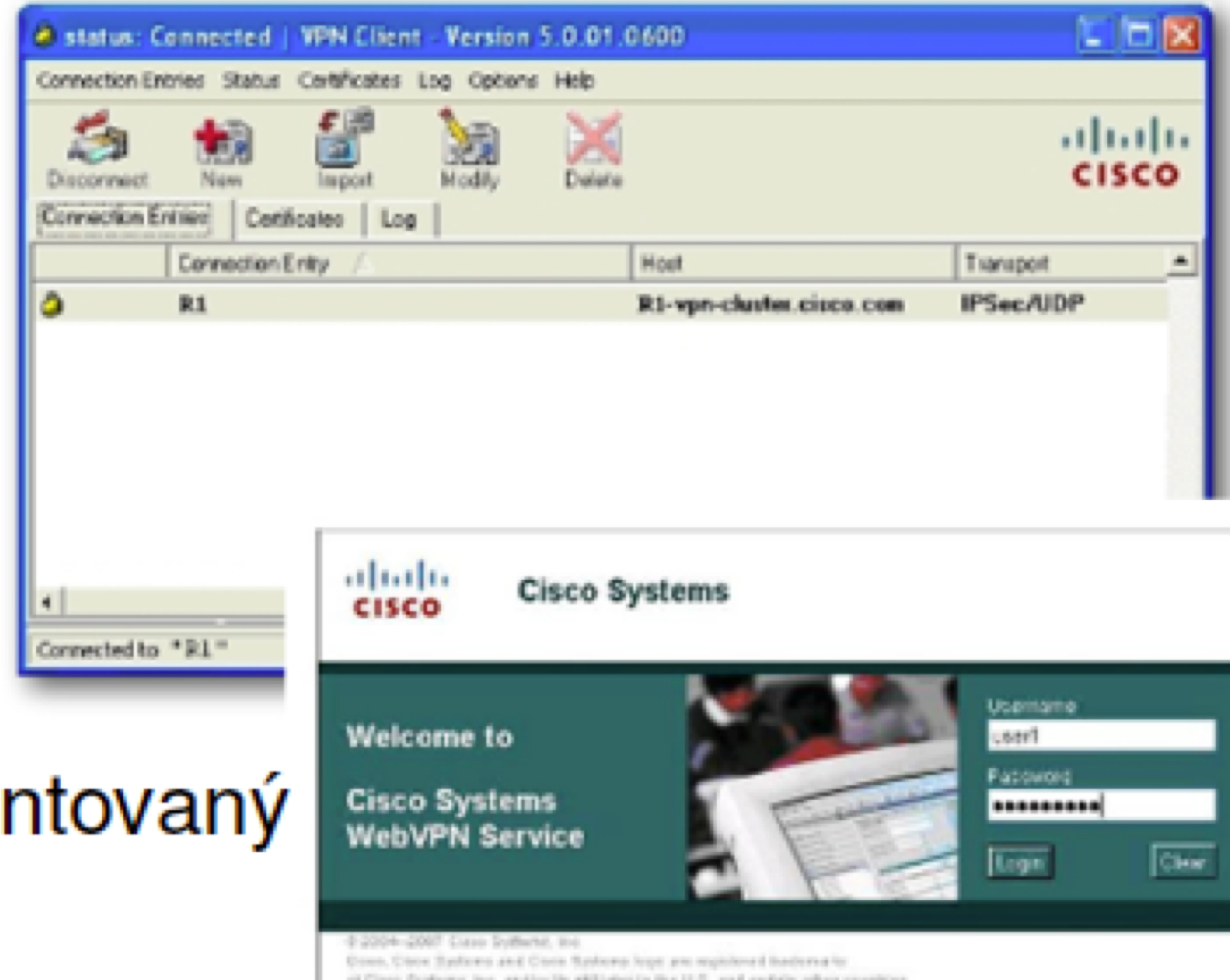
Existujú 2 základné typy VPN:

- Site-to-site
- Remote access



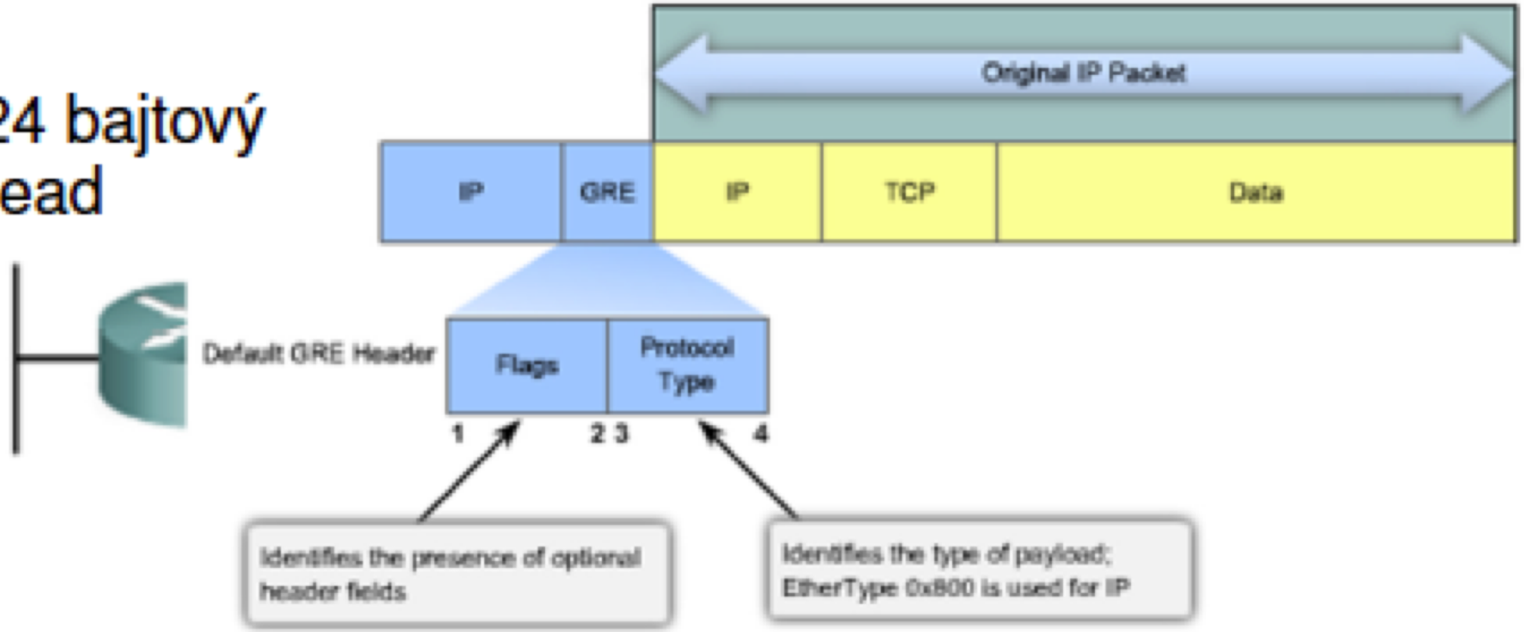
Komponenty remote-access VPN

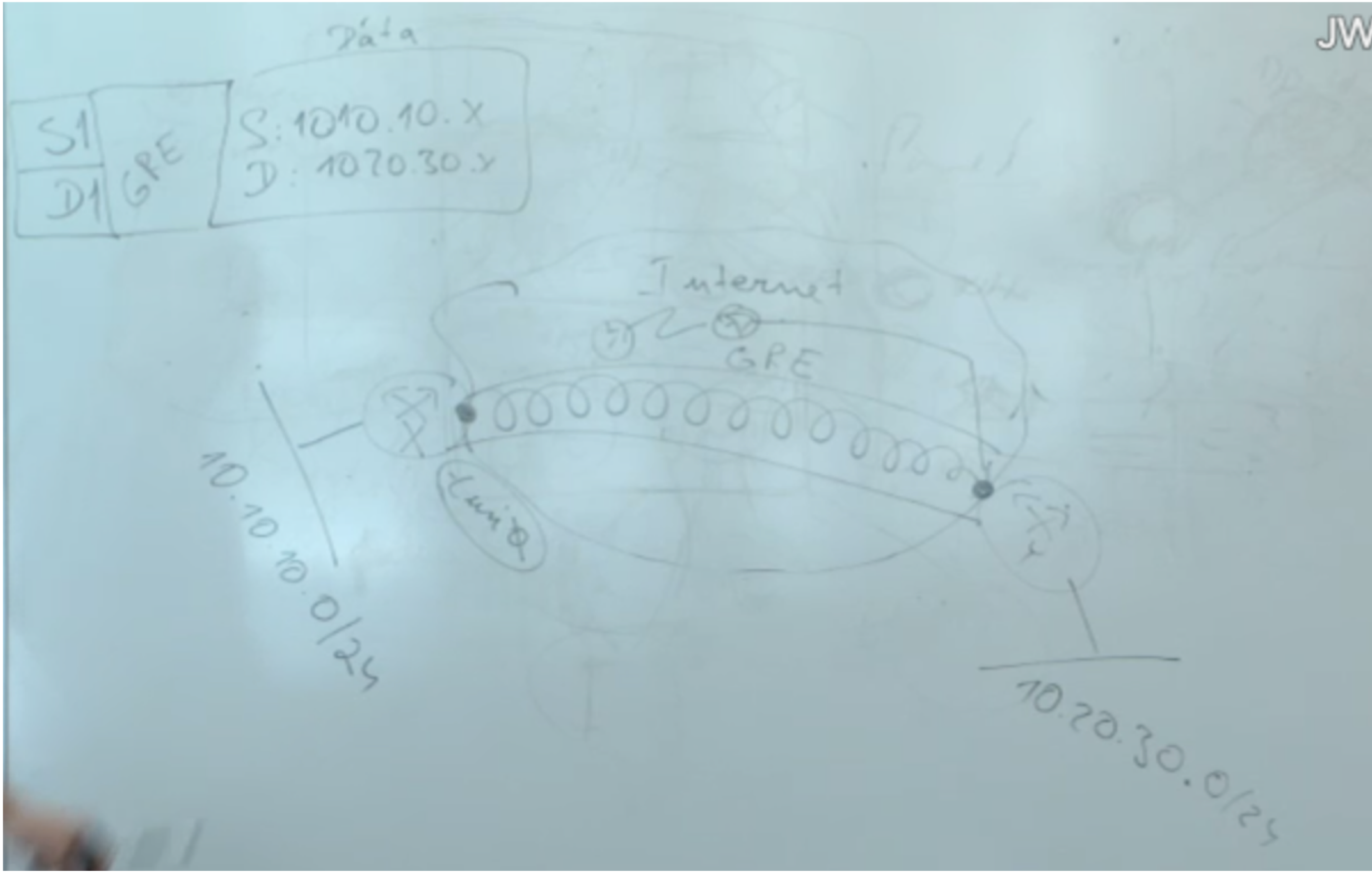
- VPN server
- VPN klient alebo
- Webovo orientovaný SSL VPN



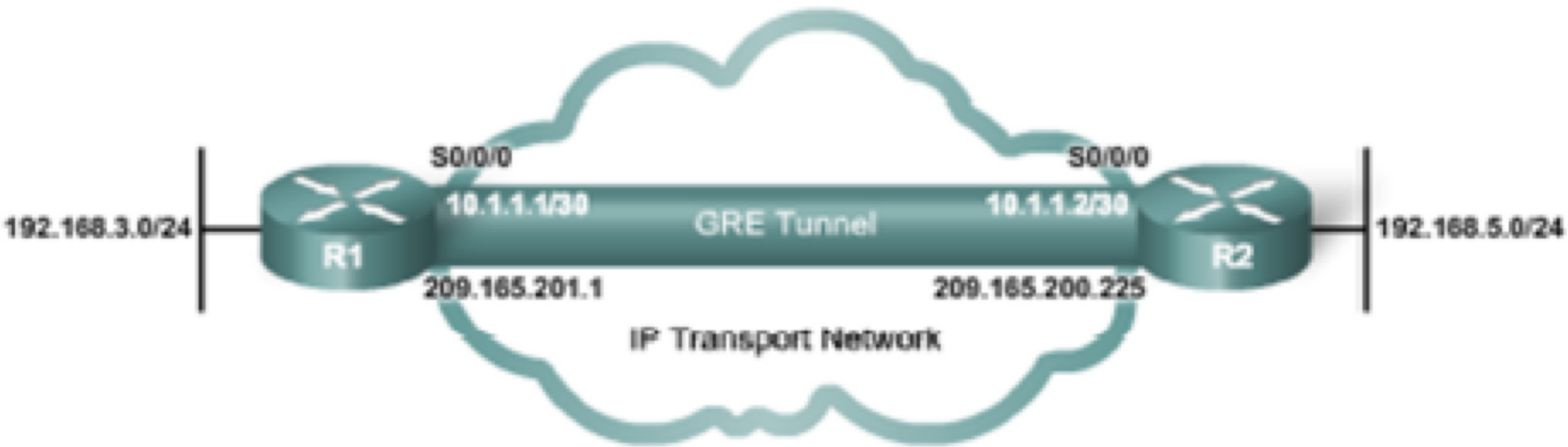
Site-to-site GRE

- GRE je tunelovací protokol definovaný v RFC 1702 a RFC 2784
- GRE zapúzdruje celý IP packet, ktorý je tunelovaný a pridáva k nemu GRE hlavičku
- Min. 24 bajtový overhead




Data
S1
D1
GRE
S: 10.10.10.X
D: 10.20.30.X
Internet
GRE
10.10.10.0/24
10.20.30.0/24

Konfigurácia Site-to-site GRE




```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# tunnel source serial 0/0/0
R1(config-if)# tunnel destination 209.165.200.225
R1(config-if)# tunnel mode gre ip
R1(config-if)#
```

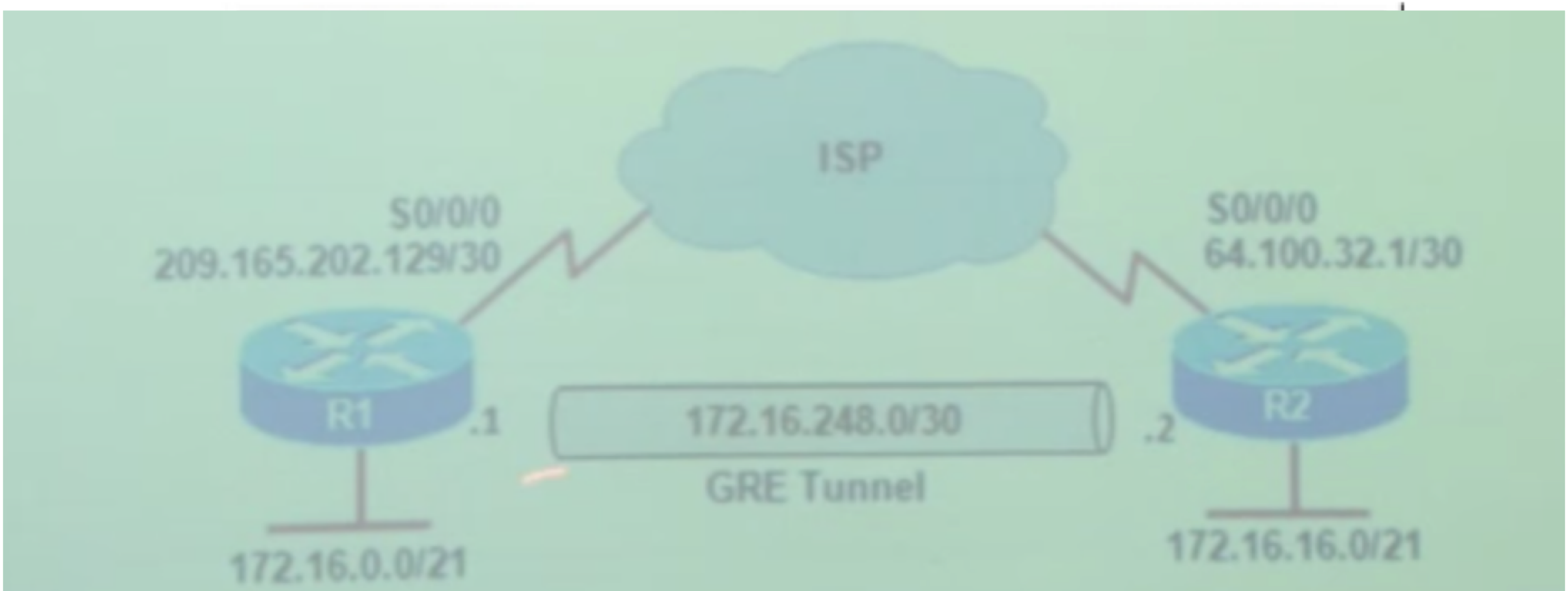
```
R2(config)# interface tunnel 0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# tunnel source serial 0/0/0
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# tunnel mode gre ip
R2(config-if)#
```

GRE tunnel is up and the protocol is up if:

- Tunnel source and destination are configured
- Tunnel destination is in routing table
- GRE keepalives are received (if used)
- GRE is the default tunnel mode

GRE a NAT

- Pomocou pravidla s akciou „deny“ v ACL je potrebné definovať, že pri prechode cez tunnelové rozhranie sa preklad nesmie udiať



GRE a NAT

- Pomocou pravidla s akciou „deny“ v ACL je potrebné definovať, že pri prechode cez tunnelové rozhranie sa preklad nesmie udiať

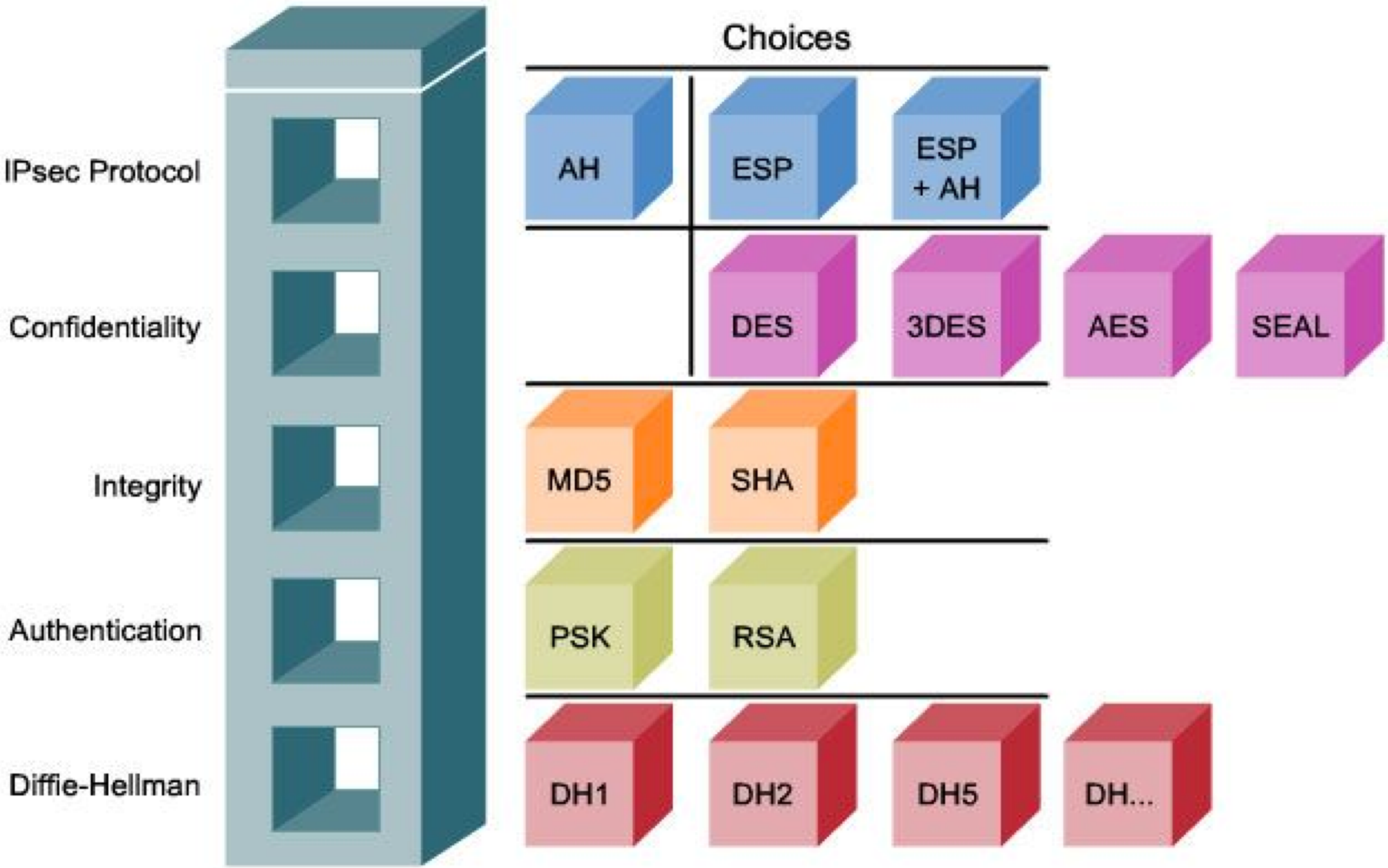
```
R1(config)# interface tunnel0
R1(config-if)# tunnel source serial0/0/0
R1(config-if)# tunnel destination 64.100.32.1
R1(config-if)# ip address 172.16.248.1 255.255.255.252
R1(config-if)# no shut
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
```

```
R2(config)# interface tunnel0
R2(config-if)# tunnel source serial0/0/0
R2(config-if)# tunnel destination 209.165.202.129
R2(config-if)# ip address 172.16.248.2 255.255.255.252
R2(config-if)# no shut
R2(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
```

