**Projekt**

**Przedmiot:** Projektowanie profesjonalnej instalacji sieci P1 **Temat:** Przykład wykorzystania sieci VPN s2s do realizacji połączenia pomiędzy centralą i oddziałami  
**Autor:** Mateusz Chudzik, Jakub Garncarz

1. **Wprowadzanie**

VPN to usługa, która jest coraz częściej stosowana nie tylko przez osoby z branży IT oraz pracowników wielkich korporacji, ale również przez zwykłych użytkowników Internetu. Osoby, które szukają informacji na temat bezpieczeństwa w sieci oraz sposobów na ochronę prywatności, prędzej lub później trafiają na pojawiające się w różnych miejscach pojęcie - VPN.VPN dosłownie oznacza Wirtualną Sieć Prywatną (ang. Virtual Private Network), wirtualność w tym pojęciu odnosi się do tego, że jest to sieć, która fizycznie nie istnieje. Funkcjonuje jedynie jako umowne powiązanie dwóch obiektów, które komunikują się ze sobą za pośrednictwem sieci publicznej. Prywatna - dlatego, że dostęp do niej mają tylko określone osoby, które zostały uwierzytelnione, a podmioty z zewnątrz nie są w stanie uzyskać do niej dostępu. Treść i zawartość danych, których wymiana odbywa się za pośrednictwem VPN, jest chroniona przed dostępem osób trzecich. Chcąc odpowiedzieć na pytanie co to takiego VPN, można podać najprostszą definicję VPN - jest to szyfrowany tunel, który łączy ze sobą dwa punkty w sieci. Dzięki tym właściwościom VPN, otrzymujemy możliwość przesyłania danych w taki sposób, jakby urządzenia połączone za pośrednictwem VPN-a były również połączone ze sobą fizycznie, przy pomocy zwykłej sieci.

1. **Wstęp teoretyczny**

IPsec (ang. Internet Protocol Security, IP Security) – zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia Wirtualnej Sieci Prywatnej (ang. VPN). VPN oparta na IPsec składa się z dwóch kanałów komunikacyjnych pomiędzy połączonymi komputerami: kanał wymiany kluczy, za pośrednictwem którego przekazywane są dane związane z uwierzytelnianiem i szyfrowaniem (klucze), oraz kanału (jednego lub więcej), który niesie pakiety transmitowane poprzez sieć prywatną. Kanał wymiany kluczy jest standardowym protokołem UDP . Kanały przesyłu danych oparte są na protokole ESP.

Protokoły wchodzące w skład architektury IPsec służą do bezpiecznego przesyłania przez sieć pakietów IP. Działają one na zasadzie kapsułkowania, tj. oryginalny (zabezpieczany) pakiet IP jest szyfrowany, otrzymuje nowy nagłówek protokołu IPsec i w takiej formie jest przesyłany przez sieć. Bezpieczeństwo zapewniane przez IPsec może być dwojakie, w zależności od stosowanego protokołu. I tak: pojawia się problem dystrybucji kluczy symetrycznych. Narzuca się zastosowanie kryptografii asymetrycznej, ale jest ona o wiele wolniejsza od szybkich szyfrów symetrycznych i dodanie ich do protokołów niskiego poziomu, jakimi są ESP i AH (Authentication Header), miałoby znaczący wpływ na wydajność. Te dwa protokoły pozostały więc relatywnie prostymi protokołami niskiego poziomu, a do skomplikowanych zadań dystrybucji klucza i uwierzytelniania stron stworzono oddzielny protokół IKE.

Protokół IKE (Internet Key Exchange) został zaprojektowany w większości przez NSA (National Security Agency) i jest skomplikowany, głównie ze względu na poziom abstrakcji, na jakim operuje. Wystarczy bowiem włożyć do niego własny zestaw algorytmów kryptograficznych, czy wręcz własną arytmetykę (zestaw ten określa się jako DOI, Domain of Interpretation) by otrzymać zupełnie inny od cywilnego protokół, na przykład na potrzeby wojska.

