Naloga: IPsec tunel (LAN-LAN)

1. Uvod

Protokol IPSec je odprt standard, ki omogoča varno komunikacijo v omrežjih IP. Osnovna ideja je zaščita omrežnega sloja na podlagi varnostnih mehanizmov, ki podpirajo avtentikacijo, zaupnost, celovitost in kontrolo dostopa. Mehanizem zaščite je neodvisen od aplikacij, kar pomeni da je protokol transparenten za uporabnika in aplikacije. Z vidika povezave IPSec sta pomembni le začetna in končna točka varne zveze, ostali omrežni elementi, ki sodelujejo pri prenosu prometa, morajo poznati le običajen protokol IP. Protokol IPSec definira dva tipa varnih zveze oz. dva prenosna načina:

- tunelski način: omogoča zaščito celotnega paketa IP
- transportni način: omogoča zaščito podatkov višje ležečih protokolov

S protokolom IPSec lahko med seboj komunicirajo naslednje kombinacije naprav: terminal - terminal, terminal - varnostni prehod in varnostni prehod - varnostni prehod. Trenutno najbolj zanimiva aplikacija, ki jo omogoča protokol IPSec, je gradnja navideznih zasebnih omrežij (VPN - Virtual Private Networks).

1.1 Protokol IPSec na usmerjevalniku Cisco

Usmerjevalnik Cisco omogoča komunikacijo s protokolom IPSec, v tunelskem način varne zveze. Možen je tudi transporten način prenosa, toda le v primeru prenašanja upravljalskih podatkov, ki so potrebni za upravljanje samega usmerjevalnika. Nabor funkcionalnosti IPSec je sledeč:

- ročno vzpostavljanje varne zveze IPSec,
- avtomatsko vzpostavljanje, vzdrževanje in rušenje varne zveze IPSec s protokolom IKE. Nastavljivi parametri varne zveze IKE so sledeči:

Parametri varne zveze IKE	Razpoložljivi parametri
Avtentikacijska metoda	Predhodno izmenjani ključi, Digitalni podpis (RSA certifikati), Kriptirani podatki v načinu RSA
Enkripcijski algoritem	DES, 3DES, AES
Zgoščevalni algoritem	HMAC-MD5, HMAC-SHA-1
Življenjski čas varne zveze	Čas / sekunde
Skupina Diffie-Hellman	768-bitna, 1024-bitna

Tab. 1: *Parametri varne zveze IKE*

- zagotavljanje celovitosti in zasebnosti prenašanih paketov s protokoloma AH in ESP. Uporabljena avtentikacija nam avtomatsko zagotavlja zaščito pred podvajanjem prenašanih paketov. Nastavljivi parametri varne zveze IPSec so sledeči:

Parametri varne zveze IPSec		Razpoložljivi parametri
Protokol AH	Zgoščevalni algoritem	HMAC-MD5, HMAC-SHA-1
Protokol ESP	Zgoščevalni algoritem	HMAC-MD5, HMAC-SHA-1
	Enkripcijski algoritem	DES, 3DES, AES, NULL
Kompresija prenašanih paketov		LZS
Prenosni način		Tunelski, transportni
Življenjski čas varne zveze		Čas / sekunde, količina podatkov / Kbytes
Koncept poudarjene zaupnosti - PFS		

Tab. 2: *Parametri varne zveze IPSec*

2. Namen vaje

1. Nastavite osnove parametre usmerjevalnika in terminalne opreme.
2. Nastavite stikalo, da boste lahko opazovali promet, ki se posreduje med dvema usmerjevalnikoma. S protokolnim analizatorjem Wireshark opazujte prenašane pakete.
3. Vzpostavite tunelsko povezavo IPSec med varnostnima prehodoma (Sl. 1) Za parametre varne zveze IKE izberite sledeče algoritme:

   - enkripcijski algoritem DES,
   - zgoščevalni algoritem MD5.