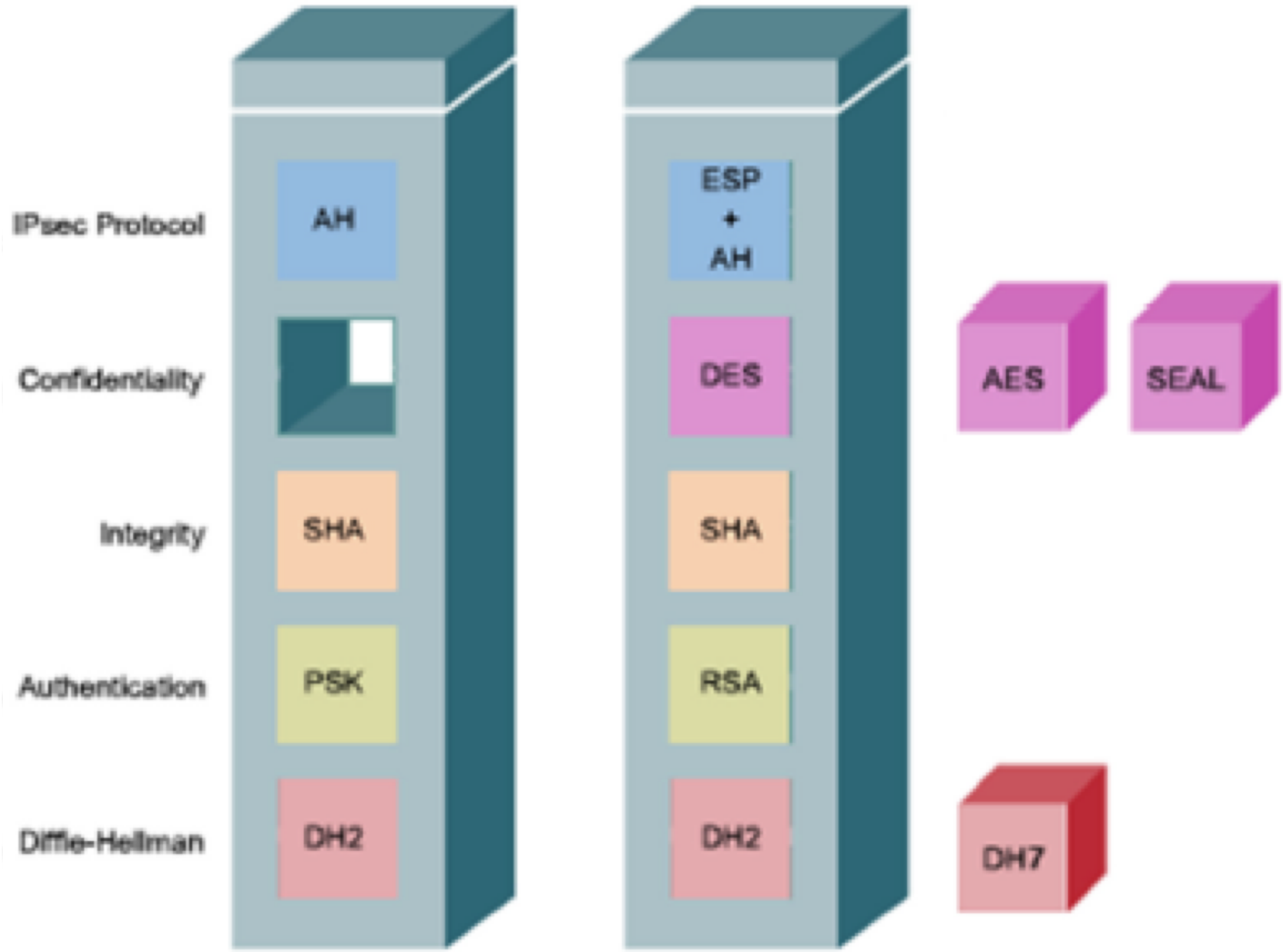
IPSec

- IETF štandard (RFC 2401-2412)
- Predstavuje framework pre bezpečnú komunikáciu
- Pracuje na 3. vrstve ISO/OSI s cieľom šifrovať a autentifikovať IP pakety
- IPSec framework je tvorený piatimi základnými blokmi

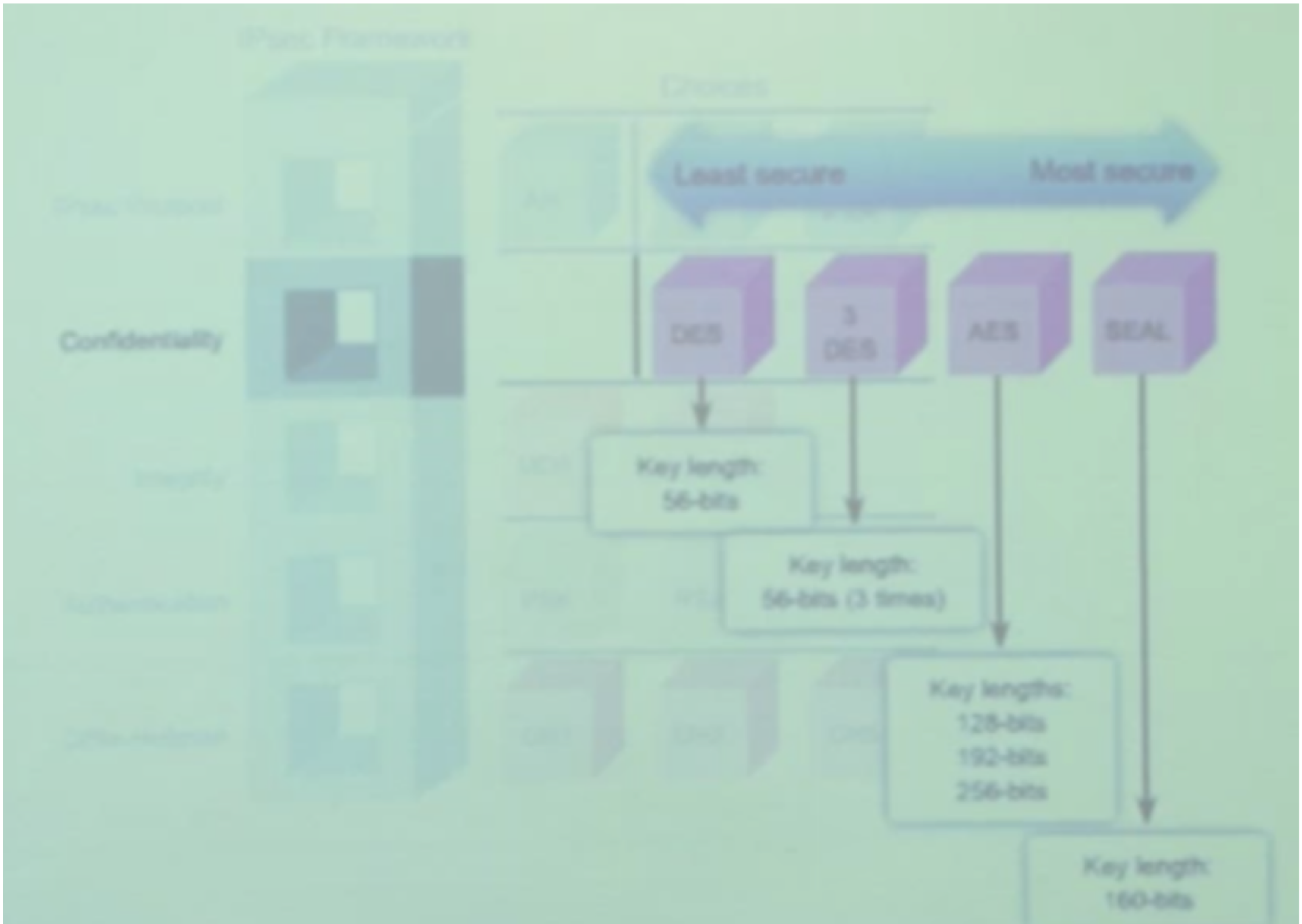
Základné bloky IPSec



Základné bloky IPSec

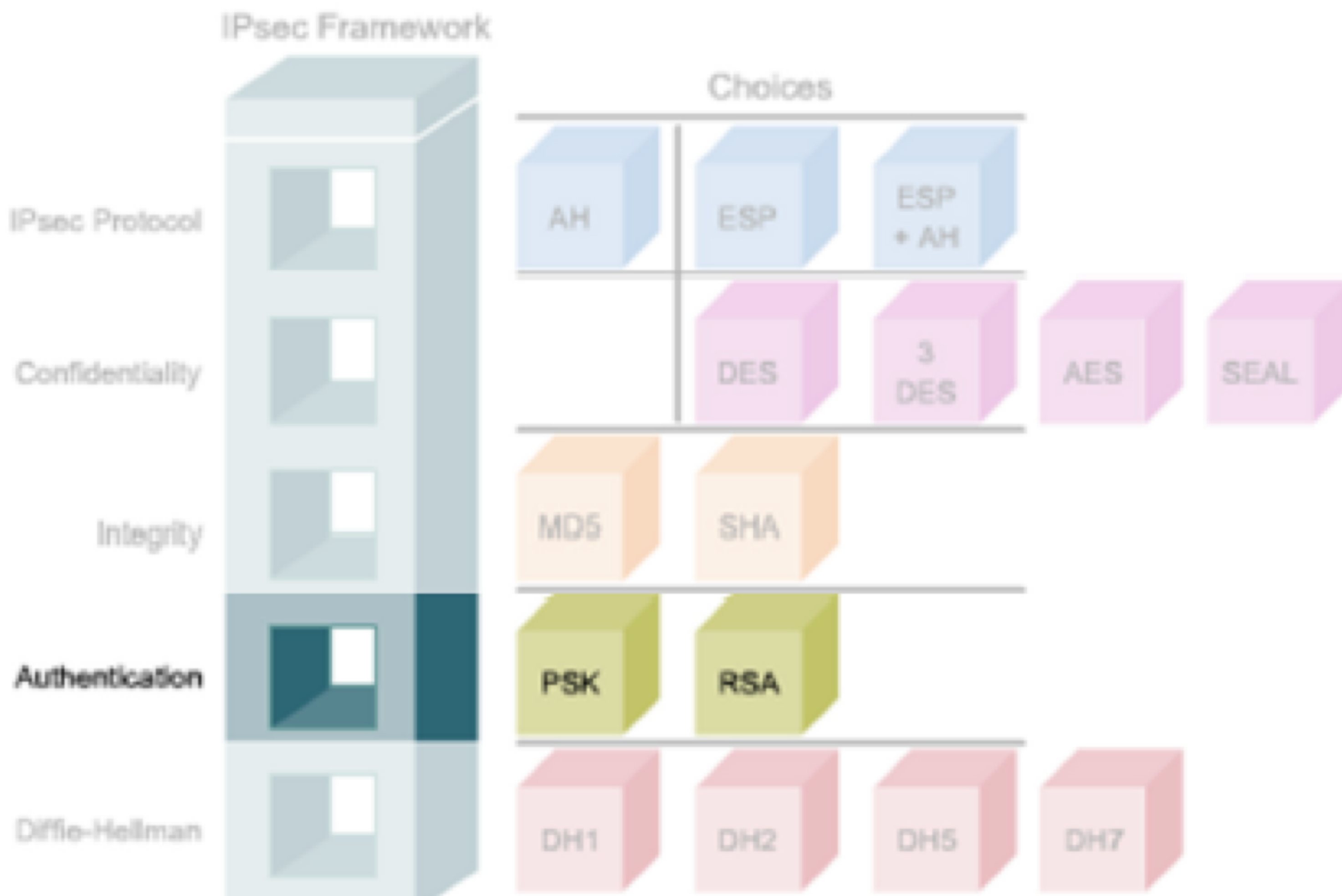


Základné bloky IPSec

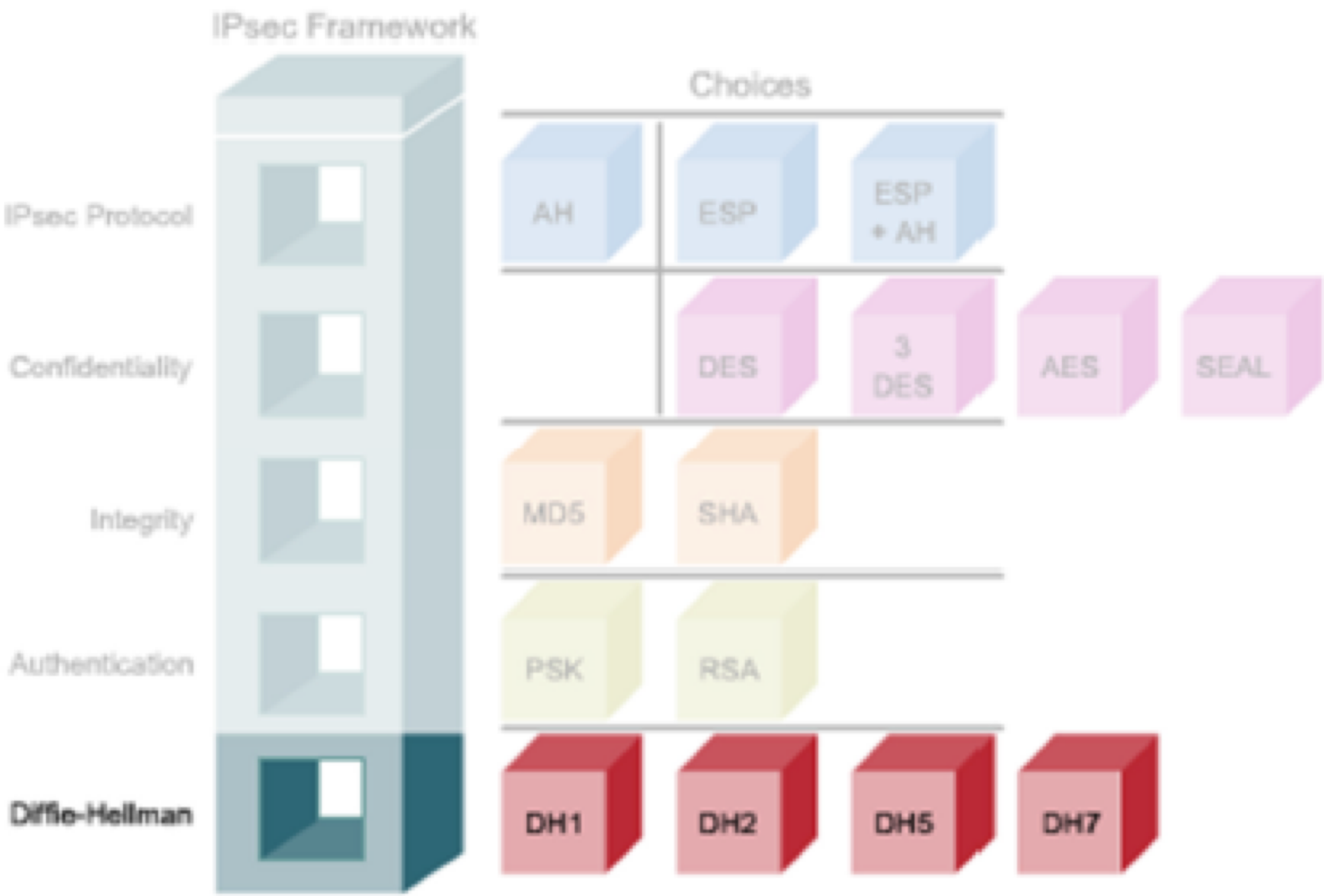


Základné bloky IPSec

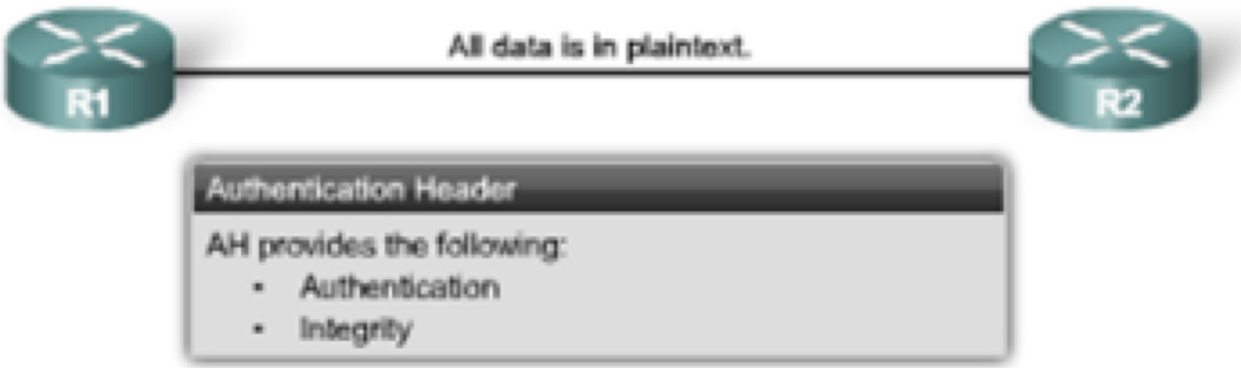
Základné bloky IPSec



Bezpečná výmena kľúčov - DH



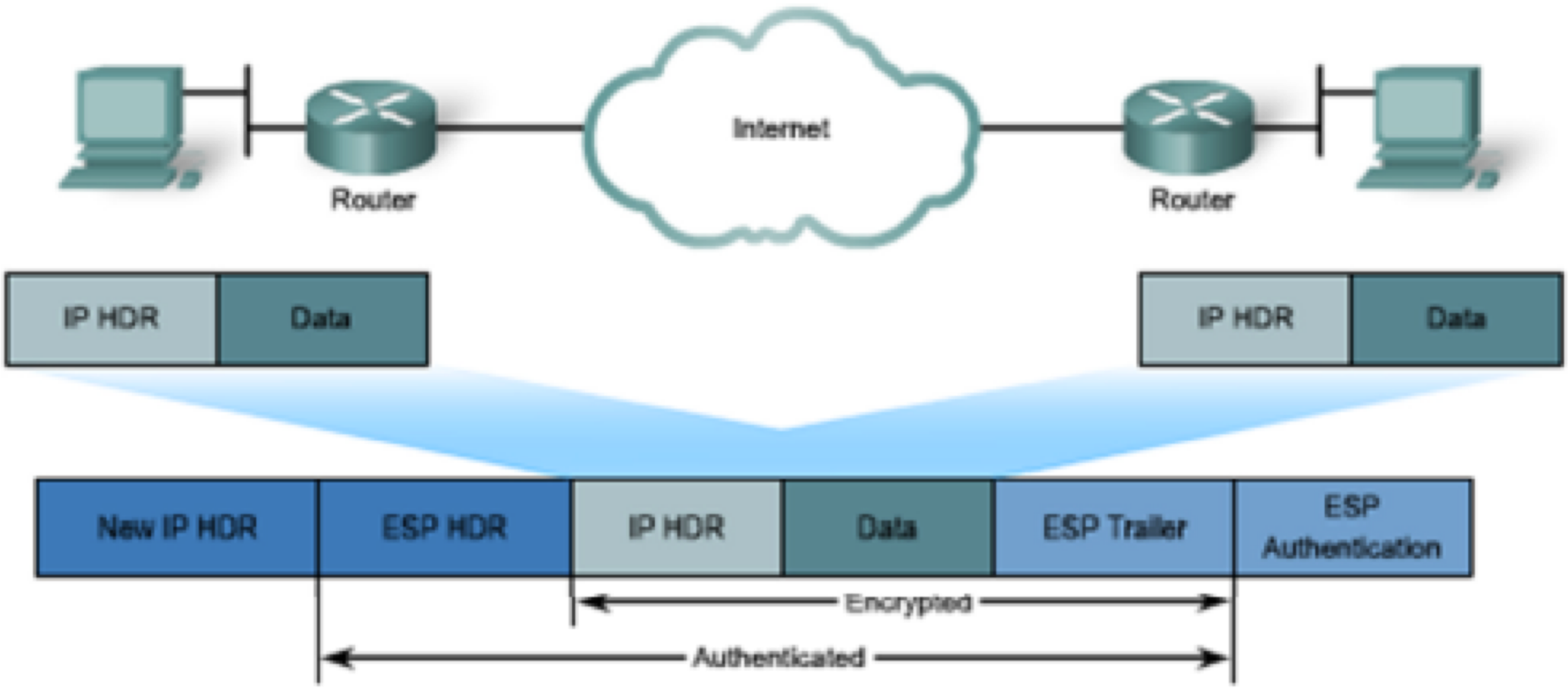
IPSec protokoly



- AH = IP protokol #51

- ESP = IP protokol #50

AH a ESP v akcii

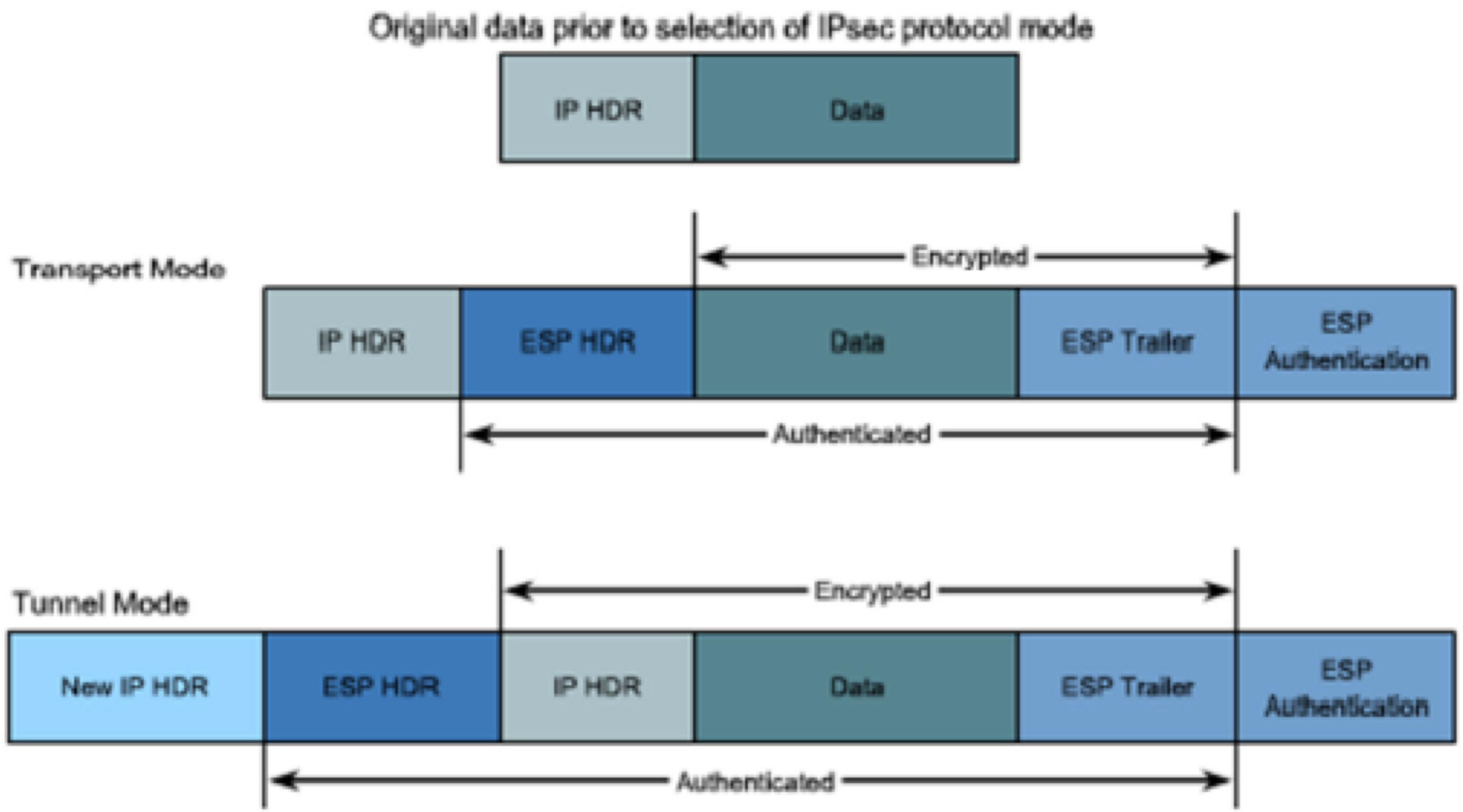


- Provides confidentiality with encryption
- Provides integrity with authentication