Istotną cechą ESP i AH jest mała ilość informacji, jakie potencjalny atakujący otrzymuje w wyniku podsłuchiwania szyfrowanej komunikacji. Po włączeniu sniffera zobaczy on tylko zaszyfrowany pakiet opatrzony dwiema liczbami:

* SPI (Security Parameters Index)
* numer sekwencyjny

Kolejną istotną cechą kanałów IPsec jest ich jednokierunkowość – dany kanał obsługuje tylko ruch idący z hosta A do B. Każda pełna łączność wykorzystuje dwa kanały – jeden od A do B, drugi od B do A. Każdy z nich ma inne SPI, osobny licznik sekwencyjny, inne klucze kryptograficzne. Taki jednokierunkowy kanał IPsec (ESP lub AH) jest określany nazwą Security Association (która nie ma dobrego polskiego tłumaczenia, stąd w artykule używane jest określenie „kanał”). Każde SA charakteryzuje się przez adresy IP początku i końca oraz SPI.

Do pełnej łączności między dwoma hostami potrzebne są dwa kanały IPsec. Jeśli wykorzystany zostanie protokół ESP, to każdy kanał będzie wymagał dwóch kluczy kryptograficznych – jednego do szyfrowania danych, drugiego do ochrony integralności i uwierzytelnienia. Jeśli będzie to AH, to odpadnie pierwszy klucz (szyfrujący). W najbardziej złożonym przypadku ESP do pełnej komunikacji będą potrzebne cztery klucze:

* szyfrujący dla kanału relacji A do B
* uwierzytelniający dla kanału relacji A do B
* szyfrujący dla kanału relacji B do A
* uwierzytelniający dla kanału relacji B do A

Jest wiele rodzajów sieci VPN różniących się sposobem realizacji transmisji, stosowanymi mechanizmami zapewniającymi bezpieczeństwo i cechami funkcjonalnymi.

Wśród nich wyróżniamy:

1. oparte na protokole IPSec

a) sieci typu site-to-site łączące ze sobą w sposób bezpieczny dwie lub więcej sieci: „tunele” pomiędzy tymi sieciami najczęściej są zakończone na dedykowanych urządzeniach takich jak routery z funkcją VPN, firewalle lub koncentratory VPN: nie wymagają instalacji żadnego oprogramowania na komputerach;

b) sieci typu remote-access lub client-to-site łączące w sposób bezpieczny pojedyncze komputery z sieciami; wymagają instalacji na komputerach specjalnego oprogramowania typu VPN Client.

2. oparte na protokole SSL- najczęściej typu remote-access, nie wymagają instalacji specjalnego oprogramowania na komputerze, za to mają mniejsza funkcjonalność niż sieci VPN oparte na protokole IPSec.

3.oparte na innych protokołach /technologiach, np.L2TP

Zalety stosowania sieci IPSec VPN

* Zapewnienie poufności poprzez szyfrowanie danych silnymi algorytmami kryptograficznymi,
* Zapewnienie integralności poprzez uniemożliwienie modyfikacji danych w trakcie transmisji,
* Uwierzytelnianie stron poprzez zapewnienie, ze nikt nie podszył się pod żadna ze stron,
* Zapewnienie niezaprzeczalności, które oznacza, ze strony nie mogą zaprzeczyć, ze nie wysłały danej informacji, o ile informacja ta była podpisana kluczem prywatnym i podpis został poprawnie zweryfikowany .

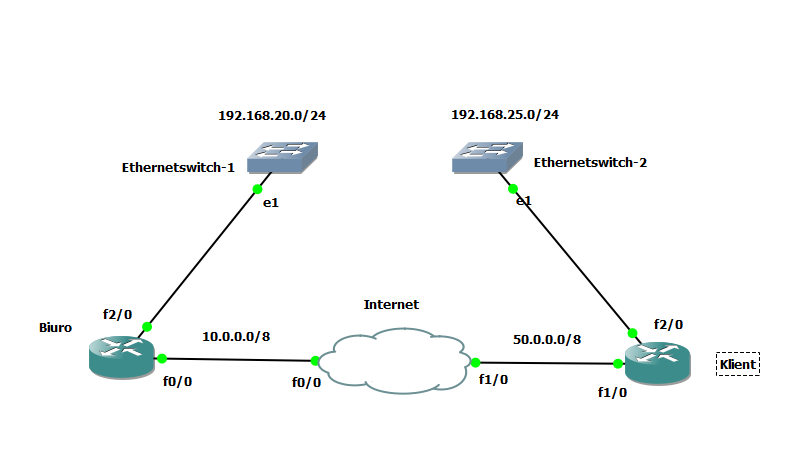
Routing w sieciach VPN-VTI:

W pierwszej kolejności należy wyjaśnić jaka jest różnica pomiędzy tradycyjnymi tunelami IPSEC a tunelami opartymi o VTI (Virtual Tunnel Interface). Tradycyjna konfiguracja tunelu IPSEC wymaga zdefiniowania zasobów które mają zostać połączone za pomocą kreowanego tunelu (local traffic to remote traffic). Taka definicja wpływa na trasowanie pakietów powodując, że proces trasowania na urządzeniu przebiega w oparciu o tablicę routingu oraz polisę IPSEC.Polisa wymusza aby wszystkie pakiety które spełniają kryteria polisy były enkapsulowane w IPSEC. Zastosowanie interfejsów VTI powoduje, że uzyskujemy możliwość wpływania na trasowanie pakietów w sposób dużo bardziej elastyczny niż ma to miejsce gdy korzystamy z polisy IPSEC (zmian routingu wymaga wprowadzenia zmiany w polisie IPSEC). Korzystając z VTI możemy do trasowania pakietów korzystać ze statycznych reguł routingu, PBR jak i użyć trasowania z wykorzystaniem dynamicznych protokołów routingu.

**3. Działanie programu**

Konfigurację VPN przedstawiliśmy za pomocą darmowego oprogramowania GNS3. Jest to graficzny emulator sieci, pozwalający kompleksowo tworzyć i testować sieci złożone z wirtualnego sprzętu Cisco i wirtualnych maszyn. Jest to kompletne narzędzie do prowadzenia inżynieryjnych laboratoriów sieciowych, administracyjnych lub dla osób chcących zdać certyfikaty sieciowa takie jak CCNA,CCNP.  
  
Do naszej konfiguracji w GNS3 wykorzystaliśmy obraz routeru C7200, a także wbudowane już ethernetswitch’e.

Topologia VPN:

  
  
**Konfiguracja Tunelu VPN**  
  
  
**Router Biuro konfiguracja:**  
  
Przejście z trybu EXEC użytkownika do trybu uprzywilejowanego   
enable

Przejście z trybu EXEC użytkownika do trybu uprzywilejowanego trybu EXEC

configure terminal

Ustawienie nazwy hosta

hostname Biuro

Konfiguracja interfejsu FastEthernet 0/0 (Do Internet )  
interface f0/0   
  
Nadanie adresu IP interfejsowi  
ip address 10.0.0.2 255.0.0.0

Włączenie interfejsu   
no shutdown

Opuszczenie trybu konfiguracji interfejsu  
exit

Konfiguracja interfejsu FastEthernet 2/0 ( Do Ethernetswitch-1 )  
interface f2/0

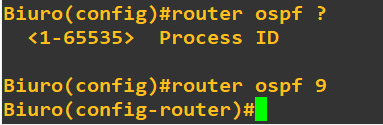
ip address 192.168.20.1 255.255.255.0

no shutdown

exit

Zapobieganie wyszukiwaniu nazwy domenowej po błędnie wpisanym poleceniu  
no ip domain lookup

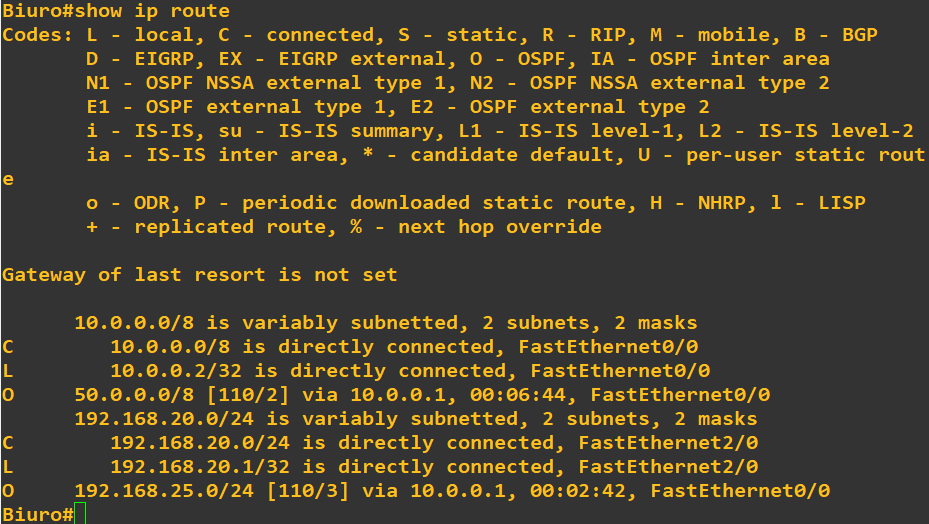
Włączenie protokołu OSPF (9 – numer procesu)  
router ospf 9