   Parametri varne zveze IPSec naj bodo sledeči:

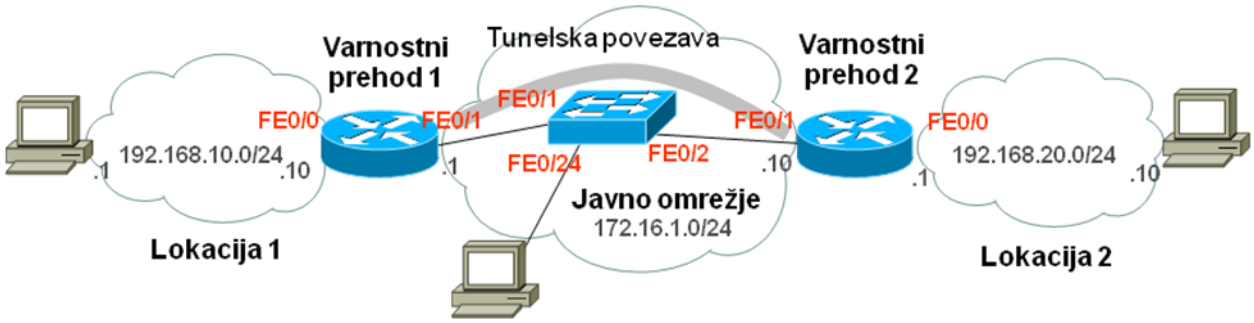
   - enkripcija s protokolom ESP (algoritem DES),
   - avtentikacija s protokolom ESP (algoritem MD5).

   Pravilnost delovanja preverite z ukazi za preverjanje nastavitev ˝show˝ (Tab. 3), ki so podprti v operacijskem sistemu IOS. S protokolnim analizatorjem Wireshark opazujte prenašane pakete in lastnosti vzpostavljenega tunela.

4. Spremenite parametre varne zveze IPSec:

   - enkripcija s protokolom ESP (način NULL),
   - avtentikacija s protokolom ESP (algoritem MD5).

   S protokolnim analizatorjem Wireshark ponovno opazujte prenašane pakete in lastnosti vzpostavljenega tunela.



***Sl. 1** Omrežje VPN*

3. Potek dela

3.1 Podatki o opremi

Usmerjevalnik

Oznaka izdelka:_____

Vgrajeni vmesniki:
Naštej vse vgrajene vmesnike in njim pripadajoče oznake

Naziv vmesnika	Oznaka vmesnika

Stikalo

Oznaka izdelka:_____

3.2 Fizične povezave

Identificiraj vrsto kabla uporabljenega za povezavo ter vmesnike na usmerjevalniku, ki so uporabljeni za povezavo:

Povezava	Vrsta kabla	Uporabljeni vmesnik(i)
Računalnik-Usmerjevalnik1		Usmerjevalnik1:
Računalnik-Usmerjevalnik2		Usmerjevalnik2:

Usmerjevalnik1-Stikalo		Usmerjevalnik1: Stikalo:
Usmerjevalnik2-Stikalo		Usmerjevalnik2: Stikalo:
Stikalo-Računalnik		Stikalo:

3.3 Nastavitev osnovnih parametrov IP

V tabelo vpišite seznam omrežij, ki so priključena na vaš usmerjevalnik.

	IP naslov omrežja
1.	
2.	
3.	