IPSec ESP režimy

- Transportný mód
  - Zabezpečenie je poskytované iba pre transportnú vrstvu ISO/OSI.
  - Záhlavie IP packetu sa ponecháva bezo zmeny (kvôli smerovaniu) a zašifrovaná je len dátová časť
  - ESP v transportnom režime je vhodné pre end-to-end komunikáciu medzi klientmi
- Tunelovací mód
  - Poskytuje zabezpečenie celého IP paketu
  - Vytvára sa nová hlavička

IPSec ESP – Transport vs. Tunnel



IPSec SA, IKE a ISAKMP

- **SA=Security Association**

  Dohodnuté parametre medzi dvoma zariadeniami používajúcimi IPSec

- **IKE=Internet Key Exchange (UDP/500)**

  Používané v IPSec za účelom dohodnutia šifrovacích kľúčov (RFC 2409)

- **ISAKMP=Internet Security Association and Key Management Protocol**

  Definuje formát správ a spôsob výmený kľúčov tak, aby bolo možné sformovať SA

IPSec IKE

IKE má dve fázy:

- Fáza 1

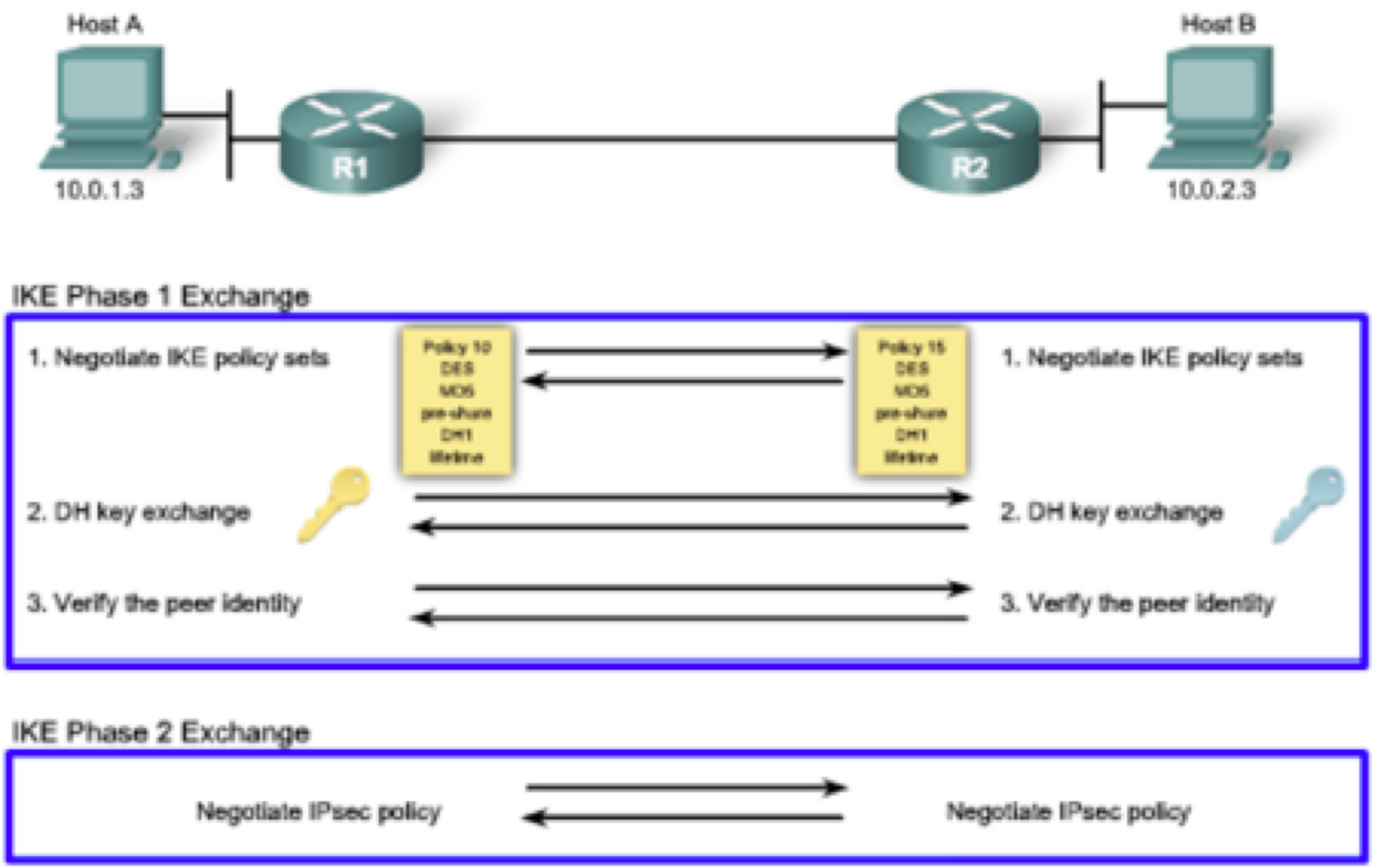
  Dohodnutie základných parametrov IKE, zhoda IKE politiky (aká bude použitá autentifikácia, DH skupina). Autentifikácia suseda.

- Fáza 2

  Prostredníctvom ISAKMP realizované dohodnutie IPSec politík

IPSec IKE

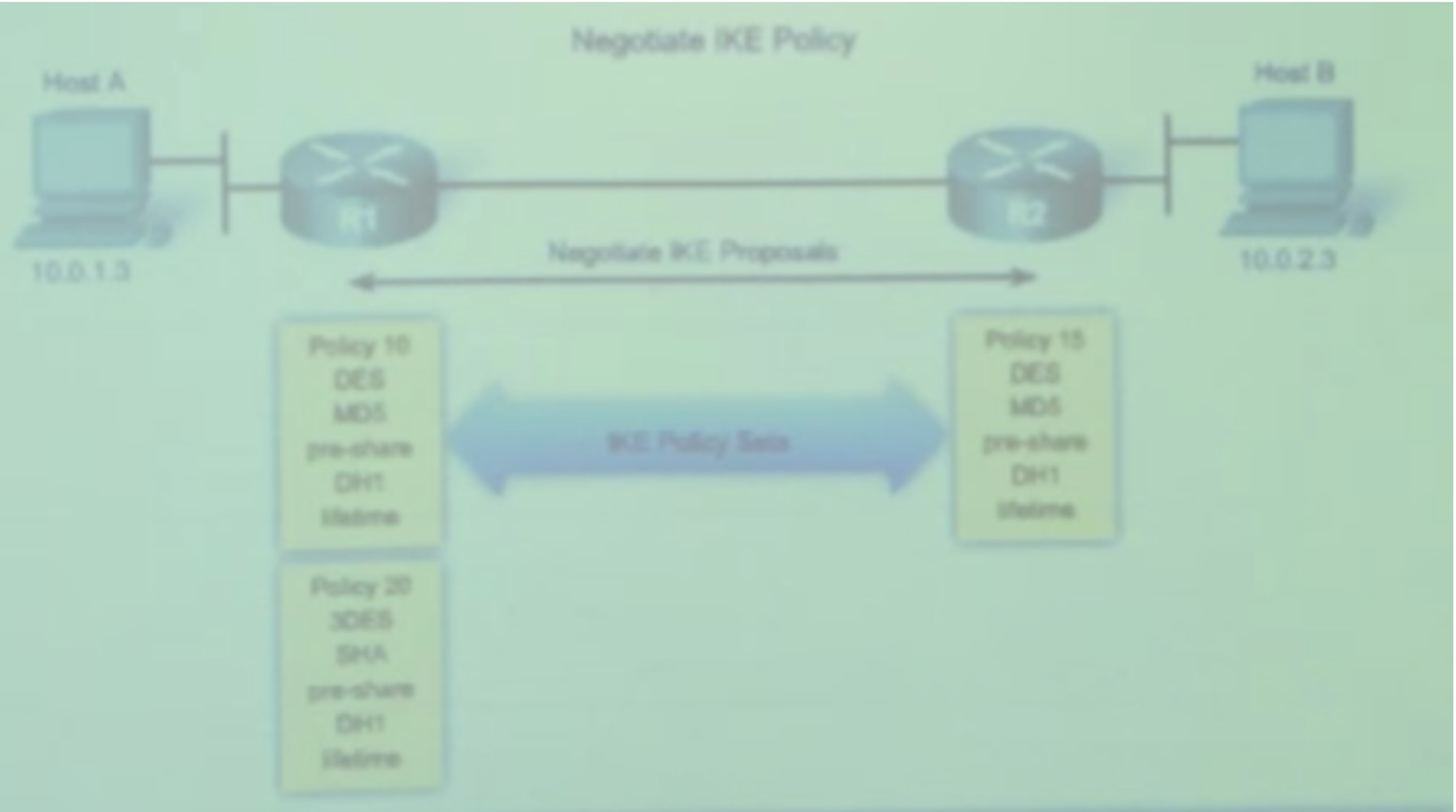
Ik



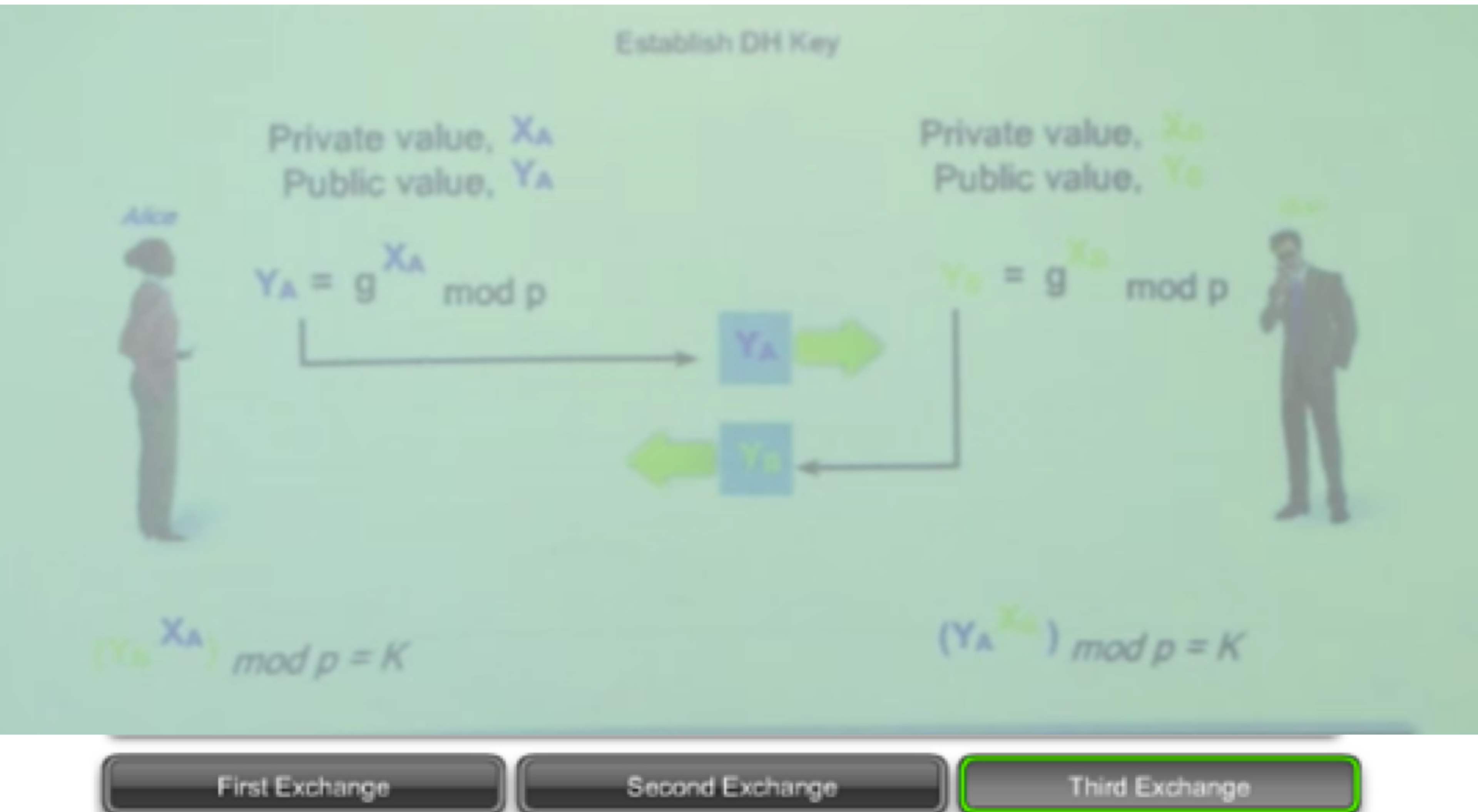
ká

a.