Określenie interfejsu na którym OSPF będzie rozgłaszany. MASKA\_WILDCARD – maska odwrotna tzn. dla maski 255.255.255.0 wildcard będzie 0.0.0.255. ID oznacza obszar OSPF – ważne aby obszary były takie same na sąsiednich ruterach.   
network 192.168.20.0 0.0.0.255 area 0

network 10.0.0.0 0.255.255.255 area 0  
  
Opuszczenie trybu konfiguracji i przejście do trybu uprzywilejowanego EXEC   
end

wr

Wyświetlenie tablicy rutingu  
show ip route   
  


**Router Internet konfiguracja:**enable

configure terminal

hostname Internet

Konfiguracja interfejsu FastEthernet 0/0 ( Do Biuro )  
interface f0/0

ip address 10.0.0.1 255.0.0.0

no shutdown

exit

Konfiguracja interfejsu FastEthernet 1/0 ( Do Biuro )  
interface f1/0 ( Do Klient )

ip address 50.0.0.1 255.0.0.0

no shutdown

exit

no ip domain lookup

router ospf 9

network 50.0.0.0 0.255.255.255 area 0

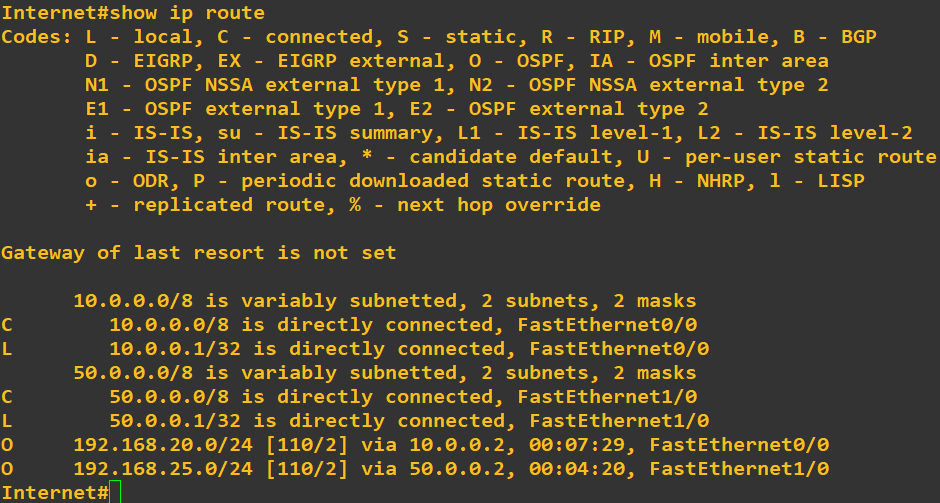
network 10.0.0.0 0.255.255.255 area 0

end

wr

Potwierdzamy nadpisanie konfiguracji.

show ip route



**Router Klient konfiguracja:**

enable

configure terminal

hostname Klient

Konfiguracja interfejsu FastEthernet F1/0 ( Do Internet )  
interface f1/0

ip address 50.0.0.2 255.0.0.0

no shutdown

exit

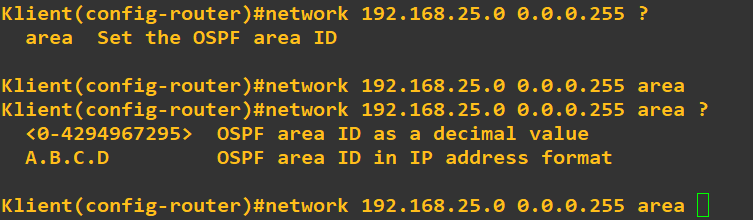
Konfiguracja interfejsu FastEthernet F2/0 ( Do Ethernetswitch-2 )  
interface f2/0

