T: Konfiguracja sieci wirtualnych.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat wirtualnych sieci lokalnych (VLAN, Virtual Local Area Network). https://www.thomas-krenn.com/pl/wiki/Podstawowe_informacje_o_VLAN http://blog.devices.pl/?p=29 http://www.tp-link.com.pl/faq-328.html http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_58_se/configuration/guide/2960scg/swvlan.html

Wirtualna sieć lokalna to wydzielony logicznie fragment sieci fizycznej. Do tworzenia sieci VLAN wykorzystywane są przełączniki zarządzane. Standard 802.1Q umożliwia zdefiniowanie 4096 różnych sieci VLAN (identyfikatorów VID). Przełączniki przekazują ruch transmisji pojedynczej (unicast), rozsyłania grupowego (multicast) oraz rozgłaszania (broadcast) tylko w danej sieci VLAN. Wymiana danych pomiędzy różnymi sieciami VLAN możliwa jest za pomocą routera.

Przykład konfiguracji sieci VLAN w przełącznikach CISCO:

```
Switch>enable
Switch#conf t
Switch(config) #hostname sw
sw(config) #vlan 101
sw(config-vlan) #name users
sw(config-vlan) #exit
sw(config)#vlan 102
sw(config-vlan) #name teachers
sw(config-vlan) #exit
sw(config)#interface range fastEthernet 0/1 - 14
sw(config-if-range) #switchport mode access
sw(config-if-range)#switchport access vlan 101
sw(config-if-range) #exit
sw(config)#interface fastEthernet 0/23
sw(config-if) #switchport mode access
sw(config-if)#switchport access vlan 102
sw(config-if) #exit
sw(config)#int F 0/24
sw(config-if) #sw mode trunk
sw(config-if)#sw trunk allowed vlan add 101
sw(config-if) #sw trunk allowed vlan remove 102
sw(config-if) #sw trunk allowed vlan all
sw(config-if) #exit
sw(config) #exit
sw#show vlan
sw#show interfaces trunk
sw#exit
sw>
```

Zadanie2:

Wykorzystując program Cisco Packet Tracer połącz dwa komputery do dwóch przełączników. Następnie skonfiguruj łącze trunkowe pomiędzy tymi przełącznikami i sprawdź możliwość komunikacji pomiędzy komputerami należącymi do tej samej jak i do różnych sieci VLAN.

Do zarządzania sieciami wirtualnymi na przełącznikach wykorzystywany jest protokół VTP (VLAN Trunking Protocol). Protokół VTP rozpoznaje sieci VLAN z przedziału normalnego (identyfikatory od 1 do 1005).

Przełączniki mogą być skonfigurowane do pracy w następujących trybach:

- serwera VTP przechowuje w pamięci NVRAM informacje o sieciach VLAN i synchronizuje je z przełącznikami z całej domeny VTP,
- klienta VTP przechowuje informacje o sieciach VLAN pozyskane z serwera VTP,
- transparentnym przekazuje ogłoszenia VTP do klientów i serwerów VTP i nie jest członkiem domeny VTP.

Pomiędzy przełącznikami w domenie VTP stosujemy tryb połączeniowy trunk.



Przykłady konfiguracji sieci wirtualnych za pomocą poleceń konsoli tekstowej:

- <u>j</u> ••		
-	vlanserver# configure terminal	
	<pre>vlanserver(config)# interface fastethernet</pre>	0/1
,	vlanserver(config-if)# switchport mode tru:	nk
-	vlanserver(config)# vtp mode server	
-	<pre>vlanserver(config) # vtp domain elektronik</pre>	#nadanie nazwy domenie VTP
,	vlanserver# show vtp status	#sprawdzenie nazwy domeny
	vlanserver(config)#vlan 10	
-	vlanserver(config-vlan)#name vlan10	
-	vlanserver(config)#vlan 20	
,	vlanserver(config-vlan)#name vlan20	
,	vlanclient(config)#vtn mode client	#ustawienie trybu klienta VTP
,	vlanclient#show vtp status	
	vlanclient#show vlan	
	vrancrienc#Snow vran	

Zadanie3:

Odszukaj w serwisie internetowym Wikipedii informacje na temat Wirtualnych Sieci Prywatnych (VPN, Virtual Private Network).