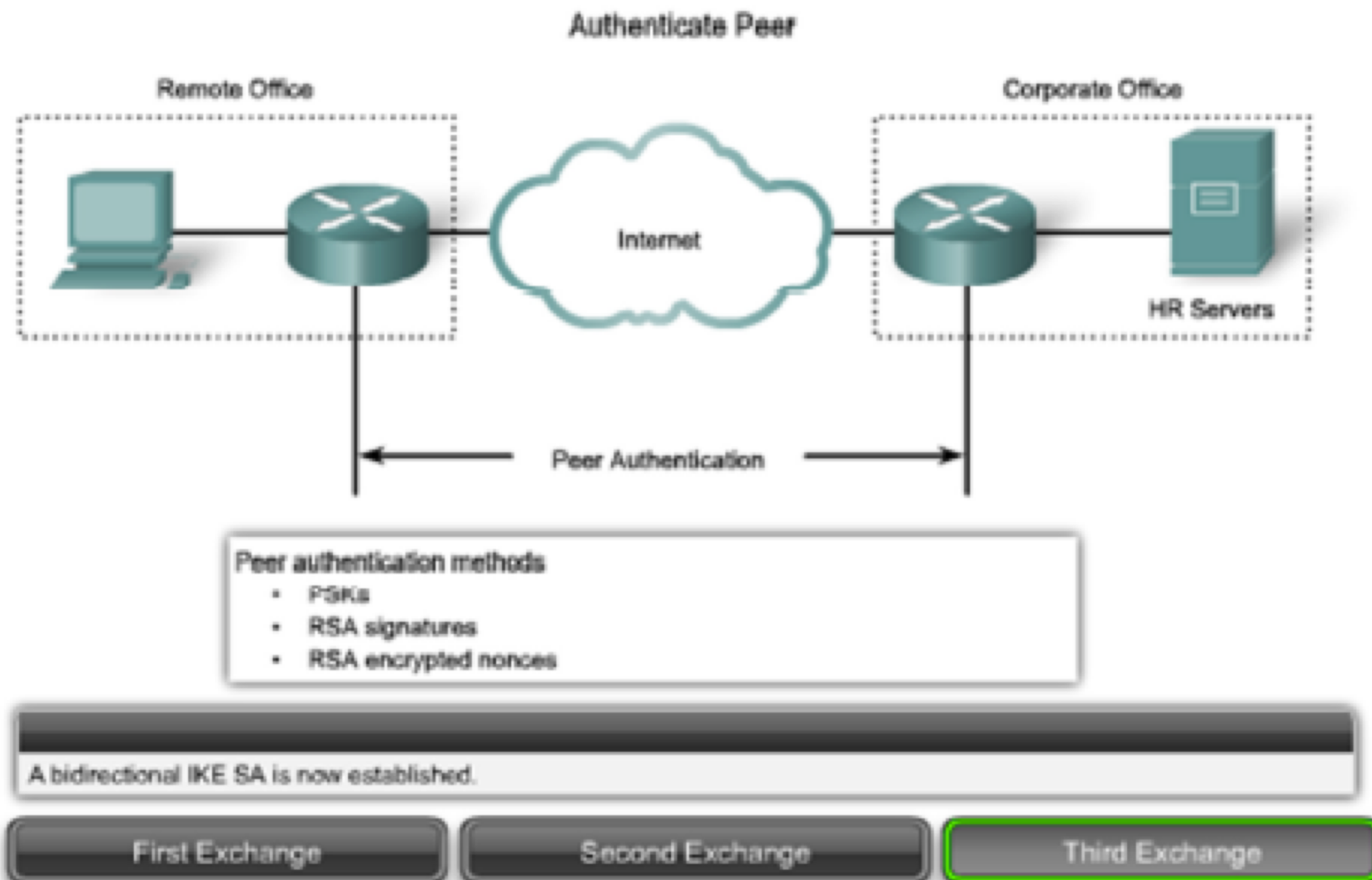
IKE fáza 1 – main mode



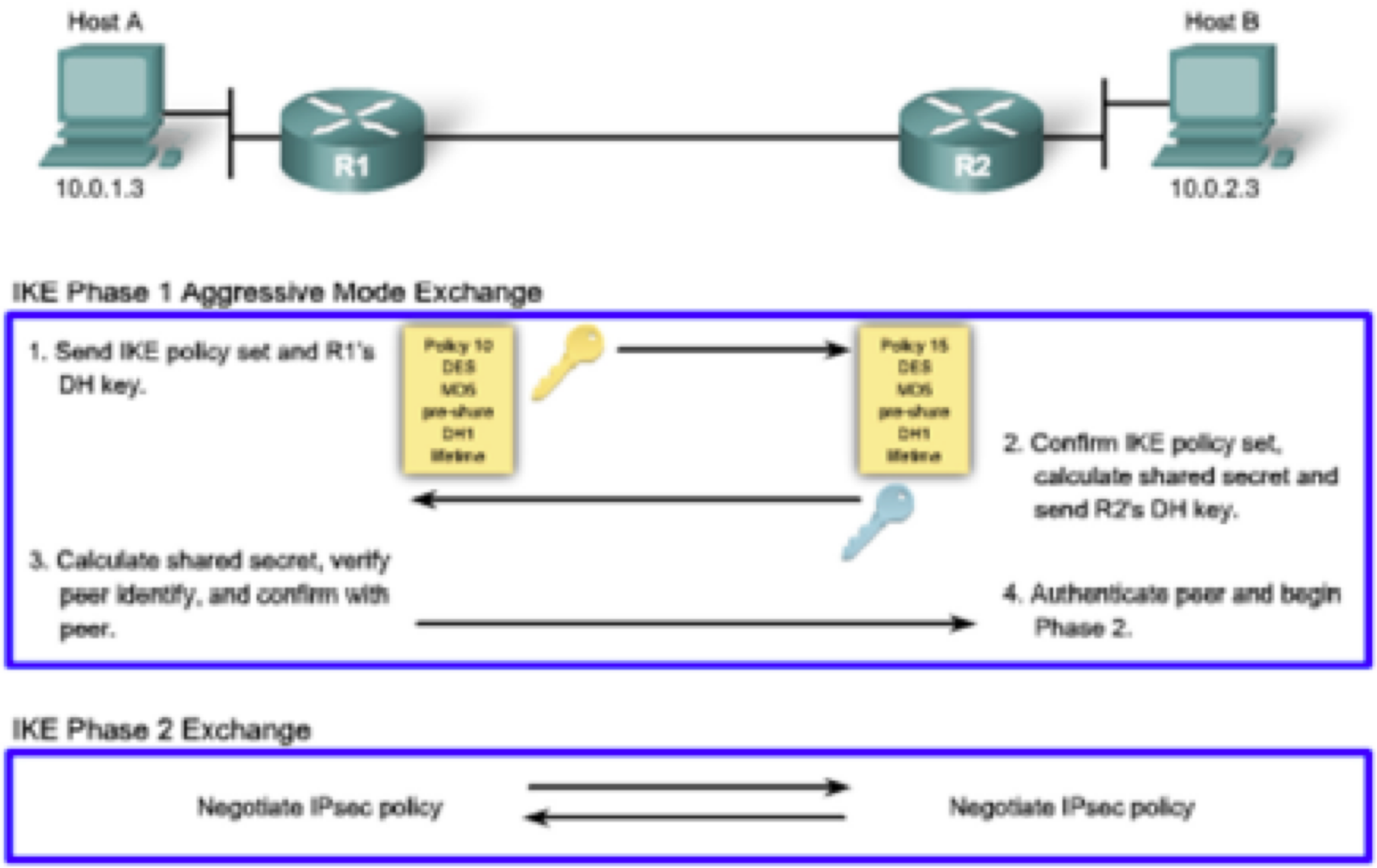
IKE fáza 1 – main mode



IKE fáza 1 – main mode



IKE fáza 1 – aggresive mode



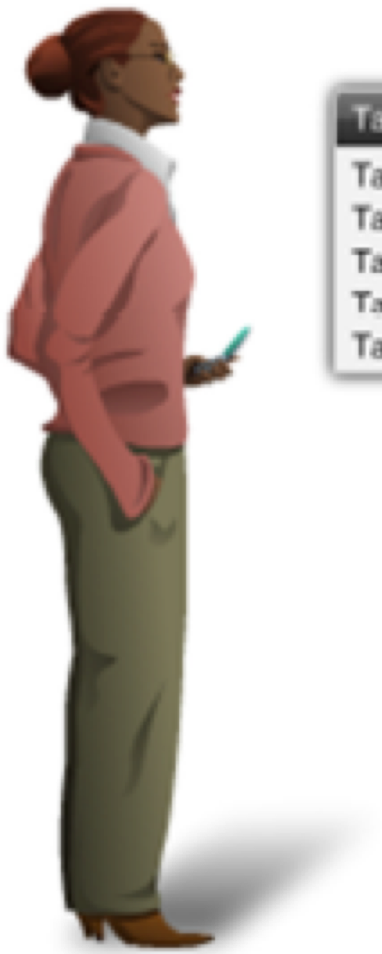
IKE fáza 2

- Cieľom je dohodnúť IPSec bezpečnostné parametre, ktoré sa použijú na samotné šifrovanie dát

- IKE negotiates matching IPsec policies.
- Upon completion, unidirectional IPsec SAs are established for each protocol and algorithm combination.

Konfigurácia site-to-site IPSec VPN

www.cnl.tuke.sk



Tasks to Configure IPsec:

Task 1: Ensure that ACLs are compatible with IPsec.
Task 2: Create ISAKMP (IKE) policy.
Task 3: Configure IPsec transform set.
Task 4: Create a crypto ACL.
Task 5: Create and apply the crypto map.

Task 1 – kontrola FW politík

Tasks to Configure IPsec:

- Task 1: Ensure that ACLs are compatible with IPsec.
- Task 2: Create ISAKMP (IKE) policy.
- Task 3: Configure IPsec transform set.
- Task 4: Create a crypto ACL.
- Task 5: Create and apply the crypto map.

- ESP používa IP protokol #50
- AH používa IP protokol #51
- ISAKMP používa UDP port 500

Task 1 – kontrola FW politík

Tasks to Configure IPsec:

- Task 1: Ensure that ACLs are compatible with IPsec.
- Task 2: Create ISAKMP (IKE) policy.
- Task 3: Configure IPsec transform set.
- Task 4: Create a crypto ACL.
- Task 5: Create and apply the crypto map.

```
R1(config)# access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 172.30.1.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ip access-group 102 in
R1(config-if)# exit
R1(config)# exit
R1#
R1# show access-lists
    access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
```

Task 2 – ISAKMP policy

Tasks to Configure IPsec:
Task 1: Ensure that ACLs are compatible with IPsec.
Task 2: Create ISAKMP (IKE) policy.
Task 3: Configure IPsec transform set.
Task 4: Create a crypto ACL.
Task 5: Create and apply the crypto map.

```
router(config)#
crypto isakmp policy priority
```

Defines the parameters within the IKE policy

```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption des
R1(config-isakmp)# group 1
R1(config-isakmp)# hash md5
R1(config-isakmp)# lifetime 86400
```

Task 2 – ISAKMP policy

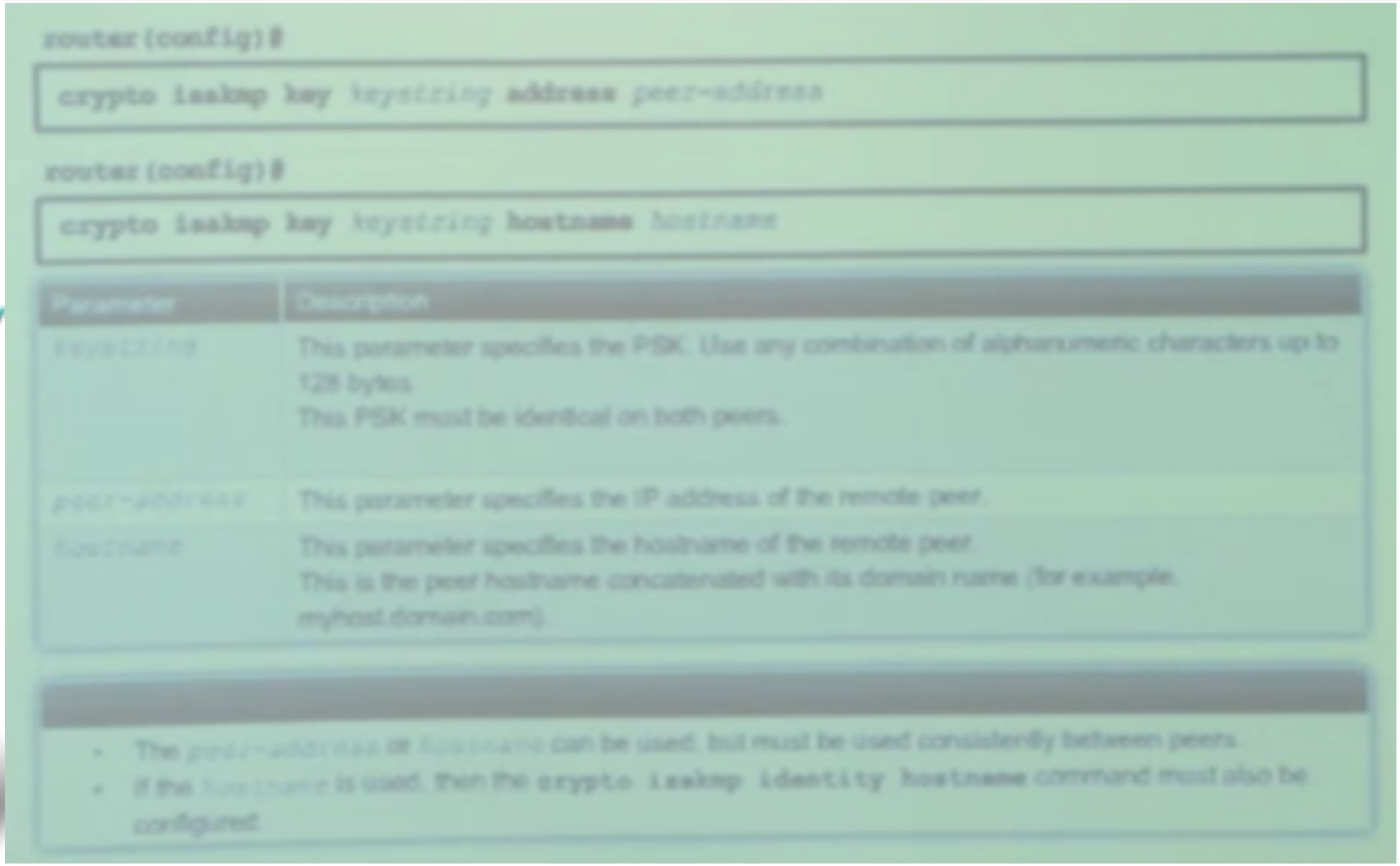
Tasks to Configure IPsec:

Task 1: Ensure that ACLs are compatible with IPsec.
Task 2: Create ISAKMP (IKE) policy.
Task 3: Configure IPsec transform set.
Task 4: Create a crypto ACL.
Task 5: Create and apply the crypto map.

Policy 100 and 200 can be successfully negotiated, but policy 300 cannot.

Note: smaller priority numbers have higher priority.

Task 2 – IKE kľúč



```
router(config)#
crypto isakmp key keystring address peer-address

router(config)#
crypto isakmp key keystring hostname hostname
```

Parameter	Description
keystring	This parameter specifies the PSK. Use any combination of alphanumeric characters up to 128 bytes. This PSK must be identical on both peers.
peer-address	This parameter specifies the IP address of the remote peer.
hostname	This parameter specifies the hostname of the remote peer. This is the peer hostname concatenated with its domain name (for example, myhost.domain.com).

- The *peer-address* or *hostname* can be used, but must be used consistently between peers.
- If the *hostname* is used, then the **crypto isakmp identity hostname** command must also be configured.

Task 2 – IKE kľúč

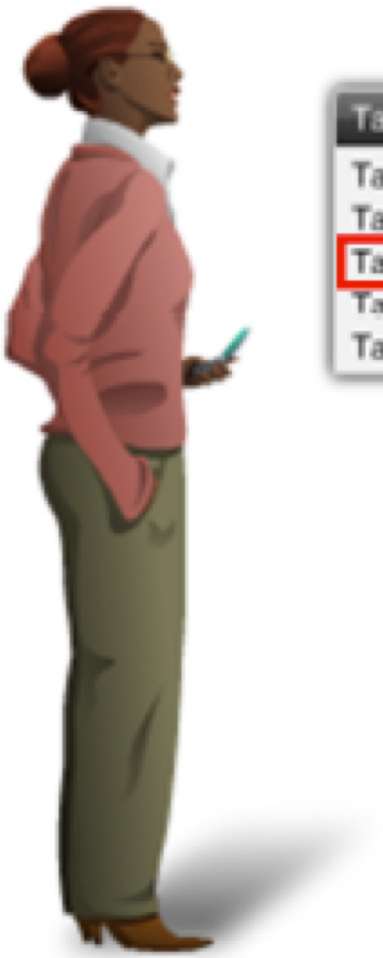

```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)#
```

Note:

- The keystring cisco123 matches.
- The address identity method is specified.
- The ISAKMP policies are compatible.
- Default values do not have to be configured.

```
R2(config)# crypto isakmp policy 110
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)#
```

Task 3 – konfigurácia transformu-setu



Tasks to Configure IPsec:

- Task 1: Ensure that ACLs are compatible with IPsec.
- Task 2: Create ISAKMP (IKE) policy.
- Task 3: Configure IPsec transform set.
- Task 4: Create a crypto ACL.
- Task 5: Create and apply the crypto map.

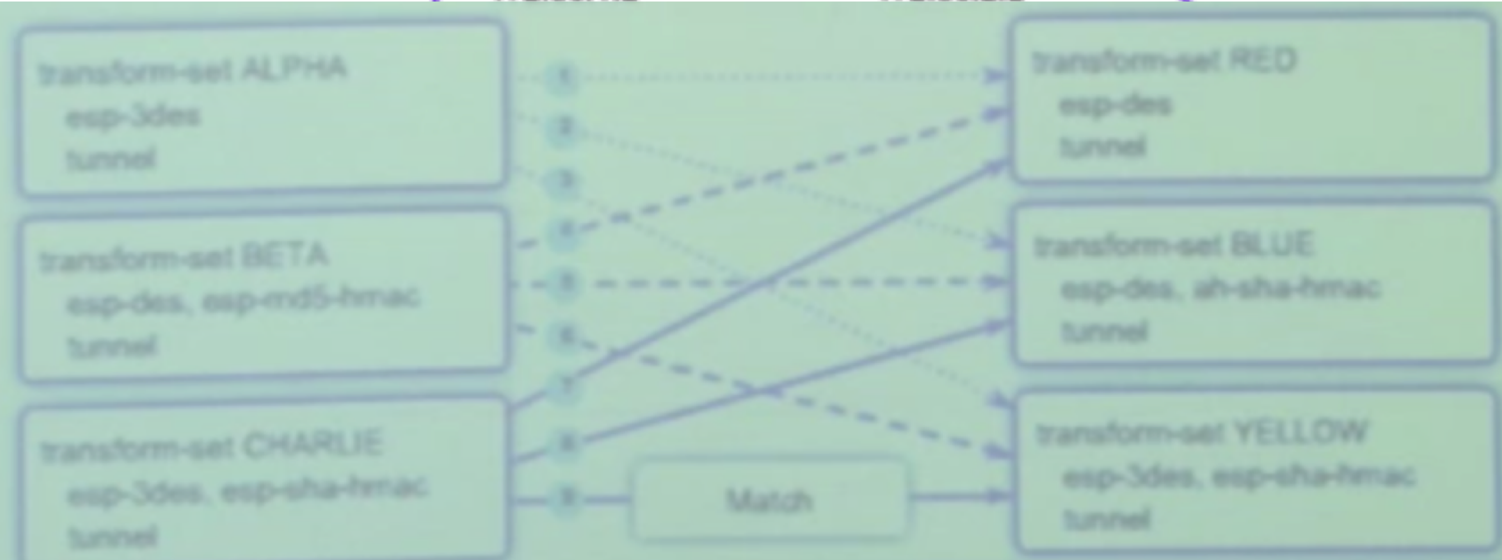
```
router(config)#
crypto ipsec transform-set transform-set-name transform1 [transform2]
[transform3][transform4]
```

crypto ipsec transform-set Parameters

Command	Description
`transform-set-name`	This parameter specifies the name of the transform set to create (or modify).
`transform1, transform2, transform3, transform4`	Type of transform set. Specify up to four "transforms": one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication. These transforms define the IP Security (IPsec) security protocols and algorithms.

- A transform set is a combination of IPsec transforms that enact a security policy for traffic.
- A transform set can have one AH transform and up to two ESP transforms.

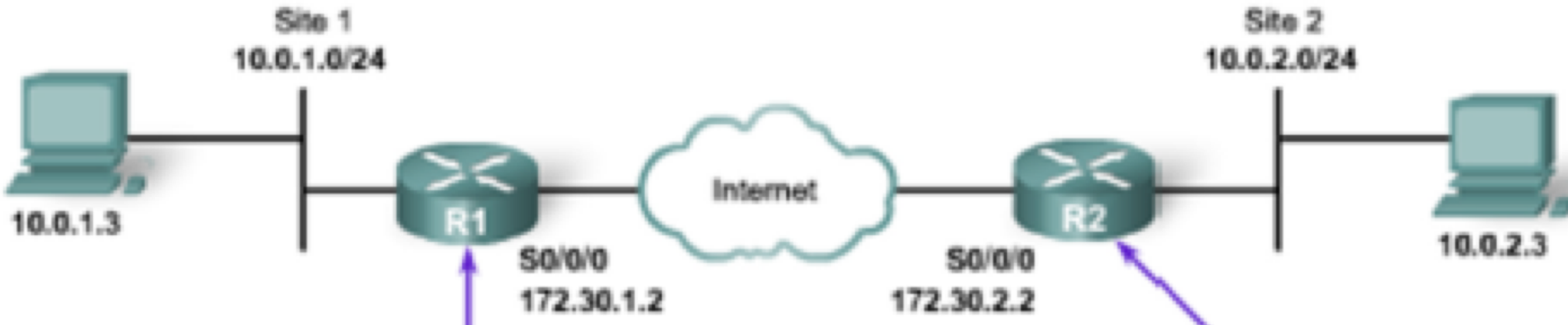
Task 3 – zhoda transform-setu



Note:

- Peers must share the same transform set settings.
- Names are only locally significant.

Task 3 – zhoda transform-setu



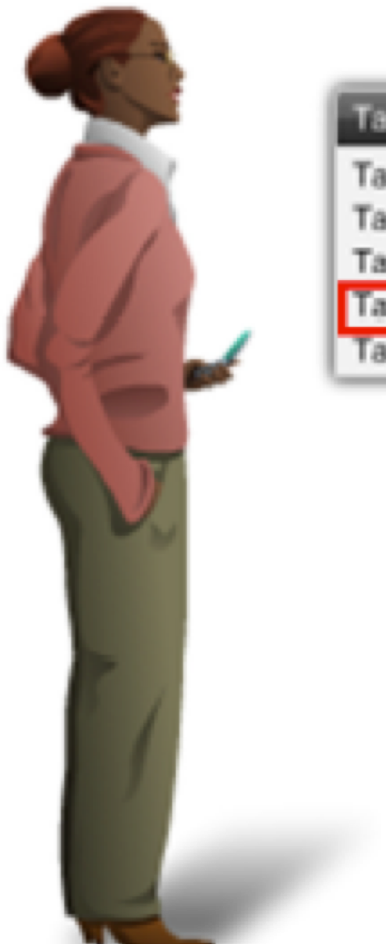

```
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)# crypto ipsec transform-set MYSET esp-aes 128
R1(cfg-crypto-trans)# exit
R1(config)#
```

```
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)# crypto ipsec transform-set OTHERSET esp-aes 128
R2(cfg-crypto-trans)# exit
```

Note:

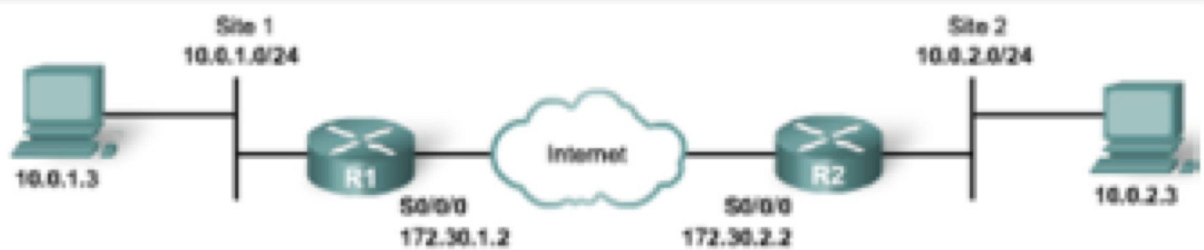
- Peers must share the same transform set settings.
- Names are only locally significant.

Task 4 – konfigurácia Crypto ACL



Tasks to Configure IPsec:

- Task 1: Ensure that ACLs are compatible with IPsec.
- Task 2: Create ISAKMP (IKE) policy.
- Task 3: Configure IPsec transform set.
- Task 4: Create a crypto ACL.
- Task 5: Create and apply the crypto map.



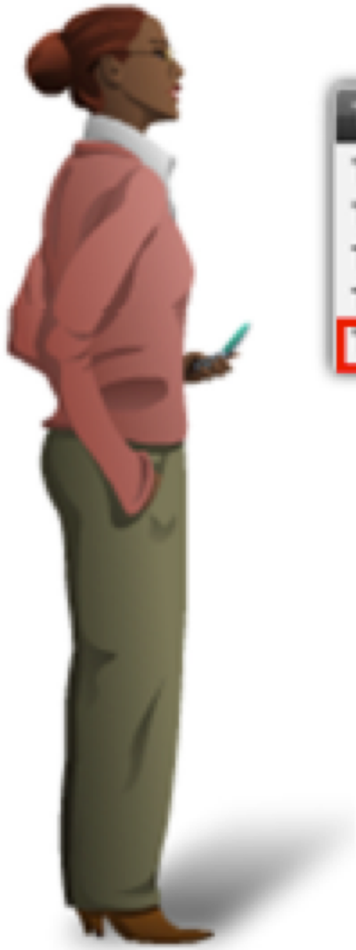
Applied to R1 S0/0/0 outbound traffic:

```
R1(config)# access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

Applied to R2 S0/0/0 outbound traffic:

```
R2(config)# access-list 101 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

Task 5 – konfigurácia Crypto mapy



Tasks to Configure IPsec:

Task 1: Ensure that ACLs are compatible with IPsec.
Task 2: Create ISAKMP (IKE) policy.
Task 3: Configure IPsec transform set.
Task 4: Create a crypto ACL.
Task 5: Create and apply the crypto map.