ip address 192.168.25.1 255.255.255.0

no shutdown

exit

no ip domain lookup

router ospf 9  
  


network 192.168.25.0 0.0.0.255 area 0

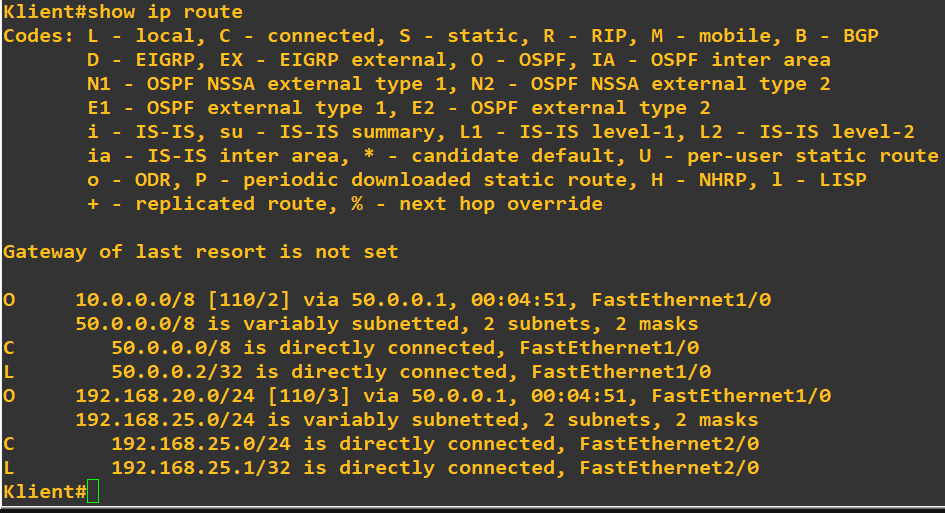
network 50.0.0.0 0.255.255.255 area 0

exit

do write

end

show ip route

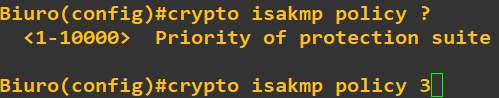


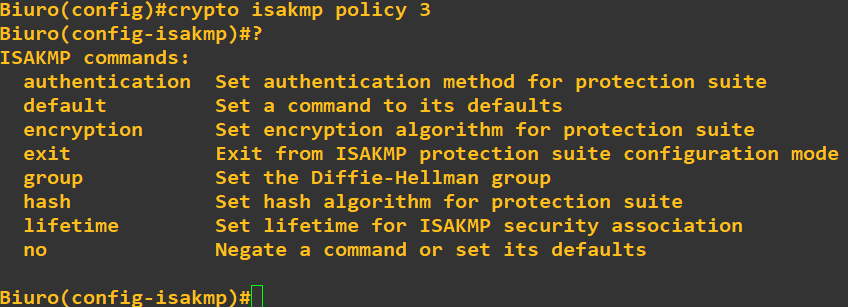
**Stworzenie strategii negocjacji kluczy i ustanowienia sieci VPN**

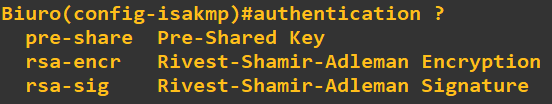
**Router Biuro konfiguracja:**

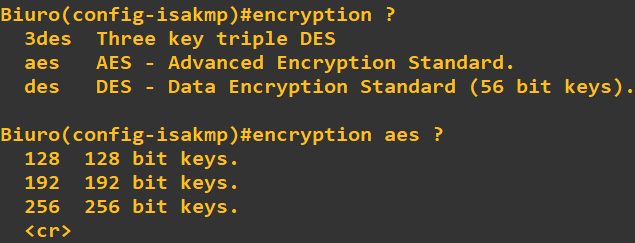
enable

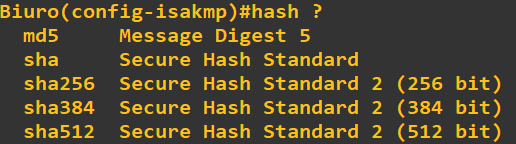
configure terminal

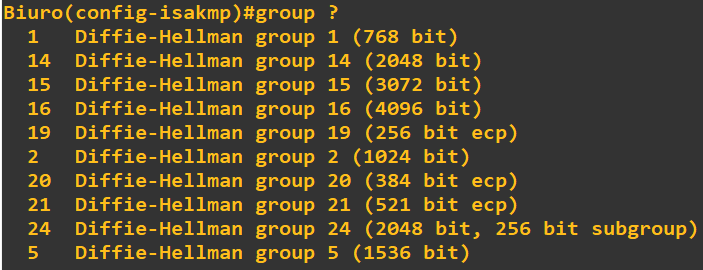
Ustawienie priorytetu (3 – numer priorytetu )  
crypto isakmp policy 3  
  












authentication pre-share

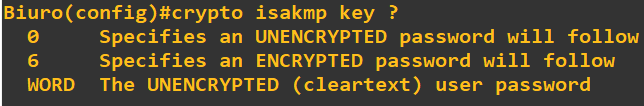
Advanced Encryption Standard wspiera długość klucza o 256-bitach.  
encyrption aes 256