Wirtualne sieci prywatne (VPN, Virtual Private Network) pozwalają na zabezpieczenie informacji przesyłanych za pomocą Internetu. Przesyłane dane są zabezpieczane i szyfrowane oraz dodatkowo mogą być kompresowane. Połączenie pomiędzy klientami VPN poprzez sieć Internet nazywane jest tunelem VPN.

System Windows obsługuje następujące rodzaje połączeń VPN:

- PPTP (Point-to-Point Tunneling Protocol), uwierzytelnianie odbywa się przed zaszyfrowaniem połączenia,
- L2TP (L2TP/IPSEC) (Layer 2 Tunneling Protocol/IP Security), transmisja jest szyfrowana przed uwierzytelnianiem, IPSEC zapewnia dodatkowe zabezpieczenia,
- SSTP (Secure Socket Tunneling Protocol), korzysta z zaszyfrowanych połączeń HTTP do ustanowienia połączeń VPN (Windows Server 2008).

Do uwierzytelniania użytkowników w systemach Windows Server 2003 używana jest usługa IAS (Internet Authentication Service). Usługa IAS pozwala na uwierzytelnianie użytkowników w oparciu o serwer RADIUS stosując nazwy i hasła z usługi Active Directory. Usługę instalujemy poprzez Dodawanie/Usuwanie składników systemu Windows, w Usługach sieciowych, wybierając Usługę uwierzytelniania internetowego.

Tomasz Greszata	- Koszal	in 2020 - http://gresza	ata.pl
Kreator składników systemu Windows		Usługi sieciowe	×
Składniki systemu Windows Możesz dodać lub usunąć składniki systemu Windows.		Aby dodać lub usunąć składnik, kliknij pole wyboru. Pole zacieniowane oznacza, że zainstalowana zostanie tylko część składnika. Aby obejrzeć zawartość składnika, kliknij przycisk Szczegóły. <u>P</u> odskładniki: Usługi sieciowe	
Aby dodać lub usunąć składnik, kliknij to pole wyboru. Pole zacieniow tylko część składnika będzie zainstalowana. Aby zobaczyć, co zawier kliknij przycisk Szczegóły. <u>S</u> kładniki:	ane oznacza, że a dany składnik,	✓ Protokół dynamicznej konfiguracji hosta (DHCP) 0,0 MB ✓ BRPC przez serwer proxy HTTP 0,0 MB ✓ System DNS (Domain Name System) 1,7 MB □ Usługa kwarantanny dostępu zdalnego 0,1 MB	-
– I Isługi certyfikatów I Isługi instalacji zdalnej I Isługi sieciowe IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	1,4 MB _ 2,0 MB 2,8 MB 4,9 MB _ 15 3 MB _	Image: State Stat	- -
Opis: Zawiera rozmaite specjalistyczne usługi i protokoły związane z Wymagane miejsce na dysku razem: 0,0 MB Miejsce dostępne na dysku: 1767,7 MB	siecią. Sz <u>c</u> zegóły	Wymagane miejsce na dysku razem: 0,0 MB <u>Szczegór</u> Miejsce dostępne na dysku: 1767,7 MB OK Anuluj	y
< <u>W</u> stecz <u>D</u> alej >A	Anuluj F	omoc	

Tworzenie VPN za pomocą usługi Routing i dostęp zdalny (RRAS, Routing and Remote Access) Kolejne kroki instalacji: Narzędzia administracyjne/Kreator konfigurowania serwera/Dalej/Dalej/Serwer dostępu zdalnego/sieci VPN/wybrać kombinację usług VPN i NAT/Zakończ.

Zezwolenie na połączenie VPN dla użytkownika konfigurujemy na zakładce Telefonowanie we właściwościach danego konta.

Etapy tworzenia połączenia VPN:

- nadanie uprawnień dla konta użytkownika do logowania VPN,
- instalowanie usługi dostępu zdalnego,
- konfiguracja usługi dostępu zdalnego,
- konfiguracja połączenia sieciowego klienta VPN.