V skladu s podano topologijo omrežja izpolnite tabelo za nastavitev usmerjevalnika:

Naziv vmesnika	**IP naslov vmesnika**	**Maska podomrežja**

Glede na zgornje podatke nastavite osnovne parametre IP na usmerjevalniku (*primer nastavitev za varnostni prehod 1, glej Sl. 1).*

Primer konfiguracije vmesnika FastEthernet 0/0:

Router # **configure terminal**	vstop v globalni način konfiguracije
Router(config)# **interface FastEthernet 0/0**	izbira vmesnika FastEthernet 0/0
Router(config-if)# **ip address 192.168.10.10 255.255.255.0**	nastavitev naslova IP
Router(config-if)# **no shutdown**	vklop vmesnika
Router(config-if)# **exit**	vrnitev v prejšnji nivo dostopa
Router(config)#	

Primer konfiguracije vmesnika FastEthernet 0/1:

Router(config)# **interface FastEthernet 0/1**	izbira vmesnika FastEthernet 0/0
Router(config-if)# **ip address 172.16.1.1 255.255.255.0**	nastavitev naslova IP
Router(config-if)# **no shutdown**	vklop vmesnika
Router(config-if)# **exit**	vrnitev v prejšnji nivo dostopa
Router(config)#	

Ustrezno nastavite parametre IP računalnika in vpišite nastavljene podatke.

Naslov IP:	
Maska (pod)omrežja:	
Privzeti prehod:	

3.4 Nastavitev usmerjanja

Router# **configure terminal**	vstop v globalni način konfiguracije
Router(config)# **ip route 0.0.0.0 0.0.0.0 172.16.1.10**	nastavitev privzete statične poti

i. Kakšen način usmerjanja ste uporabili?

_____

ii. S katerim ukazom ste nastavili to usmerjanje?

_____

3.5 Nastavite stikalo za opazovanje prometa med usmerjevalnikoma. S pomočjo protokolnega analizatorja Wireshark opazujte promet.

Switch# **configure terminal**	vstop v globalni način konfiguracije
Switch(config)# **monitor session 1 source interface FastEthernet 0/1**	Nastavitev vmesnika na katerem se zajema promet
Switch(config)# **monitor session 1 source interface FastEthernet 0/2**	Nastavitev vmesnika na katerem se zajema promet
Switch(config)# **monitor session 1 destination interface FastEthernet 0/24**	Nastavitev vmesnika, ki bo sprejemal promet

i. Kateri vmesnik na stikalu ste uporabili za izvor in kateri za ponor v monitoring načinu?

_____

ii. Ali je promet med usmerjevalnikoma šifriran?

_____

iii. Kakšna je vsebina ukaza ping pri preverjanju dosegljivosti med računalnikoma? Kakšna je velikost paketa?

_____

3.6 Nastavite parametre protokola IPSec

Osnovni koraki pri nastavitvi protokola IPSec na usmerjevalniku so sledeči *(primer nastavitev za varnostni prehod 1, glej Sl. 1):*

1. *Nastavitev parametrov varne zveze IKE*

Router(config)#**crypto isakmp policy 1**	definiranje politike IKE
Router(config-isakmp)#**hash md5**	izbira zgoščevalnega algoritma
Router (config-isakmp)#**encryption des**	izbira enkripcijskega algoritma
Router(config-isakmp)#**authentication pre-share**	določitev avtentikacijskega postopka
Router(config-isakmp)#**lifetime 86400**	čas trajanja zveze v sekundah
Router(config-isakmp)#**group 2**	izbira skupine Diffie-Hellman
Router(config)#**crypto isakmp key 0** *KLJUC* **address** *172.16.1.10*	določitev ključa za avtentikacijo, ki ga povežemo s končno točko tunela (IP naslov varnostnega prehoda 2)

2. *Nastavitev parametrov tunelske povezave IPSec*

Router(config)#**crypto ipsec transform-set** *TUNEL* **esp-des esp-md5-hmac**	izbira protokolov in algoritmov tunelske povezave IPSec
Router(cfg-crypto-trans)#**mode tunnel**	določitev tunelskega načina varne zveze

3. *Nastavitev šifrirnega načrta*

Router(config)#**crypto map** *NACRT* 1 **ipsec-isakmp**	šifrirni načrt določimo z imenom, številko in načinom vzpostavljanja tunelske povezave
Router(config-crypto-map)#**set peer** *172.16.1.10*	določitev končne točke tunelske povezave
Router(config-crypto-map)#**set transform-set** TUNEL	izbira predhodno definiranega nabora protokolov in algoritmov
Router(config-crypto-map)#**match address 100**	izbira dostopovnega seznama oz. prometa, ki se naj kriptira