Crypto maps define the following:

- ACL to be used
- Remote VPN peers
- Transform set to be used
- Key management method
- SA lifetimes

Task 5 – konfigurácia Crypto mapy


```
router(config)#
```

```
crypto map map-name seq-num ipsec-manual
```

```
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]
```

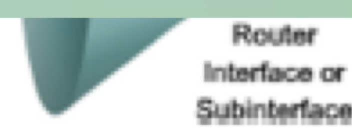
crypto map Parameters

Command Parameters	Description
map-name	Defines the name assigned to the crypto map set or indicates the name of the crypto map to edit.
seq-num	The number assigned to the crypto map entry.
ipsec-manual	Indicates that ISAKMP will not be used to establish the IPsec SAs.
ipsec-isakmp	Indicates that ISAKMP will be used to establish the IPsec SAs.
cisco	(Default value) Indicates that CET will be used instead of IPsec for protecting the traffic.
dynamic	(Optional) Specifies that this crypto map entry references a preexisting static crypto map. If this keyword is used, none of the crypto map configuration commands are available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.

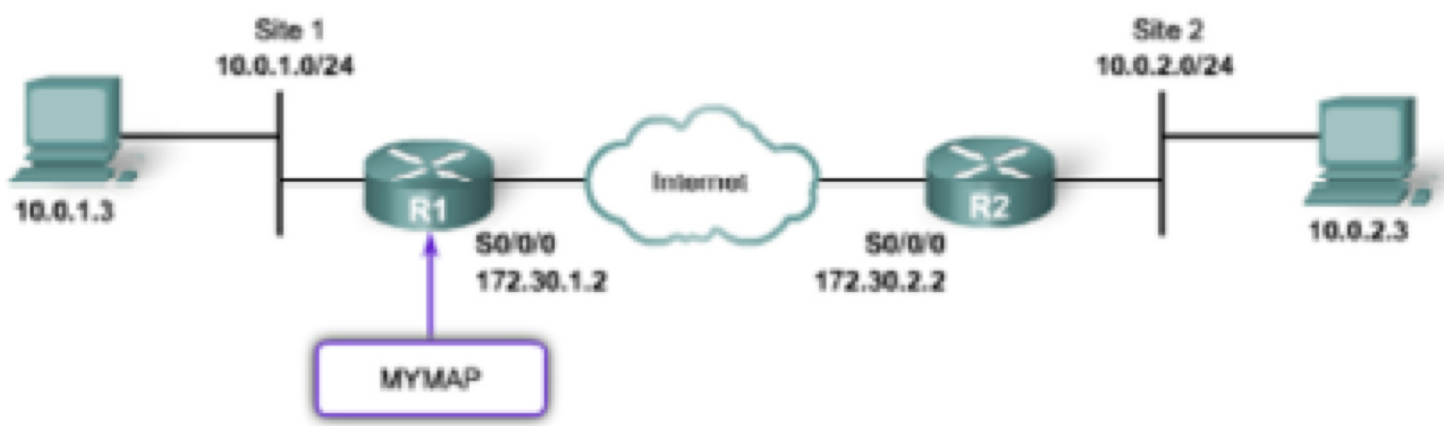
Task 5 – konfigurácia Crypto mapy

crypto map Configuration Mode Commands

Command	Description
set	Used with the **peer**, **pfs**, **transform-set**, and **security-association** commands.
peer [*hostname* | *ip-address*]	Specifies the allowed IPsec peer by IP address or hostname.
pfs [**group1** | **group2**]	Specifies DH Group 1 or Group 2.
transform-set [*set_name(s)*]	Specify list of transform sets in priority order. When the **ipsec-manual** parameter is used with the **crypto map** command, then only one transform set can be defined. When the **ipsec-isakmp** parameter or the **dynamic** parameter is used with the **crypto map** command, up to six transform sets can be specified.
security-association lifetime	Sets SA lifetime parameters in seconds or kilobytes.
match address [*access-list-id* | *name*]	Identifies the extended ACL by its name or number. The value should match the access-list-number or name argument of a previously defined IP-extended ACL being matched.
no	Used to delete commands entered with the **set** command.
exit	Exits crypto map configuration mode.

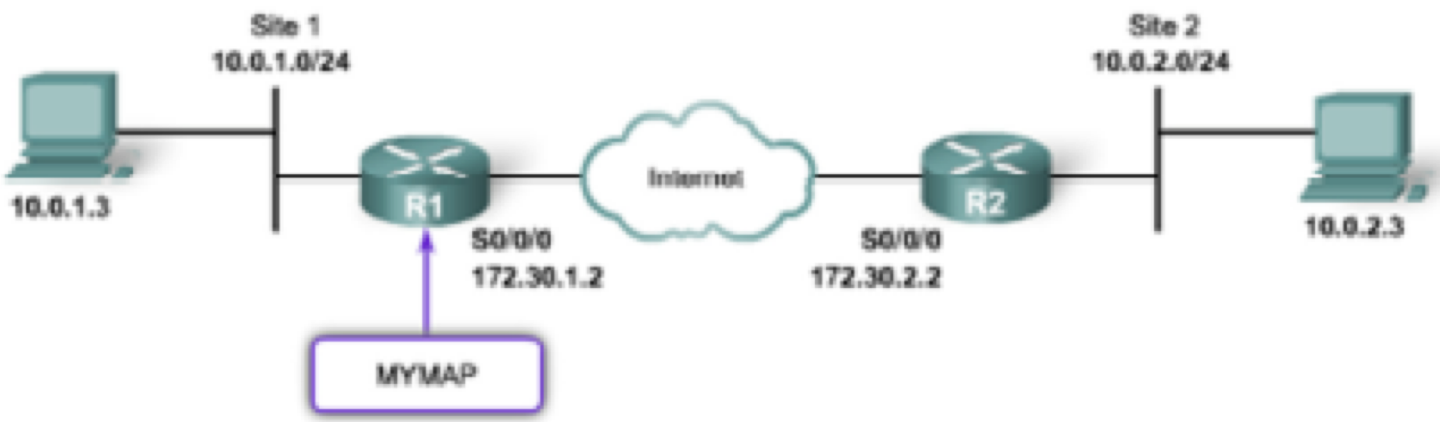


Task 5 – konfigurácia Crypto mapy




```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set mine
R1(config-crypto-map)# set security-association lifetime seconds 86400
```


Task 5 – konfigurácia Crypto mapy




```
router(config-if)#
crypto map map-name
```

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map MYMAP
```

- Multiple peers can be specified for redundancy.

Overenie a troubleshooting IPSec

router#

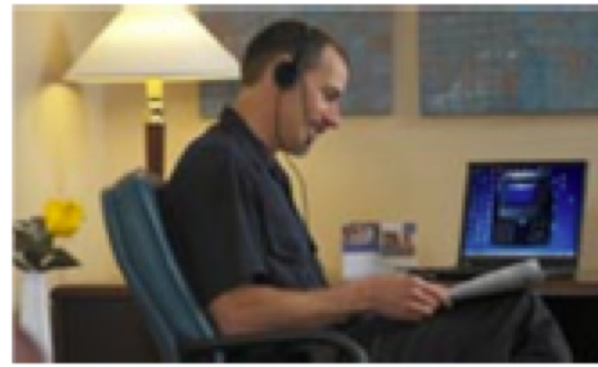
```
debug crypto isakmp
```

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0 1d00h: ISAKMP
(0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer
at 172.30.2.2
```

- This is an example of the Main Mode error message.
- The failure of Main Mode suggests that the Phase 1 policy does not match on both sides.
- Verify that the Phase 1 policy is on both peers and ensure that all the attributes match.

Vzdialený prístup

- Poskytuje flexibilitu
- Používateľ môže byť fyzicky na ľubovoľnom mieste



Teleworking Benefits:

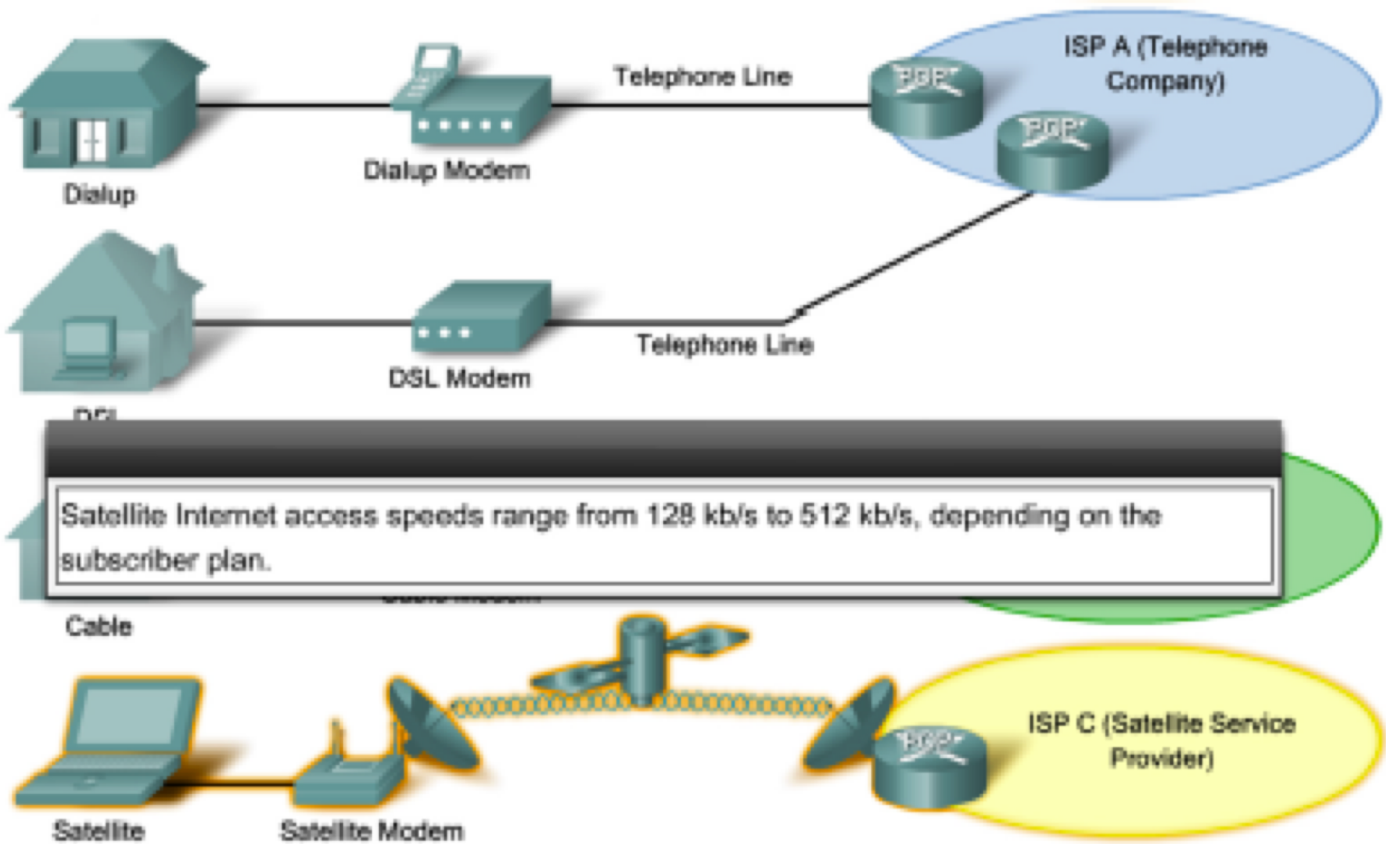
Organizational benefits:
- Continuity of operations
- Increased responsiveness
- Secure, reliable, and manageable access to information
- Cost-effective integration of data, voice, video, and applications
- Increased employee productivity, satisfaction, and retention

Social benefits:
- Increased employment opportunities for marginalized groups
- Less travel and commuter related stress

Environmental benefits:
- Reduced carbon footprints, both for individual workers and organizations

Vzdialený prístup

- Pre vzdialený prístup je potrebné vysokorýchlostné pripojenie

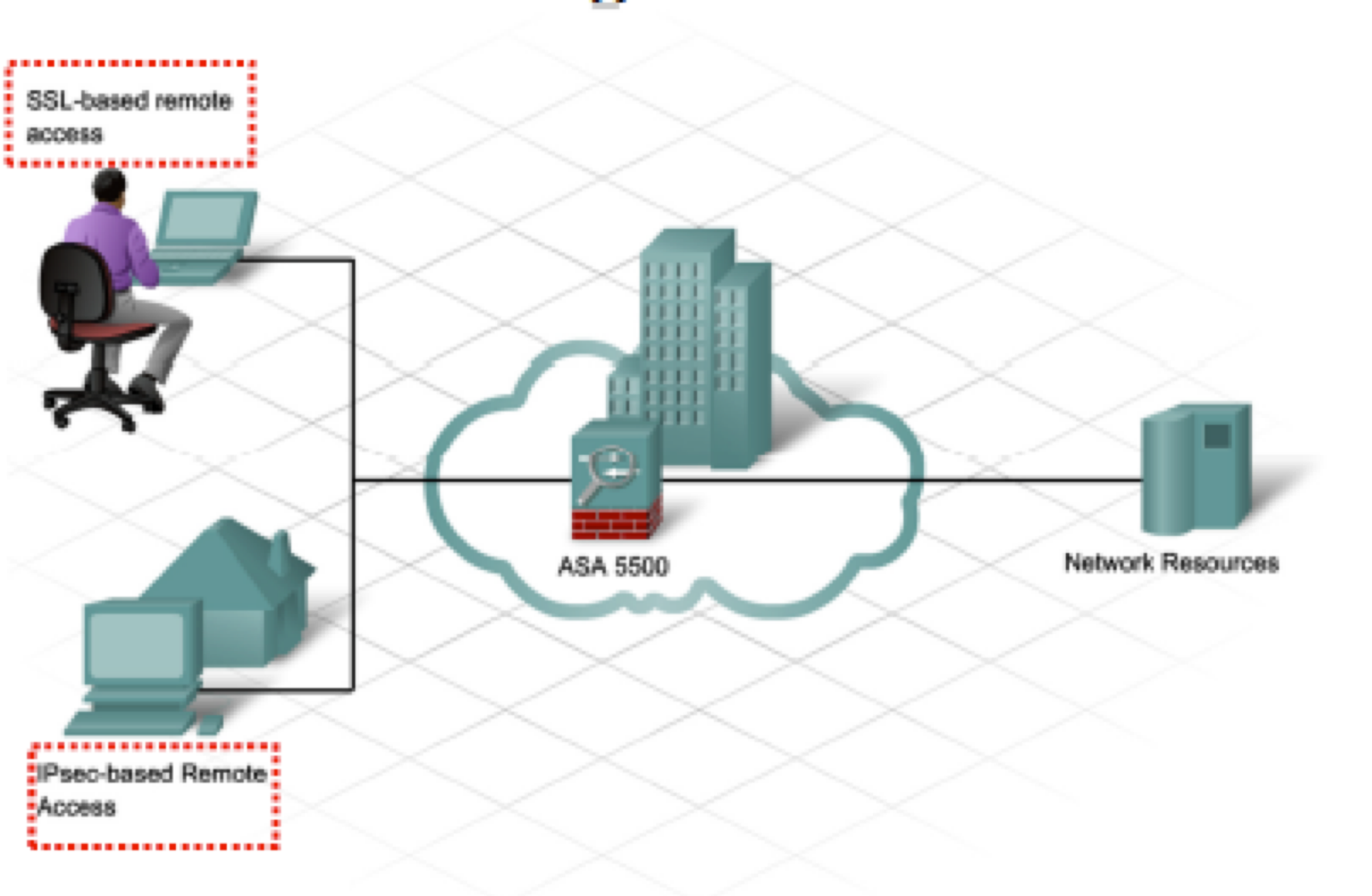


Broadbandový prístup

- Dostup siete 24/7
- Podpora služieb Voice&Video
- Vysokorýchlostný prístup
- Najčastejšie používané: DSL – variácií je viacero
  - ADSL je asymetrický (download > upload)
  - Rýchlosť ADSL je zvyčajne > T1
  - Rýchlosť závisí od vzdialenosti

Remote-access VPN

- Dve základné kategórie remote-access VPN

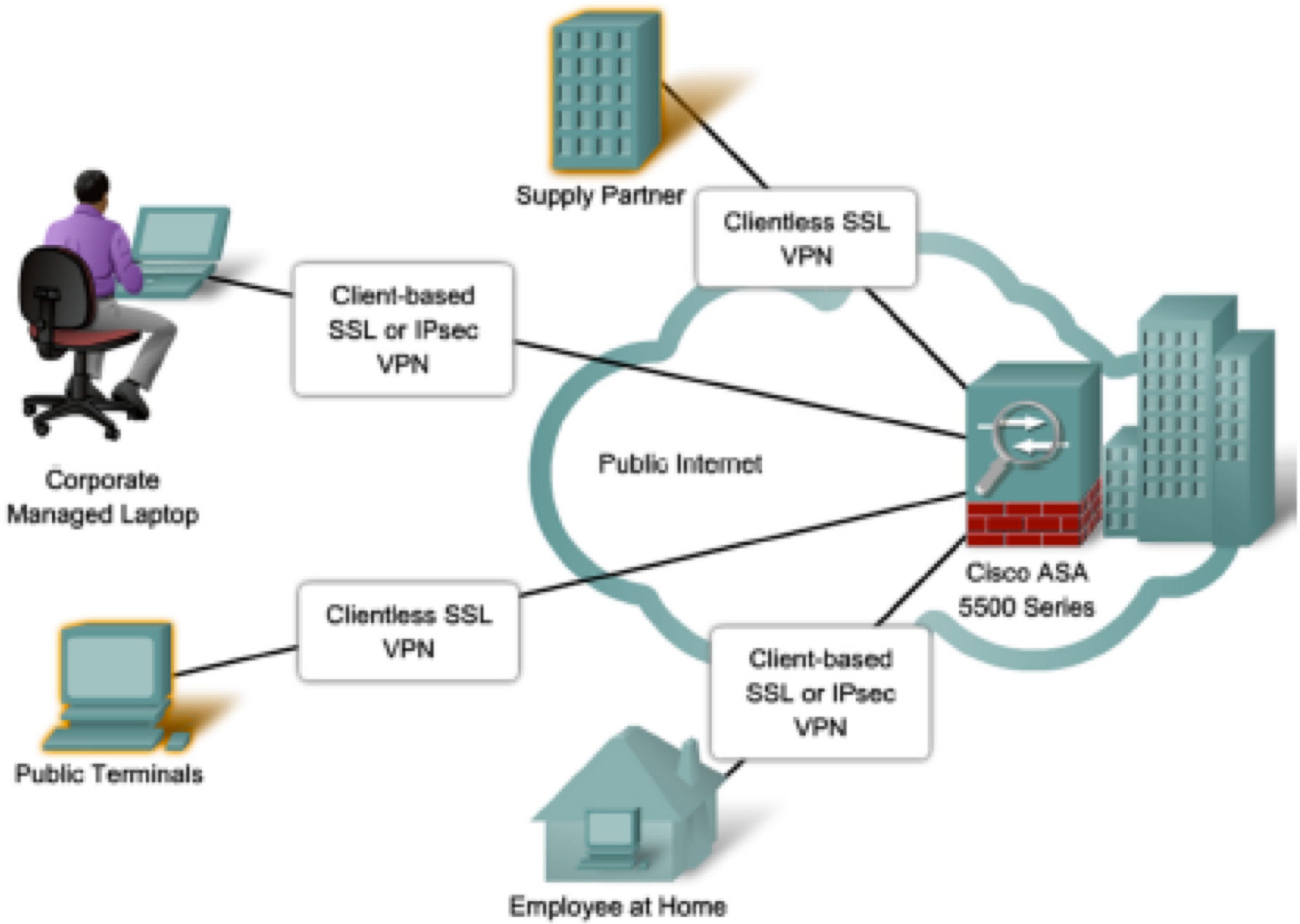


Remote-access VPN

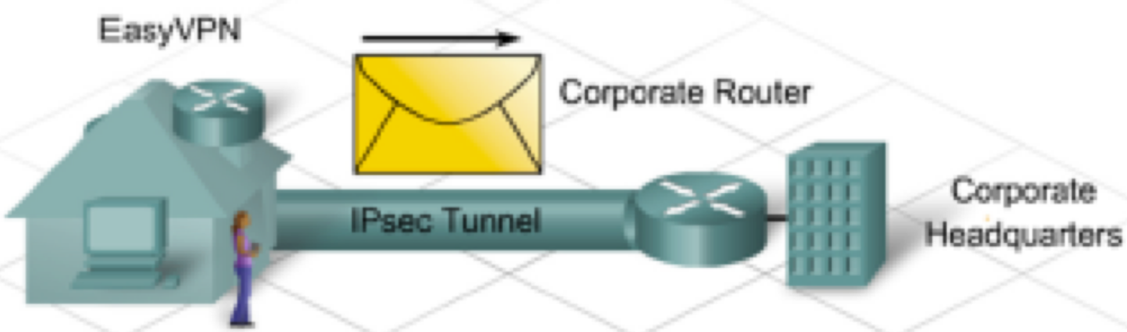
- Dve základné kategórie remote-access VPN

	SSL	IPsec
Applications	Web-enabled applications, file sharing, Email	All IP-based applications
Encryption	Moderate Key lengths from 40 bits to 128 bits	Stronger Key lengths from 56 bits to 256 bits
Authentication	Moderate One-way or two-way authentication	Strong Two-way authentication using shared secrets or digital certificates
Ease of Use	Very high	Moderate Can be challenging to nontechnical users
Connection Options	Any device can connect	Only specific devices with specific configurations can connect