Zadanie4:

Zapoznaj się z informacjami publikowanymi na następujących witrynach internetowych: <u>http://technet.microsoft.com/pl-</u> pl/library/cc731954%28v=ws.10%29.aspx <u>http://technet.microsoft.com/pl-</u> pl/library/cc736357%28v=ws.10%29.aspx https://technet.microsoft.com/pl-pl/library/cc781006%28v=ws.10%29.aspx

Właściwości: student141d Zdalne sterowanie Profil usług terminalowych COM+ Exchange General | E-mail Addresses | Exchange Features | Exchange Geatures | Exchange Geatures | Exchange Advanced Ogólne | Adres | Konto | Profil | Telefony | Organizacja | Opublikowane certyfikaty Cztonek grupy | Telefonowanie | Objekt | Zabezpieczenia | Srodowisko | Sesje Uprawnienie usługi Dostęp zdalny (telefonowanie lub sieci VPN) Zezwalaj na dostępi Odmów dostępu 🔿 Kontroluj dostęp poprzez zasady dostępu zdalneg Weryfikuj identyfikator rozmówcy: Opcie wywołania zwrotnego Bez www.okania zwrotnego Ustawiane przez komputer wywołujący (tylko usługa Routing i dostęp zdalny) 🔿 Zawsze używaj wywołania zwrotnego na numer: Przypisz statyczny adres IP Zastosui trasv statvozne Zdefiniuj trasy, które mają być użyte w tym połączeniu telefonicznym. OK Anuluj Zastosuj

Kanał VPN zestawiany między dwoma, odległymi fizycznie, sieciami LAN. Urządzeniem VPN może być serwer firmowy lub odpowiednio skonfigurowany router z obsługą sieci VPN.



Kanał VPN zestawiany między komputerem PC zdalnego użytkownika, a odległą siecią LAN.



Konfiguracja połączenia VPN w systemie Windows XP



Kreator nowego połączenia	Kreator nowego połączenia
Typ połączenia sieciowego Co chcesz zrobić?	Połączenie sieciowe Jak chcesz połączyć się z siecią w swoim miejscu pracy?
 Połącz z Internetem Połącz się z Internetem, aby móc przeglądać sieć Web i czytać wiadomości e-mail. Połącz z sięcią w miejscu pracy Połącz się z siecią firmową (za pomocą połączenia telefonicznego lub sieci VPN), aby móc pracować z domu, biura w terenie lub innej lokalizacji. Konfiguruj sieć w domu lub w małej firmie Połącz się z istniejącą siecią w domu lub w małej firmie Połącz się z istniejącą siecią w domu lub w małej firmie Połącz się z istniejącą siecią w domu lub w małej firmie kokonfiguruj nową. Konfiguruj połączenie zaawansowane Połącz się bezpośrednio z innym komputerem używając portu szeregowego, równoległego lub portu podczerwieni, lub skonfiguruj ten komputer tak, aby inne komputery mogły się z nim połączyć. 	Utwórz następujące połączenie: C Połączenie telefoniczne Łączy używając modemu i zwykłej linii telefonicznej lub linii telefonicznej sieci cyfrowej zintegrowanych usług ISDN. C Połączenie wirtualnej <u>sieci prywatnej</u> Łączy z siecią używając połączenia wirtualnej sieci prywatnej (VPN) przez Internet.
<u>≺ W</u> stecz <u>D</u> alej > Anuluj	<u>< ₩</u> stecz <u>D</u> alej > Anuluj

Tomasz Greszata	- Koszalin 2020 -	http://greszata.pl
<mark>Kreator nowego połączenia</mark> Nazwa połączenia Podaj nazwę tego połączenia do swojego miejsca pracy.	Kreator nowego połączenia Wybór serwera sieci VPN Jaka jest nazwa lub adres serwera	a sieci VPN?
W poniższym polu wpisz nazwę tego połączenia. <u>N</u> azwa firmy zs9elektronik.pl Na przykład możesz wpisać nazwę swojego miejsca pracy lub nazwę serwera, z któr się łączysz.	Podaj nazwę hosta lub adres proto łączysz. <u>N</u> azwa hosta lub adres IP (np. mic zs9elektronik.pl	okołu internetowego (IP) komputera, z którym się rosoft.com lub 157.54.0.1):
< <u>W</u> stecz <u>Dalej</u> >	Anuluj Kreator nowego połączenia	<u> ≺ W</u> stecz <u>D</u> alej > Anuluj
Dostępność połączeń Możesz utworzyć nowe połączenie dostępne dla każdego użytkownika lub tylko dla siebie. Połączenie utworzone tylko do Twojego użytku jest zapisywane w Twoim koncie użytkownika i jest dostępne tylko po Twoim zalogowaniu. Utwórz to połączenie: O Do użytku dla wszystkich I tylko do mojego użytku	Koń połą Pomyś następ zss	Iczenie pracy Kreatora nowego Iczenia ilnie ukończono czynności potrzebne do utworzenia ującego połączenia: Belektronik.pl
<u> ≺ W</u> stecz <u>D</u> alej >	Anuluj	zenie zostanie zapisane w folderze Połączenia we. odaj skrót do tego połączenia na moim pulpicie worzyć połączenie i zamknąć kreatora, kliknij przycisk icz. < <u>W</u> stecz Zakończ Anuluj