Algorytm do zapewineia integralności danych. Zapewnia, że pakiet pochodzi z miejsca, z kutego został wysłany i że nie został zmodyfikowany podczas przesyłania   
hash sha

Określa identyfikator grupy Diffiego-Hellmana, którego dwaj użytkownicy IPsec używają do wyprowadzenia wspólnego sekretu bez przesyłania go do siebie. Im niższy numer grupy Diffiego-Hellmana, tym mniej czasu procesora wymaga jego wykonanie. Im wyższy numer grupy Diffiego-Hellmana, tym większe bezpieczeństwo. Aby obsłużyć duże rozmiary kluczy wymagane przez AES, negocjacje ISAKMP powinny korzystać z grupy Diffle-Hellman 5 (1536 bitów ).   
group 5

Określa czas życia SA. Wartość domyślna to 86 400 sekund lub 24 godziny. Z reguły krótszy czas życia zapewnia bezpieczniejsze negocjacje z ISAKMP (do pewnego momentu). Jednak w przypadku krótszych okresów życia urządzenie zabezpieczające szybciej tworzy przyszłe zabezpieczenia IPsec.   
lifetime 3600

exit



Konfiguracja preshared authentication key „p1” dla adresu 50.0.0.2  
 crypto isakmp key p1 address 50.0.0.2

**Router Klient konfiguracja:**enable

configure terminal

crypto isakmp policy 3

authentication pre-share

encyrption aes 256

hash sha

group 5

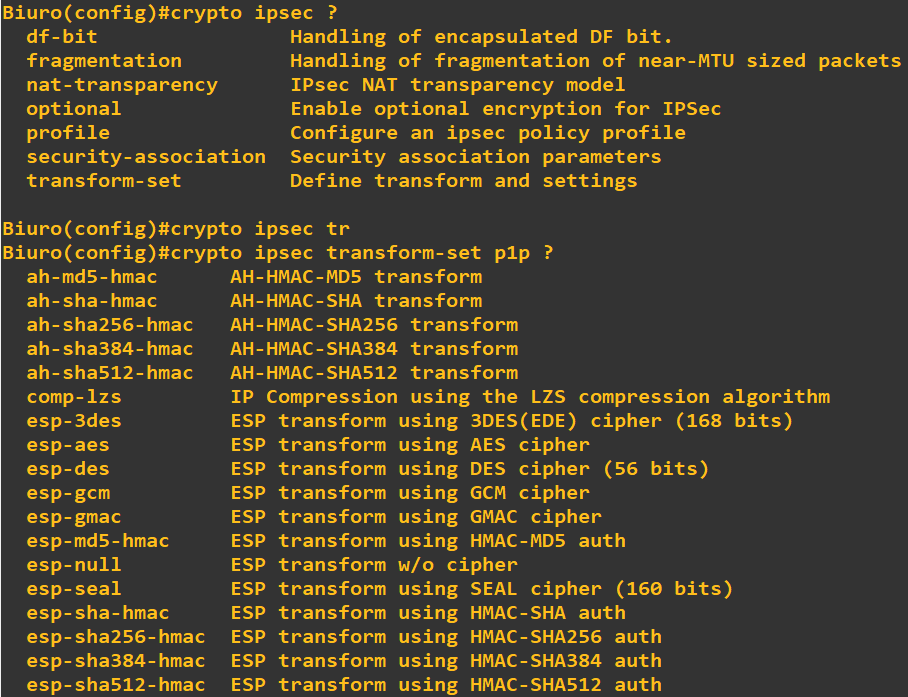
lifetime 3600

exit

crypto isakmp key p1 address 10.0.0.2

**Tworzenie metody szyfrowania transform-set**

**Router Biuro konfiguracja:**

****

ESP Encryption Transform esp-aes jest to ESP z 128-bitowym algorytmem szyfrowania AES.   
Esp-sha-hmac jest to esp algorytm uwierzytelniania SHA ( wariant HMAC )  
Cisco nie zaleca już używania ah-md5-hmac, esp-md5-hmac, esp-des lub esp-3des. Zamiast tego powinieneś użyć ah-sha-hmac, esp-sha-hmac lub esp-aes.   
crypto ipsec transform-set p1p esp-aes esp-sha-hmac

exit

Określa liczbę sekund, przez którą stowarzyszenie zabezpieczeń będzie żyć przed wygaśnięciem.  
crypto ipsec security-association lifetime seconds 3600