SSL VPN


Supply Partner
Clientless SSL VPN
Corporate Managed Laptop
Client-based SSL or IPsec VPN
Public Internet
Cisco ASA 5500 Series
Clientless SSL VPN
Public Terminals
Client-based SSL or IPsec VPN
Employee at Home

Cisco EasyVPN



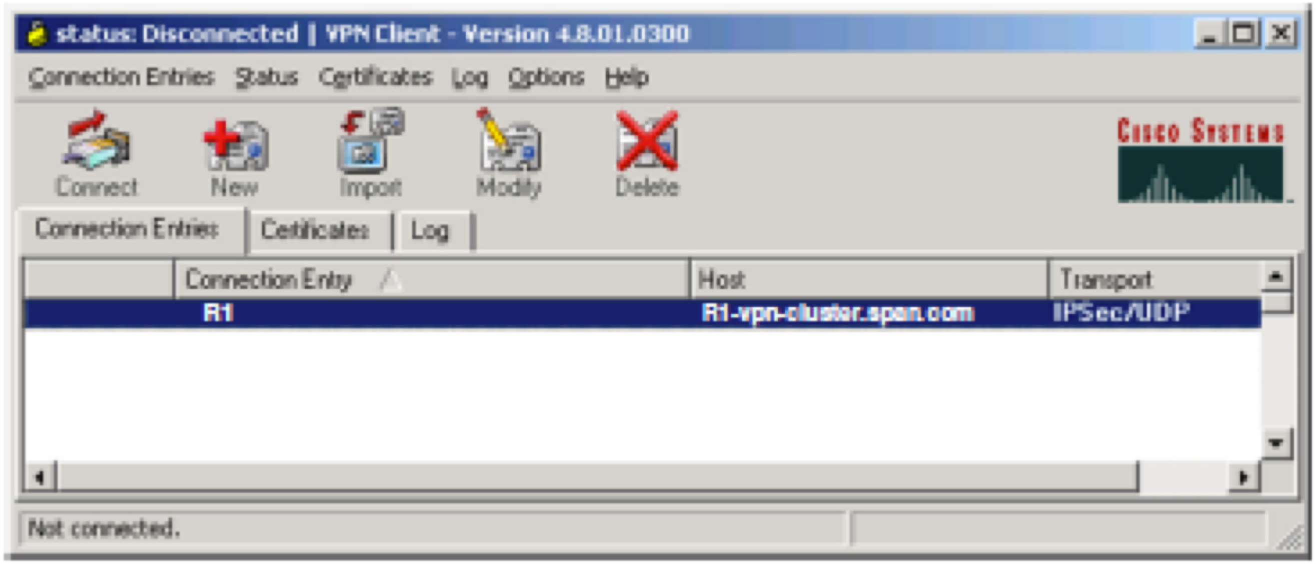
Cisco Easy VPN

- Negotiates tunnel parameters
- Establishes tunnels according to set parameters
- Authenticates users by usernames, group names, and passwords
- Manages security keys for encryption and decryption
- Authenticates, encrypts, and decrypts data through the tunnel

Komponenty:

Cisco EasyVPN Server | Cisco EasyVPN Remote | Cisco EasyVPN Client

EasyVPN Client



- Zabezpečuje end-to-end šifrované spojenie
- Je kompatibilný so všetkými Cisco VPN produktmi

Implementácia techník filtrovania sieťovej prevádzky

Filtre sieťovej prevádzky

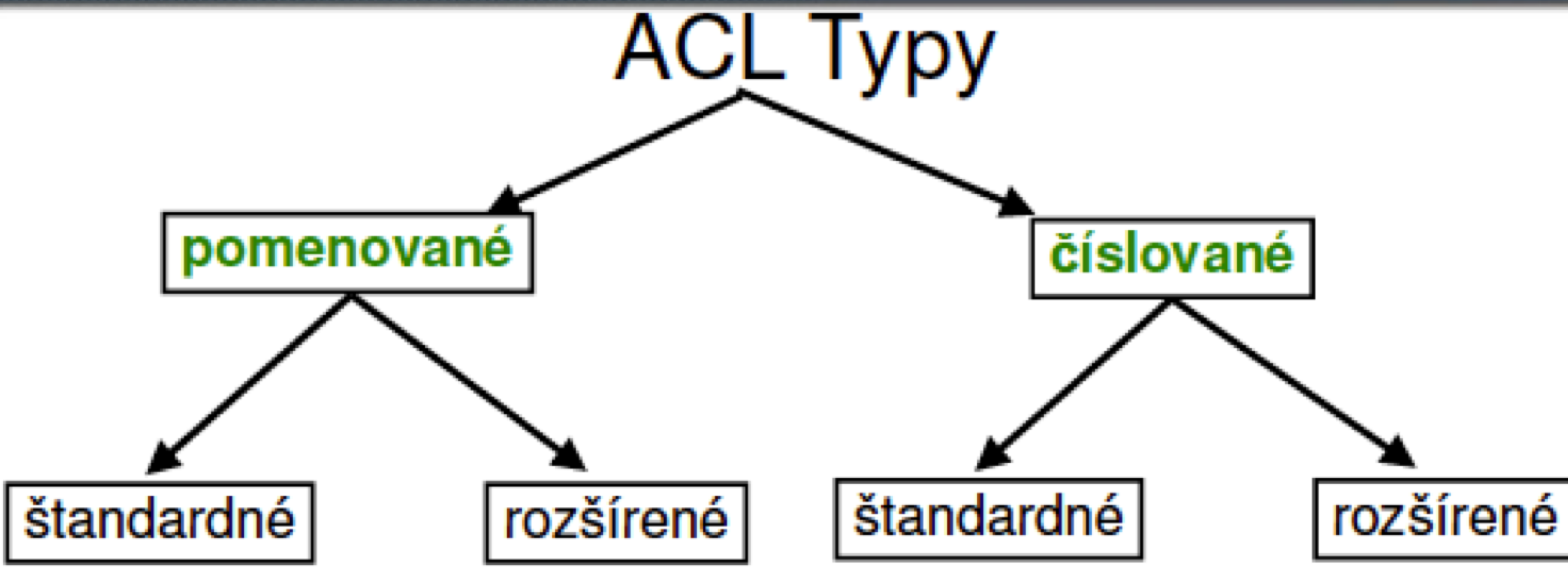
Historický vývoj filtrov sieťovej prevádzky:

- Štandardné a rozšírené ACL
- Funkcionalita TCP established v ACL
- Reflexívne ACL
- Dynamické ACL
- Time-based ACL
- CBAC
- Zone-based policy firewall

Typy ACL

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
DECnet and Extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Ethernet address	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Extended transparent bridging	1100-1199

Typy ACL



- **Štandardné** – rozhodnutie je realizované iba na základe zdroja (sieť, host)
- **Rozšírené** – rozhodovanie na základe komplexnejších kritérií:
  - zdrojová a cieľová adresa hosta / siete
  - použitý protokol
  - v prípade TCP/UDP kontrola použitého portu

ACL voľba LOG

Router(config)#

access-list 101 permit ip any any *log*

```
*May 1 22:12:13.243: %SEC-6-IPACCESSLOGP:
list ACL-IPv4-E0/0-IN permitted tcp
192.168.1.3(1024) -> 192.168.2.1(22), 1
packet

*May 1 22:17:16.647: %SEC-6-IPACCESSLOGP:
list ACL-IPv4-E0/0-IN permitted tcp
192.168.1.3(1024) -> 192.168.2.1(22), 9
packets
```

Poznámka

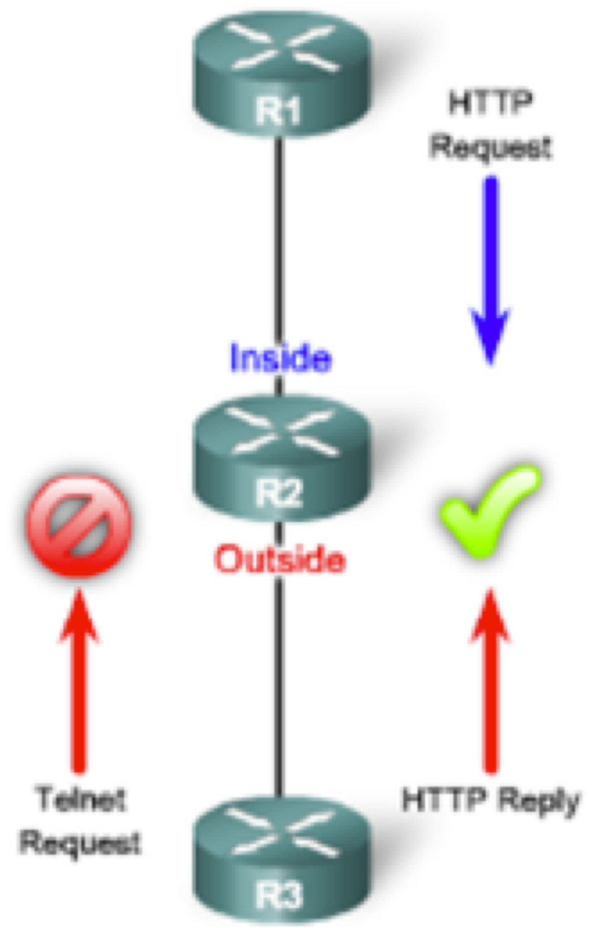
- **Outbound ACL** filtre sa nevzťahujú na prevádzku generovanú samotným zariadením

- Pre filtrovanie smerovacích aktualizácií je potrebné nakonfigurovať filttre v smerovacích protokoloch (distribučné listy)

TCP established a reflexívne ACL

Types of ACLs

- Standard IP ACLs
- Extended IP ACLs
- Extended IP ACLs using TCP **established**
- Reflexive IP ACLs
- Dynamic ACLs
- Time-Based ACLs
- Context-based Access Control (CBAC) ACLs



Konfigurácia TCP established

Router(config)# **access-list** {100-199} {permit | deny} protocol source-addr [source-wildcard] [operator operand] destination-addr [destination-wildcard] [operator operand] **[established]**

Voľba ***established*** umožňuje kontrolovať prichádzajúce IP packety z vonku siete a v prípade detekcie príznaku ACK alebo RST v hlavičkách TCP identifikuje komunikáciu ako spojenie nadviazané z vnútra siete (ide o odpoveď)

TCP established je použiteľné iba pre TCP, pre UDP je nekontrolovateľné bez hĺbkovej inšpekcie, či bolo spojenie nadviazané zvnútra

Reflexívne ACL

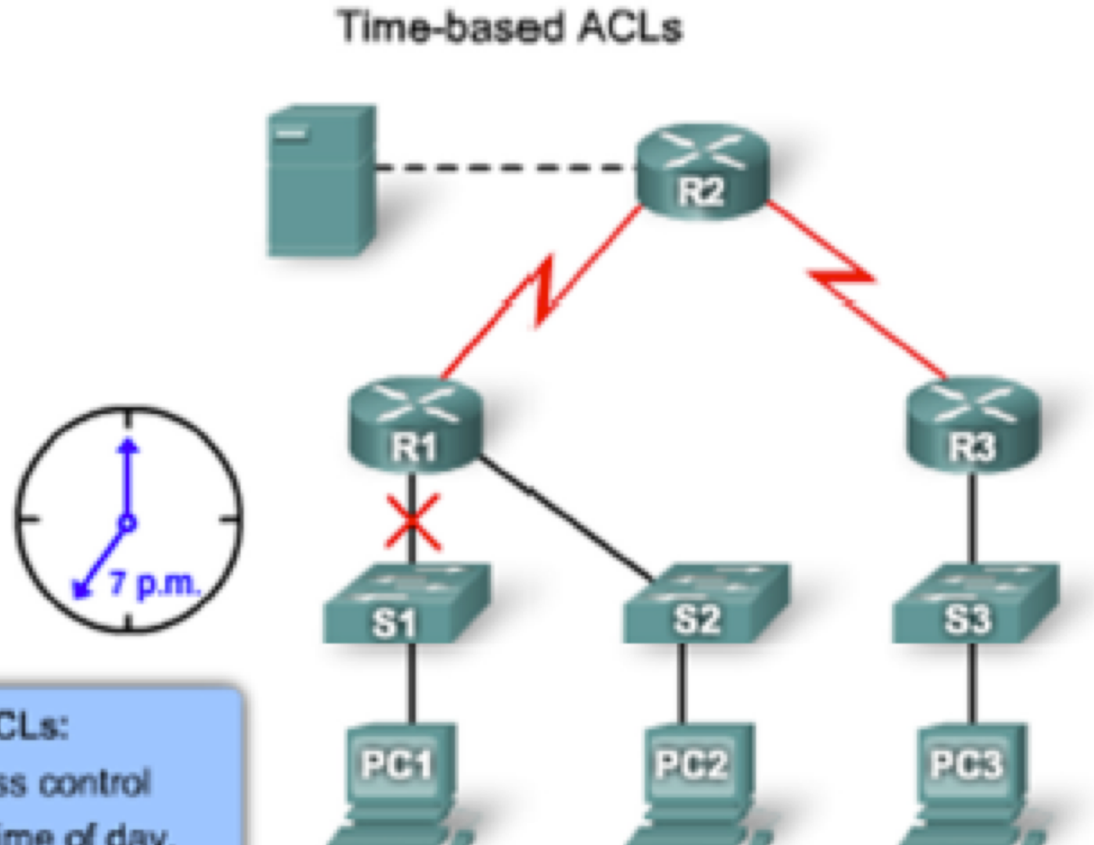
Step 1	R2(config)#ip access-list extended OUTBOUNDFILTERS R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC
Step 2	R2(config)#ip access-list extended INBOUNDFILTERS R2(config-ext-nacl)# evaluate TCPTRAFFIC R2(config-ext-nacl)# evaluate ICMPTRAFFIC
Step 3	R2(config)#interface S0/1/0 R2(config-if)#ip access-group INBOUNDFILTERS in R2(config-if)#ip access-group OUTBOUNDFILTERS out

Dynamické ACL

- Umožňujú dynamicky zavádzať pravidlá do ACL v prípade, že sa používateľ úspešne autentifikuje

- Autentifikácia môže prebehnúť voči lokálnej databáze, alebo voči centrálnemu serveru (radius/tacacs)

Časovo založené ACL



Time-based ACLs:
Allow for access control based on the time of day, day of the week, or day of the month.

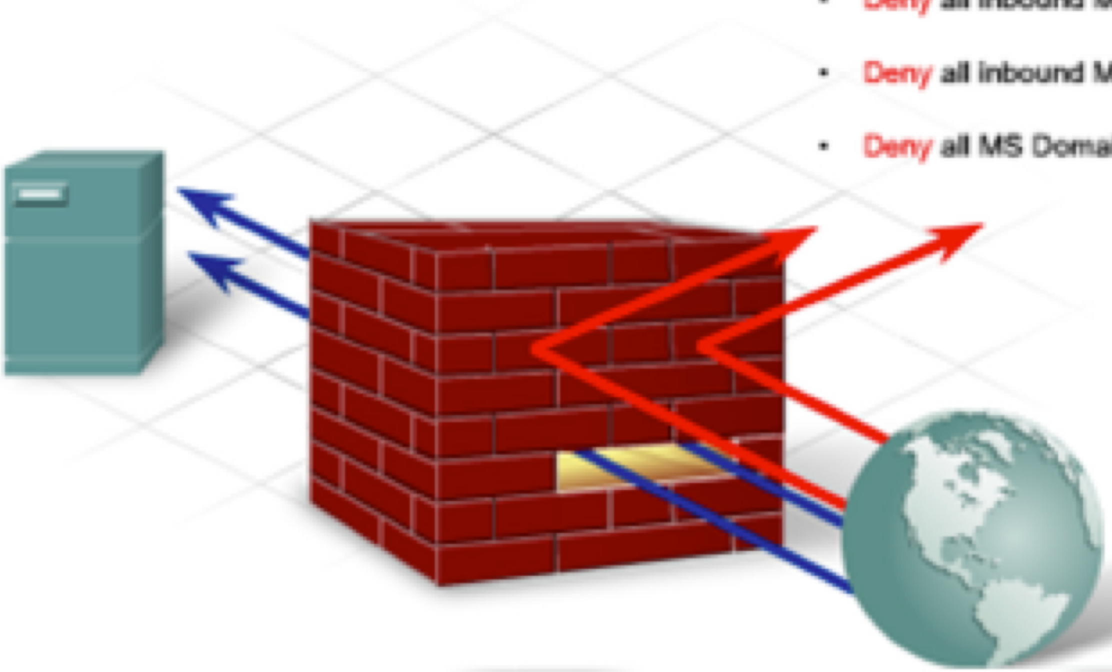
Firewally

- Úlohou je filtrovať sieťovú prevádzku
- Prvý firewall (paketový filter) bol vytvorený DEC-om v r. 1988
- V r. 1989 AT&T Bell laboratories navrhli prvý stavový firewall

Implementácia filtrovacích pravidiel

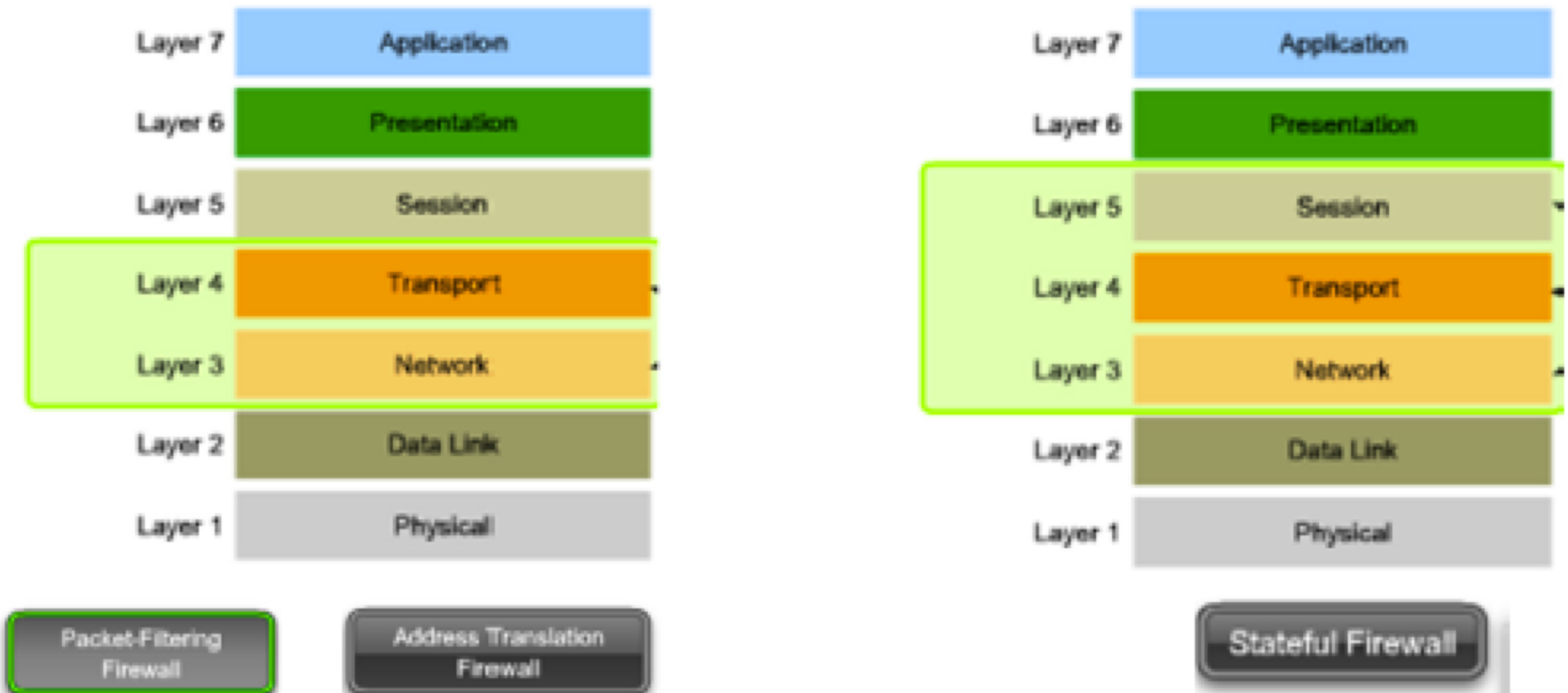
- Allow web traffic from any external address to the web server
- Allow traffic to FTP server
- Allow traffic to SMTP server
- Allow traffic to internal IMAP server

- Deny all inbound traffic with network addresses matching internal-registered IP addresses
- Deny all inbound traffic to server from external addresses
- Deny all inbound ICMP echo request traffic
- Deny all inbound MS Active Directory
- Deny all inbound MS SQL server ports
- Deny all MS Domain Local Broadcasts