Łączenie z zs9elektronik.pl	🗢 zs9elektronik.pl Właściwości	<u>? ×</u>
Nazwa greszata Hasło: •••••••	Ogólne Opcje Zabezpieczenia Sieć Nazwa hosta lub adres IP miejsca docelowego (np. microsoft.com lub 157.54.0.1): zs9elektronik.pl Łączenie najpierw System Windows może najpierw połączyć z siecią publiczną, taką jak Internet, przed próbą ustanowienia połączenia wirtualnego.	
 Zapisz tę nazwę użytkownika i hasło dla następujących użytkowników: Ijylko ja Dowolny użytkownik tego komputera 	☑ Pokaż ikonę w obszarze powiadomień podczas połączenia	
Połącz Anuluj Właściwości Pomo <u>c</u>	ОК	Anuluj

Tomasz Greszata - Kosz	alin 2020 - http://greszata.p
▼ zs9elektronik.pl Właściwości ? × Ogólne Opcje Zabezpieczenia Sieć Opcje wybierania numeru ✓ Wyświeti wskaźnik postępu w trakcie łączenia ✓ ✓ Monituj o nazwę użytkownika, hasło, certyfikat itp. ✓ Dołącz domenę logowania systemu Windows Opcje ponownego wybierania numeru 3 ★ Próby ponownego wybierania numeru: 3 ★ Czas pomiędzy kolejnymi próbami ponownego 1 minuta ▼ Wybierz numer ponownie po przerwaniu połączenia Nigdy ▼	 zs9elektronik.pl Właściwości Ogólne Opcje Zabezpieczenia Sieć Opcje zabezpieczeń Typowe (ustawienia zalecane) Weryfikuj moją tożsamość jako: Wymagaj bezpiecznego hasła Automatycznie użyi mojej nazwy logowania i hasła (oraz domeny, jeżeli istnieje) systemu Windows Wymagaj szyfrowania danych (przerywaj połączenia nie obsługujące szyfrowania) Zaawansowane (ustawienia niestandardowe) Zmiana tych ustawień wymaga znajomości protokołów zabezpieczeń. Ustawienia protokołu I<u>P</u>Sec
OK Anuluj Zaawansowane ustawienia zabezpieczeń ? × Szyfrowanie danych: ? Wymagaj szyfrowania (rozłącz, jeśli serwer odmawia) ▼ Zabezpieczenia logowania ▼ OLLizu protokoku uwierzutelpiania rozszerzopego (EAP)	OK Anuluj
 Cely protokoł d driety centralnici receberciologie (j. tr.) Zezwalaj na użycie tych protokołów Hasło nieszyfrowane (PAP) Protokół uwierzytelniania hasła <u>S</u>hiva (SPAP) Protokół uwierzytelniania typu Challenge Handshake (CHAP) Microsoft CHAP (MS-CHAP) Zezwalaj na używanie starszych wersji protokołu MS-CHAP dla serwerów Windows 95 Mjcrosoft CHAP wersja 2 (MS-CHAP v2) Dla protokołów opartych na MS-CHAP, automatycznie użyj 	Ustawienia protokołu IPSec ? 🗴
mojej nazwy logowania i hasła (oraz domeny, jeżeli istnieje) systemu Windows OK Anuluj	Klucz: klucz.elektronik.pl