4. *Določitev dostopovnega seznama oz. prometa, ki naj se šifrira*

Router(config)#**access-list 100 permit ip** 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255	določitev prometa, ki naj se kriptira (naš primer: promet, ki gre iz omrežja 192.168.10.0 v omrežje 192.168.20.0)

5. *Določitev vmesnika, kjer se izvaja enkripcija prometa*

Router(config)#**interface** *FastEthernet 0/1*	izberemo vmesnik na katerem se bo izvajala enkripcija
Router(config-if)#**crypto map** *NACRT*	izvaja naj se šifrirni načrt, ki je določen s politiko ″NACRT″

i. Kateri enkripcijski in zgoščevalni algoritem ste uporabili pri nastavitvi parametrov varne zveze IKE?

_____

ii. Kako ste poimenovali ključ in kakšen je naslov IP končne točke tunela?

_____

iii. Kako ste poimenovali tunelsko povezavo?

_____

iv. S katerim ukazom ste določili tip enkripcije in avtentikacije tunelske povezave IPSec?

_____

v. Z ukazom ping preverite dosegljivost med računalnikoma? Ali je sosednji računalnik dosegljiv?

_____

3.7 V protokolnem analizatorju opazujte promet med usmerjevalnikoma.

i. Ali je promet med usmerjevalnikoma šifriran?

_____

ii. Ali lahko ugotovite kateri transportni protokol je bil uporabljen?

_____

iii. Kakšna je velikost paketa pri preizkušanju dosegljivosti (ping)?

_____

iv. Je velikost šifriranega paketa enaka kot pri nešifriranem paketu? Če ne, utemeljite zakaj!

_____

3.8 Preverjanje nastavitev usmerjevalnika

V spodnji tabeli se nahajajo osnovni ukazi za preverjanje nastavitev usmerjevalnika.

Router# show running-config	izpis aktivne konfiguracije usmerjevalnika
Router# show crypto isakmp policy	izpis nastavljenih parametrov varne zveze IKE
Router# show crypto isakmp key	izpis ključa, ki se uporablja za avtentikacijo
Router# show crypto isakmp sa detail	izpis trenutno aktivnih varnih zvez IKE
Router# show crypto ipsec transform-set	izpis nastavljenih parametrov varne zveze IPSec
Router# show crypto engine connections active	izpis aktivnih varnih zvez *IPSec*
Router# show crypto map	izpis nastavljenih parametrov šifrirnega načrta
Router# show ip route	izpis vnosov usmerjevalne tabele
Router# show interfaces FastEthernet 0/0	preverjanje delovanja FastEthernet vmesnika
Router# ping *˝IP naslov˝*	ukaz za preverjanje povezljivosti med usmerjevalniki
Router# traceroute *˝IP naslov˝*	ukaz, ki prikaže pot (število skokov) do oddaljene naprave
Router# exit	ukaz za vrnitev v prejšnji nivo dostopa

Tab. 3: Ukazi za preverjanje nastavitev na usmerjevalniku Cisco

S pomočjo zgornjih ukazov odgovorite na vprašanja.

i. Kakšna je dolžina ključa pri DES enkripciji? (show crypto isakmp policy)

_____

ii. Koliko paketov je usmerjevalnik šifriral in dešifriral? (show crypto engine connections active)

_____

iii. Kakšno je ime tunela in kakšen je končni naslov IP? (show crypto map)

_____

3.9 Spremenite parametre varne zveze IPSec in ponovno opazujte promet.

i. Kaj dosežete z ukazom NULL?

_____

ii. Ali je promet med usmerjevalnikoma šifriran?

_____