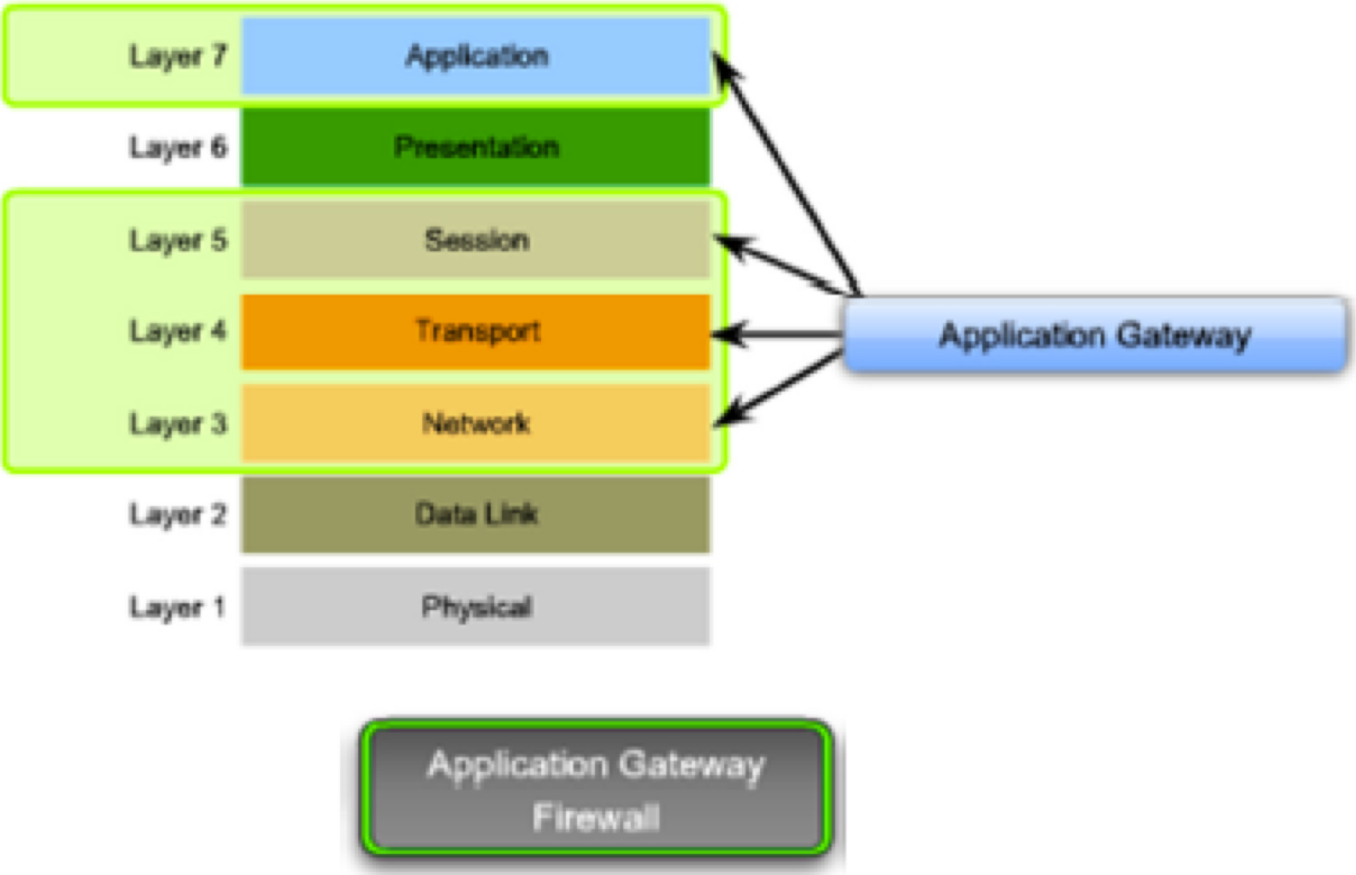


Typy firewallov

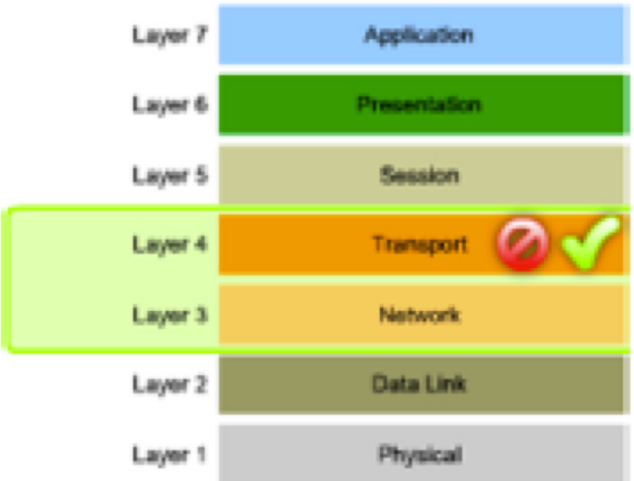
www.cnl.tuke.sk



Typy firewallov

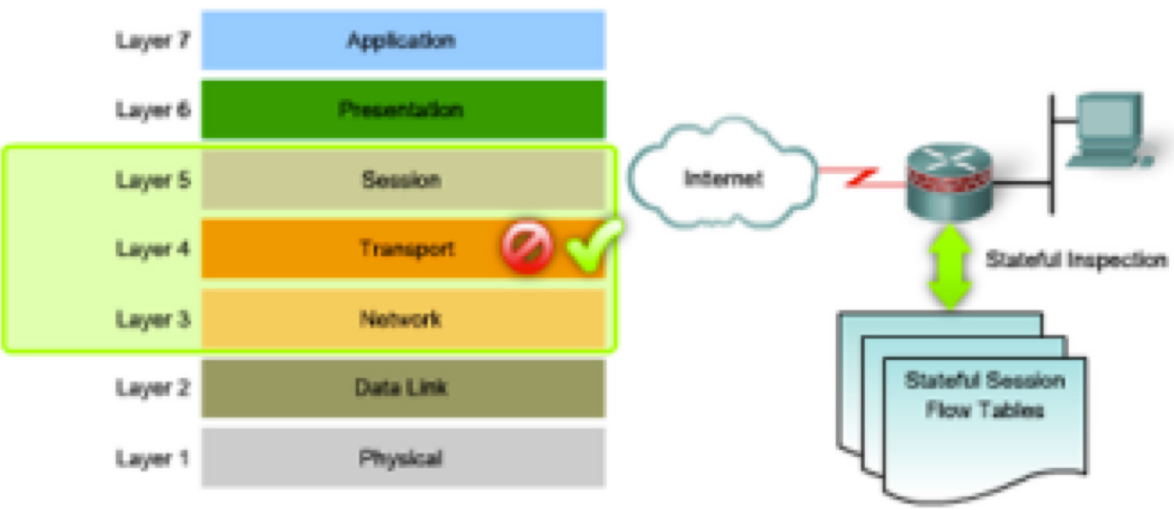


Paketové filtre (nestavové firewally)



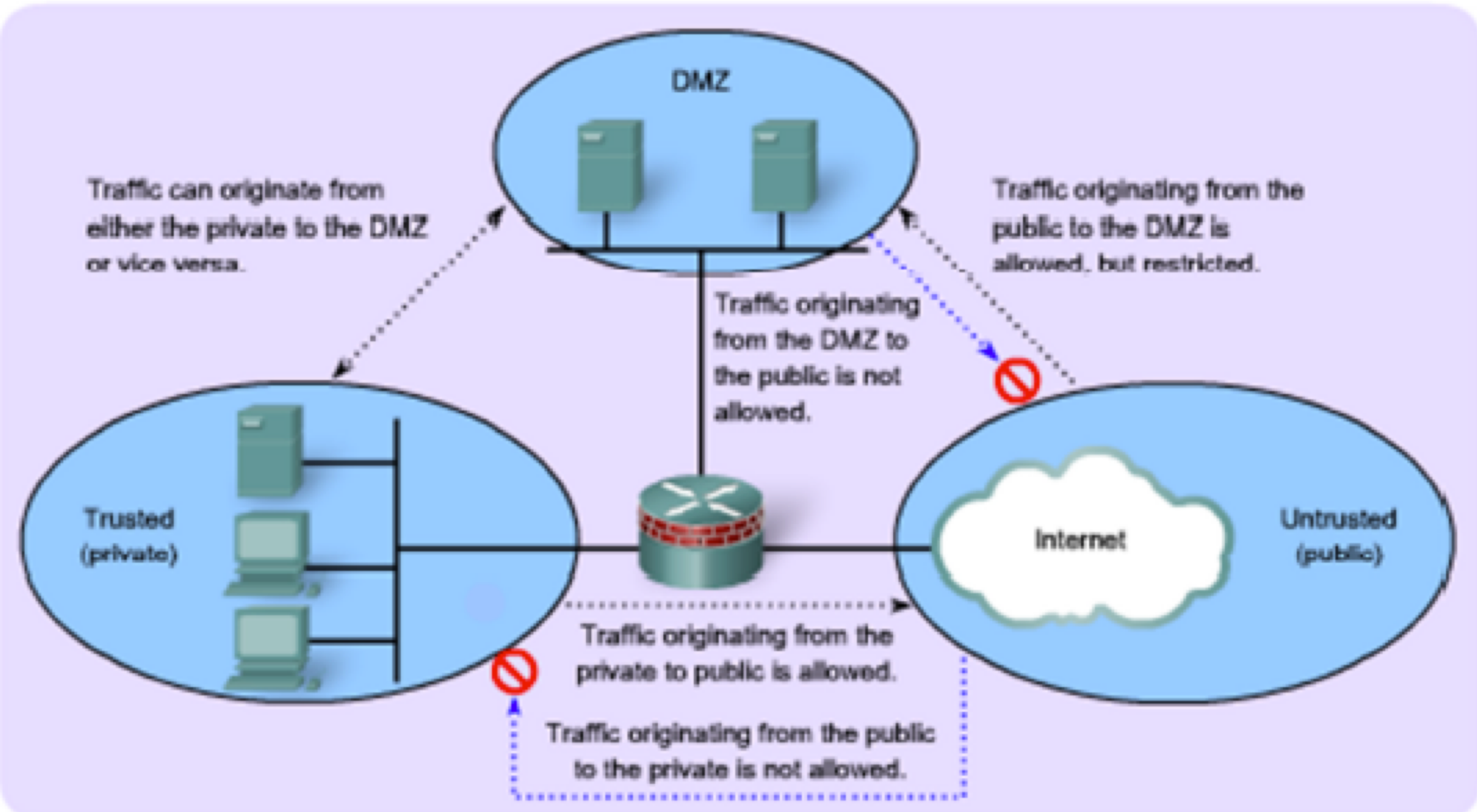
- Jednoducho zavádzané pravidlá
- Nezaťažujú zariadenie tak ako filtre s hĺbkovou analýzou prevádzky
- Základnú úroveň zabezpečenia siete je možné vytvoriť práve paketovým filtrom
- Problém predstavujú fragmentované dáta (hlavička je súčasťou iba prvého fragmentu)

Stavové firewally

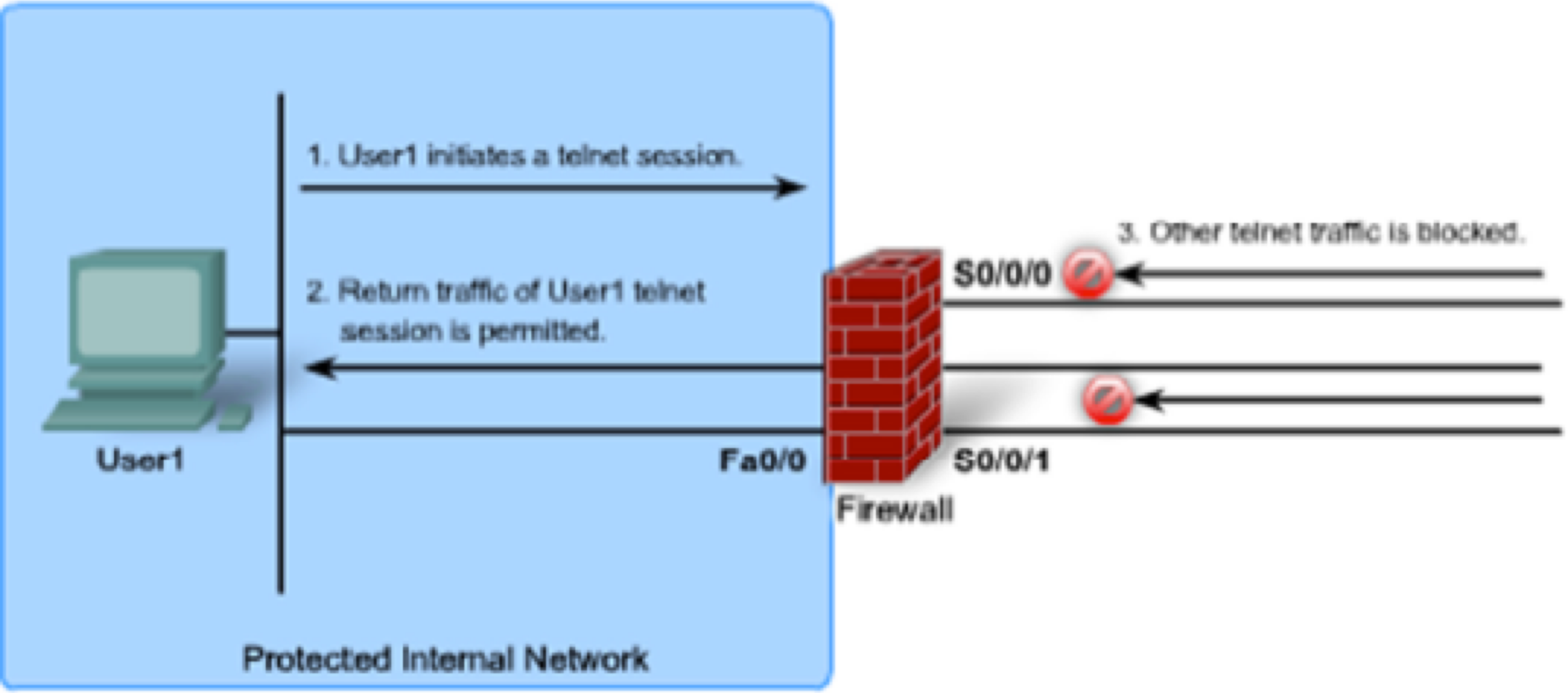


- Do osobitnej tzv. „flow table“ evidujú informácie o spojeniach nadviazaných z vnútra siete
- Dynamicky zavádzajú záznamy do inbound ACL pre spätnú komunikáciu

Design sietí s firewallmi - DMZ



Context Based Access Control (CBAC)



CBAC ako IPS

- CBAC dokáže blokovať half-open spojenia (chráni pred SYN flood útokom)
- CBAC dokáže analyzovať prevádzku na prítomnosť známych vzoriek komunikácií (napr. prenos vírusu) a aktívne prevádzku blokovať
- Pri blokovaní prevádzky dokáže logovať na Syslog server

Schopnosti CBAC

Monitors TCP Connection Setup
Examines TCP Sequence Numbers

Inspects DNS Queries and Replies

Inspects Common ICMP Message Types

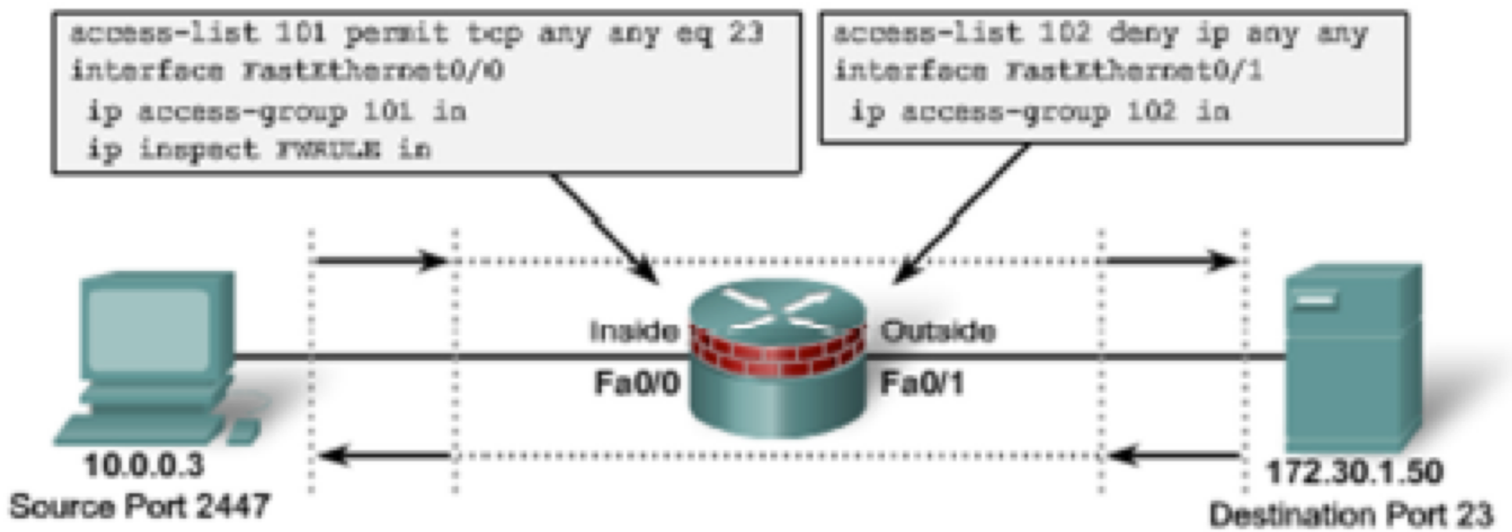
Supports Applications with Multiple Channels, such as FTP and Multimedia

Inspects Embedded Addresses

Inspects Application Layer Information

- *CBAC can limit the interaction between two devices, for example, limiting SMTP commands between two email servers.*
- CBAC uses timeout and threshold values to inspect the setup of TCP connections to prevent DoS attacks. When thresholds are reached, the IOS can start dropping incomplete connections, generate an alert, and/or block the TCP traffic.

CBAC



TCP traffic is inspected by FWRULE.

1

```
ip inspect FWRULE in
```

Firewall creates a dynamic ACL allowing return traffic back through the firewall.

2

```
access-list 102 permit tcp host 172.30.1.50 eq 23 host 10.0.0.3 eq 2447
```

3 Firewall continues to inspect control traffic and dynamically creates and removes ACLs as required by the application. It also monitors and protects against application-specific attacks.

4 Firewall detects when an application terminates or times out and removes all dynamic ACLs for that session.

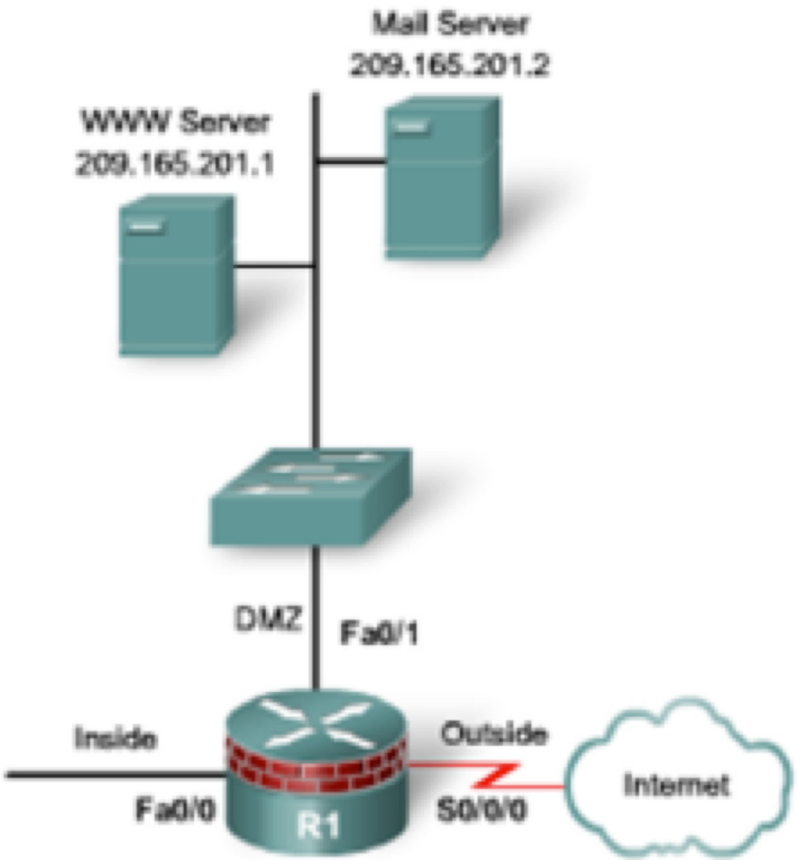
Konfigurácia CBAC


```
Router(config)#
ip inspect name inspection_name protocol [alert {on | off}] [audit-trail {on | off}]
[timeout seconds]
```

Parameter	Description
inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name for the rules.
protocol	The protocol to inspect.
alert {on | off}	(Optional) For each inspected protocol, the generation of alert messages can be set to on or off. If no option is selected, alerts are generated based on the setting of the **ip inspect alert-off** command.
audit-trail {on | off}	(Optional) For each inspected protocol, the **audit-trail** option can be set to on or off. If no option is selected, **audit trail** messages are generated based on the setting of the **ip inspect audit-trail** command.
timeout *seconds*	(Optional) Specify the number of seconds for a different idle timeout to override the global TCP or UDP idle timeouts for the specified protocol. This timeout overrides the global TCP and UDP timeouts but does not override the global Domain Name Service (DNS) timeout.