Image: Second Stress	Image: Single Constraints of the server of DNS automatycznie Image: Constraints of Constraints	://greszata.p	Fomasz Greszata	a - Koszalin 2020 -		http://greszata.p
Zainstaluj Udinstaluj Własciwości Zaawansowane Opis Protokół kontroli transmisji/Protokół internetowy (TCP/IP). Domyślny protokół dla sieci rozłegłych, umoźliwiający	Image: Specific Spectral Spectra Spectral Spectral Spectral Spectra Spectral Spectral Spectral Spe	//greszata.p	Image: Second state in the second state is in the second state in the second state is in the second state in the second state is in the second state in the second state is in the second state in the second state is i	A - Koszalin 2020 - pl Właściwości ? × Zabezpieczenia Sieć Zabezpieczenia Sieć eci prywatnej (VPN): ? × tokołem L2TP IPSec ✓ Ustawienia © Użyskaj adres IP aut © Użyskaj adres IP aut © Użyskaj adres IP aut © Użyskaj adres IP: © Użyskaj adres serwe © Użyskaj adres serwe © Użyskaj adres serwe © Użyskaj adres verwer DN Adres IP: Ny Anti-Virus NDIS Filter © ox Bridged Networking Driver ✓ eci Microsoft Networks ✓ Internatywny serwer DN Alternatywny serwer DN Alternatywny serwer DN Alternatywny serwer DN Alternatywny serwer DN Alternatywny serwer DN Internatywny serwer DN Alternatywny serwer DN	rnetowy (TCP/IP) acji sieci możesz automatycznie uz okołu IP. W przeciwnym wypadku i ołu IP od administratora sieci. omatycznie adresu IP: 192 . 168 . 19 . 1 adresów serwerów DNS: S: 192 . 168 . 19 . S:	http://greszata.p

Zadanie5:

Utwórz projekt sieci VPN w programie Cisco Packet Tracer według następujących wytycznych:

- w sieci występują dwa odrębne punkty dostępowe VPN odpowiednio w sali 27 oraz w sali 32,
- w każdej z sal komputery podłączone są przewodowo do jednego przełącznika,
- wszystkie komputery pracujące w danej pracowni posiadają statyczne adresy IP,
- adresy sieci komputerowych w salach są różne,
- w każdej pracowni znajdują się dwa komputery stacjonarne z kartami sieciowymi Ethernet,
- wszystkie komputery w sieci mają być wzajemnie widoczne.

Pracę zachowaj w pliku pod nazwą **\$nazwisko_vpn.pkt** i prześlij plik pocztą elektroniczną do nauczyciela w postaci załącznika na adres <u>greszata@zs9elektronik.pl</u>. Do wykonania zadania posłuż się instrukcją dostępną na końcu dokumentu.



Zadanie6:

Utwórz projekt sieci VPN w programie Cisco Packet Tracer według następujących wytycznych:

- w sieci występuje pięć odrębnych punktów dostępowych VPN,
- w dwóch salach komputerowych nr 27 i 32 znajdują się routery udostępniające połączenie z sieciami rozległymi,
- w każdej z sal komputery podłączone są przewodowo do jednego przełącznika,
- wszystkie komputery pracujące w danej pracowni posiadają statyczne adresy IP,
- adresy sieci komputerowych w salach są różne,
- w każdej pracowni znajdują się dwa komputery stacjonarne z kartami sieciowymi Ethernet,
- wszystkie komputery w sieci mają być wzajemnie widoczne.

Pracę zachowaj w pliku pod nazwą **\$nazwisko_vpn_lab.pkt** i prześlij plik pocztą elektroniczną do nauczyciela w postaci załącznika na adres <u>greszata@zs9elektronik.pl</u>. Do wykonania zadania posłuż się instrukcją dostępną w pliku **lab_vpn.pdf**.



Materiały pomocnicze:

http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/16448-default.html http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/ike.html

Rozwiązanie zadania

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze **s27router**:

```
s27router>enable
s27router#?
s27router#configure terminal
s27router(config)#interface GigabitEthernet0/0
s27router(config-if)#ip address 192.168.19.1 255.255.255.0
s27router(config-if)#no shutdown
s27router(config-if)#exit
s27router(config)# interface GigabitEthernet1/1
s27router(config-if)#ip address 10.0.27.254 255.255.255.0
s27router(config-if)#ip address 10.0.27.254 255.255.255.0
s27router(config-if)#no shutdown
s27router(config-if)#no shutdown
s27router(config-if)#no shutdown
s27router(config-if)#exit
s27router(config-if)#ip route 0.0.0.0 0.0.0.0 10.0.27.1
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze s32router:

```
s32router>en
s32router#conf t
s32router(config)#int g0/1
s32router(config-if)#ip address 192.168.18.1 255.255.255.0
s32router(config-if)#no shutdown
s32router(config-if)#exit
s32router(config-if)#ip address 10.0.32.254 255.255.255.0
s32router(config-if)#ip address 10.0.32.254 255.255.255.0
s32router(config-if)#no shutdown
s32router(config-if)#no shutdown
s32router(config-if)#exit
s32router(config-if)#exit
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze introuter1: introuter1>en

introuter1#config terminal
introuter1(config)#int g0/1

- Koszalin 2020 -

```
introuter1(config-if)#ip address 10.0.27.1 255.255.255.0
introuter1(config-if)#no shutdown
introuter1(config-if)#exit
introuter1(config)#int g1/1
introuter1(config-if)#ip address 27.27.27.27 255.255.255.0
introuter1(config-if)#no shutdown
introuter1(config-if)#exit
introuter1(config)#ip route 0.0.0.0 0.0.0.0 27.27.27.1
introuter1(config)#ip route 192.168.19.0 255.255.255.0 10.0.27.254
introuter1(config)#no ip route 192.168.19.0 255.255.255.0 10.0.27.254
introuter1(config)#no ip route 192.168.19.0 255.255.255.0 10.0.27.254
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze introuter2:

```
introuter2>en
introuter2#configure terminal
introuter2(config)#int g0/1
introuter2(config-if)#ip address 10.0.32.1 255.255.255.0
introuter2(config-if)#no shutdown
introuter2(config-if)#exit
introuter2(config-if)#ip address 32.32.32.32 255.255.255.0
introuter2(config-if)#ip address 32.32.32.32 255.255.255.0
introuter2(config-if)#no shutdown
introuter2(config-if)#exit
introuter2(config-if)#exit
introuter2(config)#ip route 0.0.0.0 0.0.0.0 32.32.32.1
introuter1(config)#ip route 192.168.18.0 255.255.255.0 10.0.32.254
introuter1(config)#no ip route 192.168.18.0 255.255.255.0 10.0.32.254
introuter2(config)#exit
```

Polecenia wydawane w zakładce Command Line Interface (CLI) na routerze internet:

```
Router#configure terminal
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 27.27.27.1 255.255.255.0
Router(config-if) #no shutdown
Router (config-if) #exit
Router(config) #interface GigabitEthernet1/0
Router(config-if) #ip address 32.32.32.1 255.255.255.0
Router(config-if) #no shutdown
Router (config-if) #exit
Router (config) #hostname internet
internet(config)#ip route 27.27.27.0 255.255.255.0 27.27.27.27
internet(config)#ip route 32.32.32.0 255.255.255.0 32.32.32.32
internet(config) #ip route 10.0.27.0 255.255.255.0 27.27.27.27
internet(config) #ip route 10.0.32.0 255.255.255.0 32.32.32.32
#internet(config)#ip route 192.168.19.0 255.255.255.0 27.27.27.27
#internet(config)#no ip route 192.168.19.0 255.255.255.0 27.27.27.27
#internet(config)#ip route 192.168.18.0 255.255.255.0 32.32.32.32
#internet(config)#no ip route 192.168.18.0 255.255.255.0 32.32.32.32
internet(config)#exit
internet#
```

Ustawienia polityki ISAKMP/IKE (niezbędne do nawiązania połączenia tunelowego) wydawane w zakładce Command Line Interface (CLI) na routerze **introuter1**:

```
introuter1>enable
introuter1#configure terminal
introuter1(config)#crypto isakmp policy 5
introuter1(config-isakmp)#encryption 3des
```

- Koszalin 2020 -

introuter1(config-isakmp)#group 2 introuter1(config-isakmp)#hash sha introuter1(config-isakmp)#lifetime 28800 introuter1(config-isakmp)#autentication pre-share introuter1(config-isakmp)#exit introuter1(config)#crypto isakmp key hr5xb8416aa9r6 address 32.32.32.32 introuter1(config)#access-list 101 permit ip 10.0.27.0 0.255.255.255 10.0.32.0 0.255.255.255 introuter1(config)#ip route 0.0.0.0 0.0.0.0 27.27.27.1 introuter1(config)#ip route 10.0.32.0 255.255.255.0 27.27.27.1 introuter1(config)#crypto ipsec transform-set STRONG esp-3des espsha-hmac introuter1(config)#crypto map CISCO 10 ipsec-isakmp introuter1(config-crypto-map)#set security-association life seconds 3600 introuter1(config-crypto-map) #set transform-set STRONG introuter1(config-crypto-map)#set pfs group2 introuter1(config-crypto-map)#set peer 32.32.32.32 introuter1(config-crypto-map)#match eddress 101 introuter1(config-crypto-map)#exit introuter1(config)#int g1/1 introuter1(config-if)#crypto map CISCO introuter1(config-if)#exit

Ustawienia polityki ISAKMP/IKE (niezbędne do nawiązania połączenia tunelowego) wydawane w zakładce Command Line Interface (CLI) na routerze **introuter2**:

```
introuter2>en
introuter2#configure terminal
introuter2(config)#crypto isakmp policy 5
introuter2(config-isakmp)#encryption 3des
introuter2(config-isakmp)#group 2
introuter2(config-isakmp)#hash sha
introuter2(config-isakmp)#lifetime 28800
introuter2(config-isakmp) #autentication pre-share
introuter2(config-isakmp)#exit
introuter2(config)#crypto isakmp
                                             hr5xb8416aa9r6
                                      key
                                                               address
27.27.27.27
introuter2(config)#access-list 101 permit ip 10.0.32.0 0.255.255.255
10.0.27.0 0.255.255.255
introuter2(config) #ip route 0.0.0.0 0.0.0.0 32.32.32.1
introuter2(config)#ip route 10.0.27.0 255.255.255.0 32.32.32.1
introuter2(config)#crypto ipsec transform-set STRONG esp-3des esp-
sha-hmac
introuter2(config)#crypto map CISCO 10 ipsec-isakmp
introuter2(config-crypto-map)#set security-association
                                                         life seconds
3600
introuter2(config-crypto-map) #set transform-set STRONG
introuter2(config-crypto-map)#set pfs group2
introuter2(config-crypto-map)#set peer 27.27.27.27
introuter2(config-crypto-map)#match address 101
introuter2(config-crypto-map)#exit
introuter2(config)#int g1/1
introuter2(config-if)#crypto map CISCO
introuter2(config-if)#exit
```

Konfiguracja VPN w systemie Linux OpenSUSE

Tomasz Greszata

- Koszalin 2020 -

Instalacja OpenVPN zipper install openvpn Sprawdzenie, czy posiadamy sterownik wirtualnego interfejsu TUN/TAP #nic nie powinno zostać wyświetlone modprobe tun dmesq | grep tun Generowanie klucza wykorzystywanego do szyfrowania i uwierzytelniania transmisji openvpn -genkey -secret /etc/openvpn/static.key Zezwolenie na przekazywanie pakietów, dokonujemy zmiany wpisu w pliku /etc/sysctl.conf net.ipv4.ip forward=1 Utworzenie grupy oraz uzytkownika na potrzeby połączenia tunelowego groupadd openvpn useradd -q openvpn -d /usr/local/etc/openvpn -s /bin/false -f 1 openvpn Tworzenie pliku konfiguracyjnego dla połączenia tunelowego /etc/openvpn/openvpn.conf o nastepujacej treści: dev tun #określnenie interfejsu local 192.168.19.21 #adres IP serwera proto udp #protokół transmisji danych port 17997 #port transmisji danych, należy odblokować w zaporze sieciowej user openvpn group openvpn secret static.kev #klucz prywatny serwera ifconfig 10.0.0.0 255.255.255.0 #adres sieci, z której przydzielane zostaną adresy IP klientom comp-lzo #algorytm kompresji Uruchomienie serwera VPN /etc/init.d/openvpn start Sprawdzenie interfejsu połączenia tunelowego ifconfig | grep tun

Zadanie7:

Zainstaluj i skonfiguruj usługę VPN w systemie Linux OpenSUSE.

Zadanie8:

Zapoznaj się z informacjami na temat oprogramowanie VPNonline, Cyber GhostVPN, BartVPN lub OpenVPN.

Konfiguracja połączenia VPN w programie Cisco Packet Tracer: Create a VPN in Packet Tracer

This is a brief "Sample configuration", to create a VPN in the Packet tracer v5.3



Step 1: Add two routers 2811

```
Step 2: Here are the configuration files.
      hostname Left
      crypto isakmp policy 5
      encr 3des
      authentication pre-share
      group 2
      lifetime 72000
      crypto isakmp key cisco address 10.0.0.2
      crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
      crypto map CISCO 10 ipsec-isakmp
      set peer 10.0.0.2
      set pfs group2
      set transform-set STRONG
      match address 101
      interface FastEthernet0/0
      ip address 10.0.0.1 255.255.255.0
      duplex auto
      speed auto
      crypto map CISCO
      interface FastEthernet0/1
      ip address 192.168.0.1 255.255.255.0
      duplex auto
      speed auto
      interface Vlan1
      no ip address
      shutdown
      ip classless
      ip route 0.0.0.0 0.0.0.0 10.0.0.0
      ip route 192.168.2.0 255.255.255.0 10.0.0.0
      access-list 101 permit ip 192.168.0.0 0.0.0.255 192.168.2.0 0.0.0.255
      line con 0
      line vtv 0 4
      login
      end
And the Second Configuration:
      hostname Right
      crypto isakmp policy 5
      encr 3des
      authentication pre-share
      group 2
      lifetime 72000
      crypto isakmp key cisco address 10.0.0.1
      crypto ipsec transform-set STRONG esp-3des esp-sha-hmac
      crypto map Cisco 10 ipsec-isakmp
      set peer 10.0.0.1
      set pfs group2
      set transform-set STRONG
      match address 101
      interface FastEthernet0/0
      ip address 10.0.0.2 255.255.255.0
      duplex auto
      speed auto
```

- Koszalin 2020 -

```
crypto map Cisco
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
interface Vlan1
no ip address
shutdown
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.0
ip route 192.168.0.0 255.255.255.0 10.0.0.0
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.0.0 0.0.0.255
line con 0
line vty 0 4
login
end
```

This works perfectly, and it is a good start for someone who wants to create a VPN on Packet tracer. It is also possible to Implement GRE tunnels since the Version 3.2 (if I remember well).

Instrukcje do zadania 5:



CONFIGURATION ON ROUTER R1:

```
Router>enable
Router#config t
Router(config)#host r1
r1(config)#int fa0/0
r1(config-if)#ip add 192.168.1.1 255.255.255.0
r1(config-if)#no shut
r1(config-if)#exit
r1(config)#int fa0/1
r1(config-if)#ip address 1.0.0.1 255.0.0.0
r1(config-if)#no shut
```

CONFIGURATION ON ROUTER R2:

Router>enable Router#config t Router(config)#host r2
r2(config)#int fa0/0
r2(config-if)#ip add 1.0.0.2 255.0.0.0
r2(config-if)#no shut
r2(config-if)#exit
r2(config)#int fa0/1
r2(config-if)#ip add 2.0.0.1 255.0.0.0
r2(config-if)#no shut

CONFIGURATION ON ROUTER R3:

Router>enable Router#config t Router(config)#host r3 r3(config)#int fa0/0 r3(config-if)#ip add 2.0.0.2 255.0.0.0 r3(config-if)#no shut r3(config-if)#exit r3(config)#int fa0/1 r3(config-if)#ip add 192.168.2.1 255.255.255.0 r3(config-if)#no shut

DEFAULT ROUTING CONFIGURATION ON ROUTER R1:

r1>enable
r1#config t
Enter configuration commands, one per line. End with CNTL/Z.
r1(config)#ip route 0.0.0.0 0.0.0.0 1.0.0.2
r1(config)#

DEFAULT ROUTING CONFIGURATION ON ROUTER r3:

r3>enable r3#config t Enter configuration commands, one per line. End with CNTL/Z. r3(config)#ip route 0.0.0.0 0.0.0.0 2.0.0.1 r3(config)#

FIRST CREATE A VPN TUNNEL ON ROUTER R1:

rl#config t
rl(config)#interface tunnel 10
rl(config-if)#ip address 172.16.1.1 255.255.0.0
rl(config-if)#tunnel source fa0/1
rl(config-if)#tunnel destination 2.0.0.2
rl(config-if)#no shut

NOW CREATE A VPN TUNNEL ON ROUTER R3:

r3#config t r3(config)#interface tunnel 100 r3(config-if)#ip address 172.16.1.2 255.255.0.0 r3(config-if)#tunnel source fa0/0 r3(config-if)#tunnel destination 1.0.0.1 r3(config-if)#no shut

Now Do routing for created VPN Tunnel on Both Router R and R3:

r1(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.2 r3(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.1

Now i am going to router R1 and R3 and test whether tunnel is created or not.

r1#show interfaces Tunnel 10
r3#show interfaces Tunnel 100

PC0>tracert 192.168.2.2 PC1>tracert 192.168.1.2