Konfigurácia CBAC

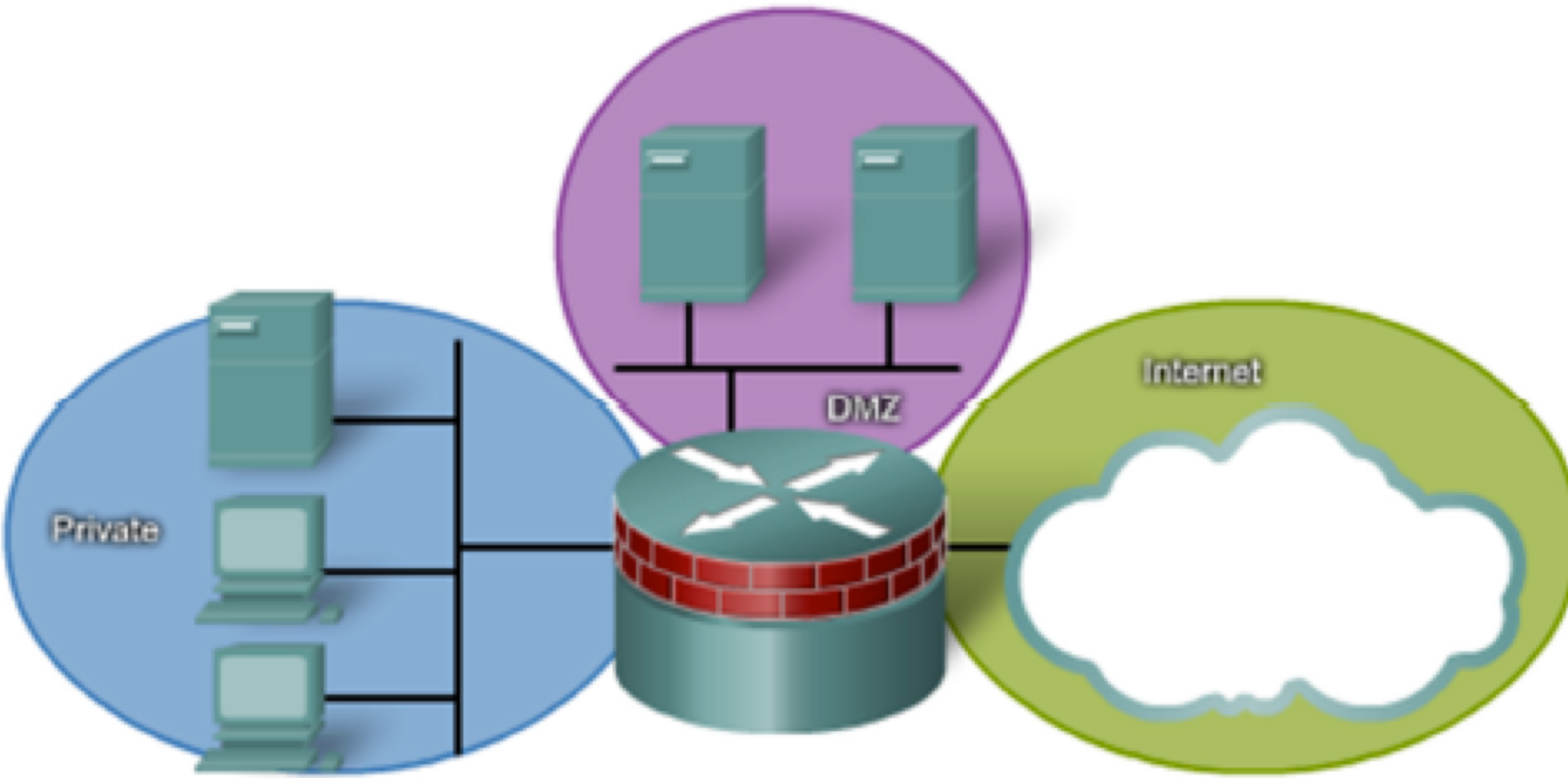

```
ip inspect name MYSITE tcp
ip inspect name MYSITE udp
!
interface FastEthernet0/0
  ip address 10.10.10.254 255.255.255.0
  ip access-group 101 in
  ip inspect MYSITE in
!
interface FastEthernet0/1
  ip address 209.165.201.30 255.255.255.224
!
interface Serial0/0/0
  ip address 209.165.200.225 255.255.255.224
  ip access-group 102 in
!
access-list 101
  permit tcp 10.10.10.0 0.0.0.255 any
  permit udp 10.10.10.0 0.0.0.255 any
  permit icmp 10.10.10.0 0.0.0.255 any
  deny ip any any
!
access-list 102
```



Zone-Based Policy Firewall

- Zavedený v r. 2006 v IOSoch 12.4(6)T
- Zaradzuje rozhrania do zón
- Aplikuje filtrovacie pravidlá medzi zónami
- ZBPFW Poskytuje:
  - Stavovú kontrolu
  - Hĺbkovú inšpekciu na aplikačnej vrstve
  - URL filtering
  - Ochrana pred DoS

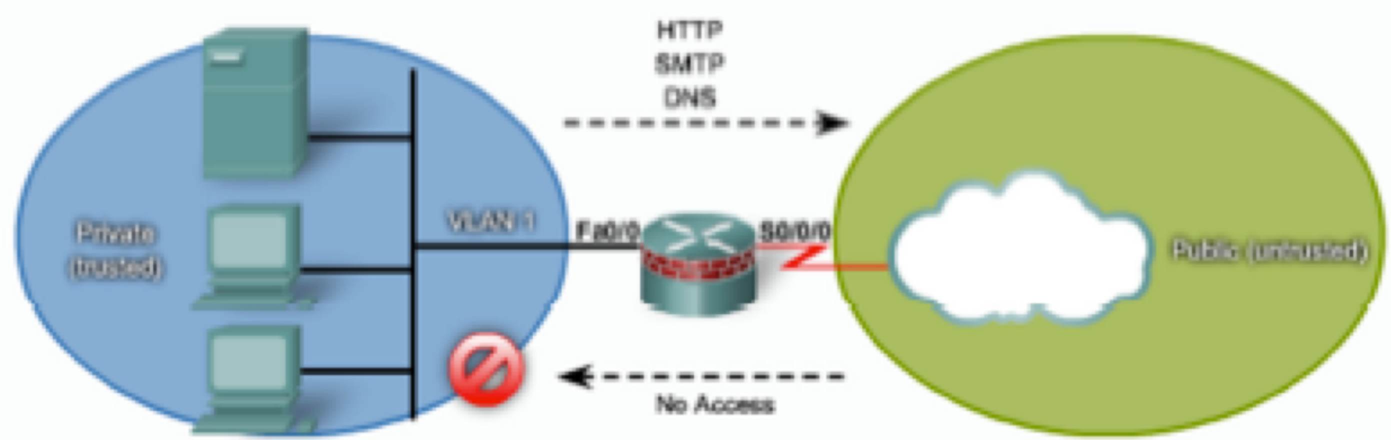
Zone-Based Policy Firewall



– Ochrana pred DoS

Zone-Based Policy Firewall

- Filtrovacie politiky sa definujú prostredníctvom jazyka C3PL (Cisco Common Classification Policy Language)



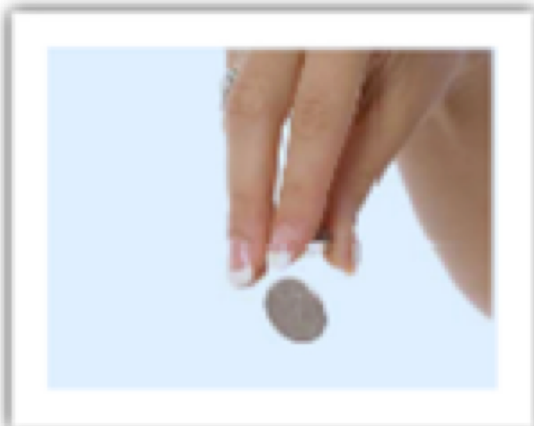
- The private zone must reach the Internet, with access to HTTP, SMTP, and DNS services.
- The public zone should not have any inbound access.

Voľby zone-based policy firewallu

- Inspect

  Ekvivalentné s IP inspect v CBAC. Automaticky povoľuje

Inspect



Drop

Pass

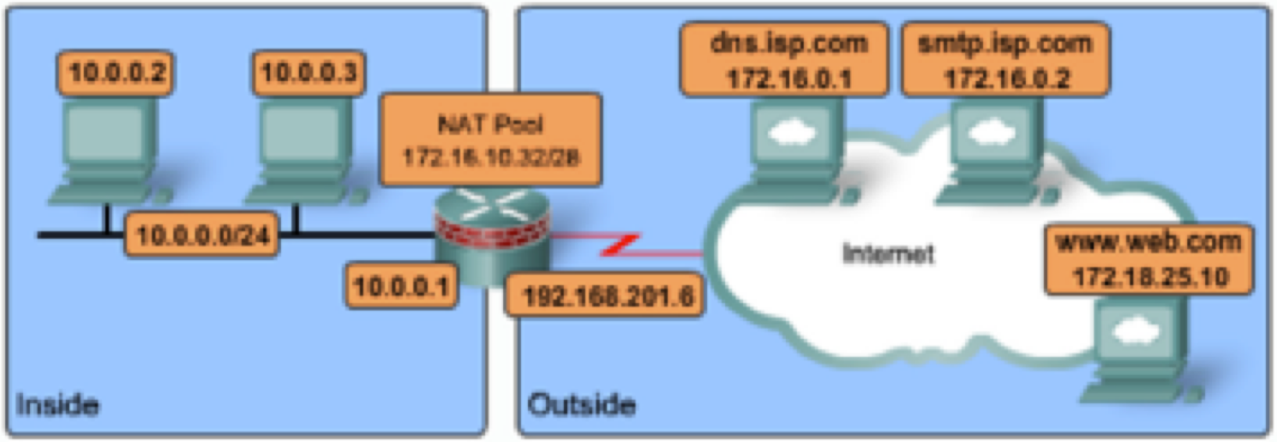
- Pass

  Ekvivalentné s *permit* pravidlom v ACL.

Pravidlá konfigurácie

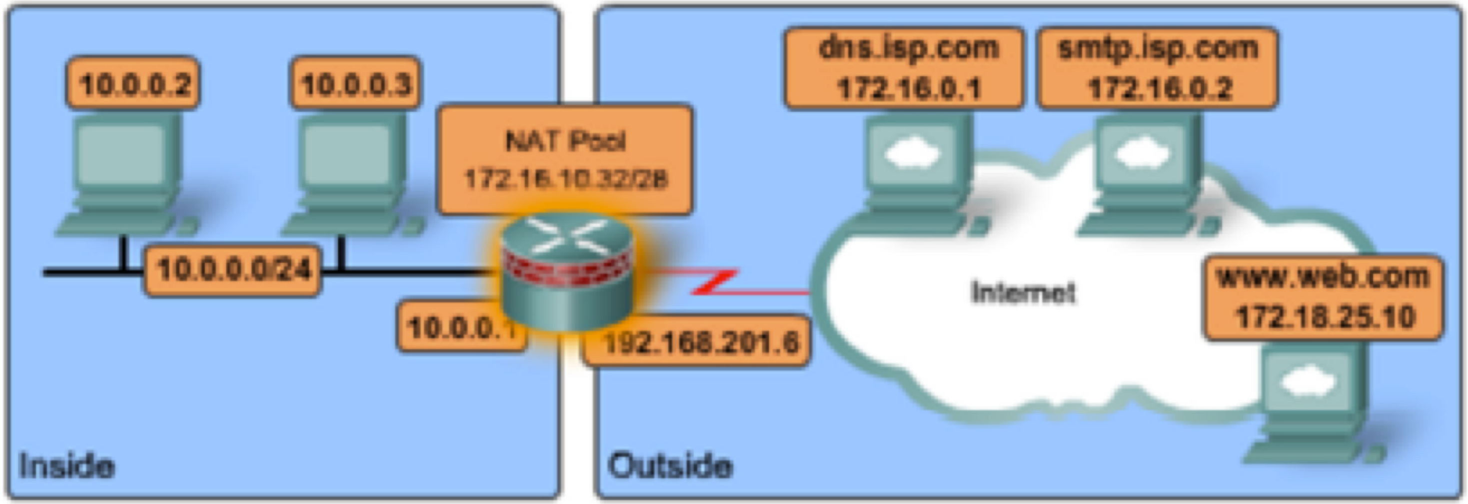
- Zóna musí byť nakonfigurovaná skôr ako sa rozhranie priradí k zóne
- Každé rozhranie smerovača musí byť členom nejakej zóny
- Jedno rozhranie môže patriť iba do jednej zóny
- Prevádzka v rámci jednej zóny tečie neobmedzene (nefiltrovane)
- Prevádzka neprechádza medzi rozhraniami z ktorých iba jedno patrí k zóne

Kroky k implementácii ZBPF



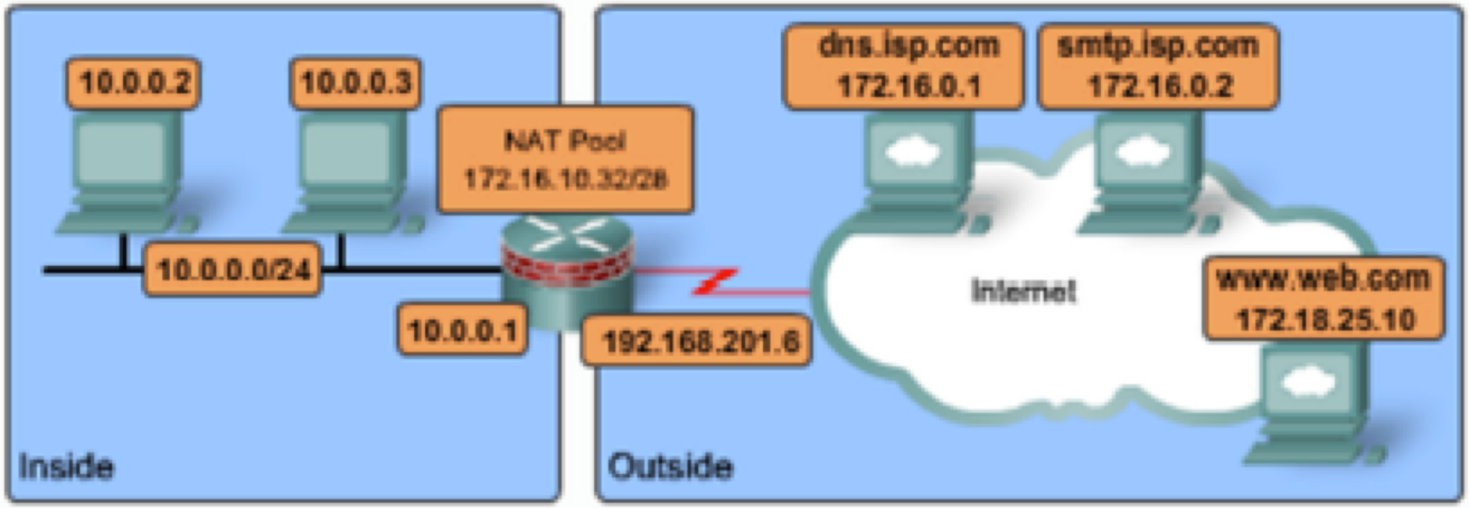
1. Vytvorenie zóny príkazom ***zone security***
2. Vytvorenie tried prevádzky príkazom ***class-map type inspect***
3. Špecifikovanie politík príkazom ***policy-map type inspect***
4. Aplikovanie filtrovacích pravidiel príkazom ***zone-pair security***
5. Priradenie rozhraní k zónam príkazom ***zone-member security***

Vytvorenie zón (príklad)




```
FW(config)# zone security Inside
FW(config-sec-zone)# description Inside network
FW(config)# zone security Outside
FW(config-sec-zone)# description Outside network
```

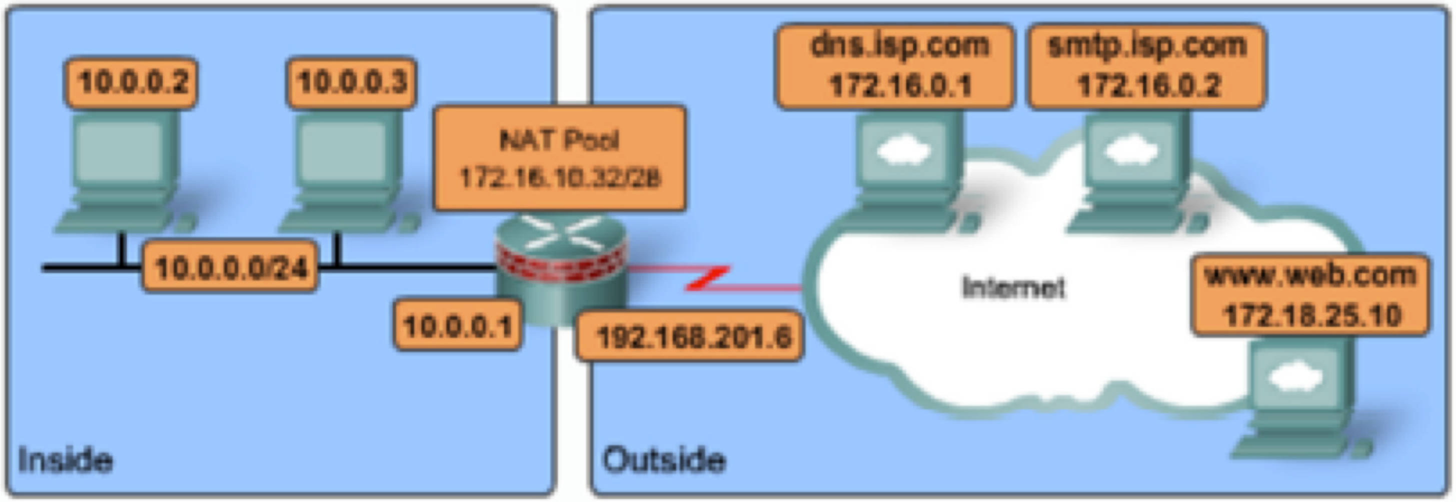
Definovanie tried prevádzky (príklad)




```
FW(config)# class-map type inspect FOREXAMPLE
FW(config-cmap)# match access-group 101
FW(config-cmap)# exit
FW(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255 any
```

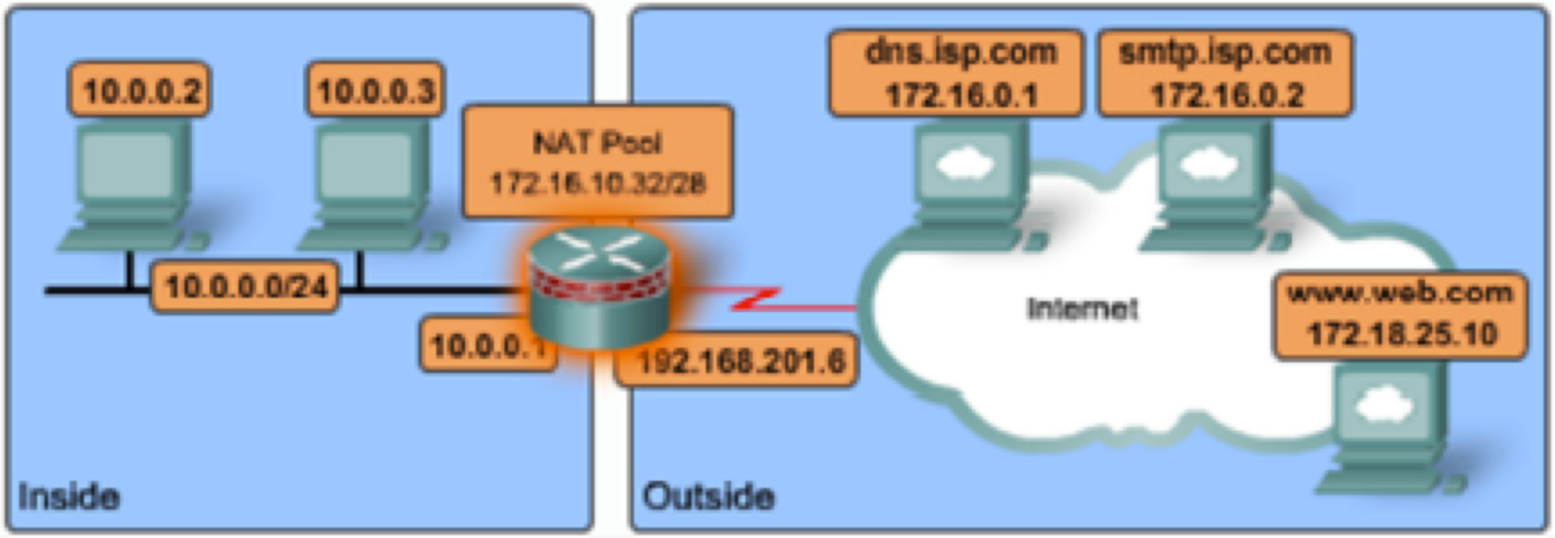
Rozšíriteľné o ***match protocol*** a ***match class-map*** pre nested-class

Špecifikovanie politík (príklad)




```
FW(config)# policy-map type inspect InsideToOutside
FW(config-pmap)# class type inspect FOREXAMPLE
FW(config-pmap-c)# inspect
```

Priradenie politík k zónam (príklad)




```
FW(config)# zone-pair security InsideToOutside source Inside destination Outside
FW(config-sec-zone-pair)# description Internet Access
FW(config-sec-zone-pair)# service-policy type inspect InsideToOutside
FW(config-sec-zone-pair)# interface F0/0
FW(config-if)# zone-member security Inside
FW(config-if)# interface S0/0/0.100 point-to-point
FW(config-if)# zone-member security Outside
```

Q and A