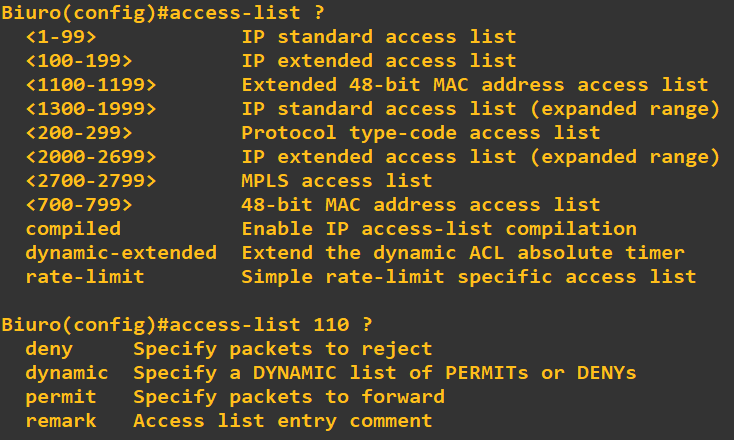
**Router Klient konfiguracja:**

crypto ipsec transform-set p1p esp-aes esp-sha-hmac

exit

crypto ipsec security-association lifetime seconds 3600

**Access list**

****

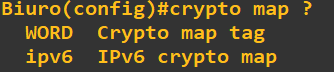
**Router Biuro konfiguracja:**

Rozszerzone listy ACL, zezwalają na ruch od source do host.  
access-list 110 permit ip 192.168.20.0 0.0.0.255 192.168.25.0 0.0.0.255

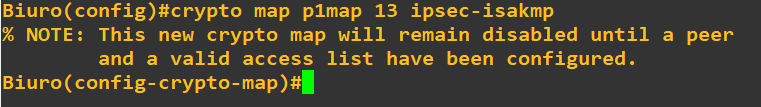
**Router Klient konfiguracja:**

access-list 110 permit ip 192.168.25.0 0.0.0.255 192.168.20.0 0.0.0.255

**Crypto Mapa**

**Router Biuro konfiguracja:  
  
**

Stworzenie crypto mapy o nazwye „p1map” - crypto map map-name seq-num ipsec-isakmp  
crypto map p1map 13 ipsec-isakmp

****Określa ACL dla wpisu mapy  
match address 110

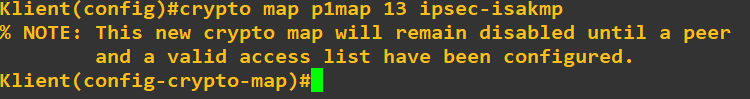
Ustawienie peer dla okręslonego adresu IP  
set peer 50.0.0.2  
  


Określa, który transform-set może zostać użyty z wpisem Crypto map  
set transform-set p1p

exit

**Router Klient konfiguracja:**

crypto map p1map 13 ipsec-isakmp



match address 110

set peer 10.0.0.2

set transform-set p1p

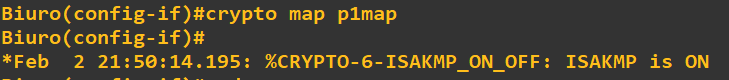
exit

**Aplikacja cryptomapy w interfejsie**

**Router Biuro konfiguracja:**

interface f0/0

Przypisanie wcześniej utworzonej crypto-mapy do konkretnego interfejsu  
crypto map p1map

****

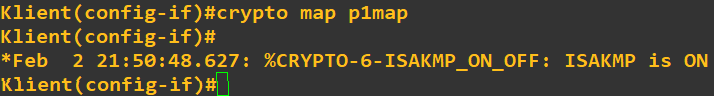
end

wr

**Router Klient konfiguracja:**

interface f1/0

crypto map p1map



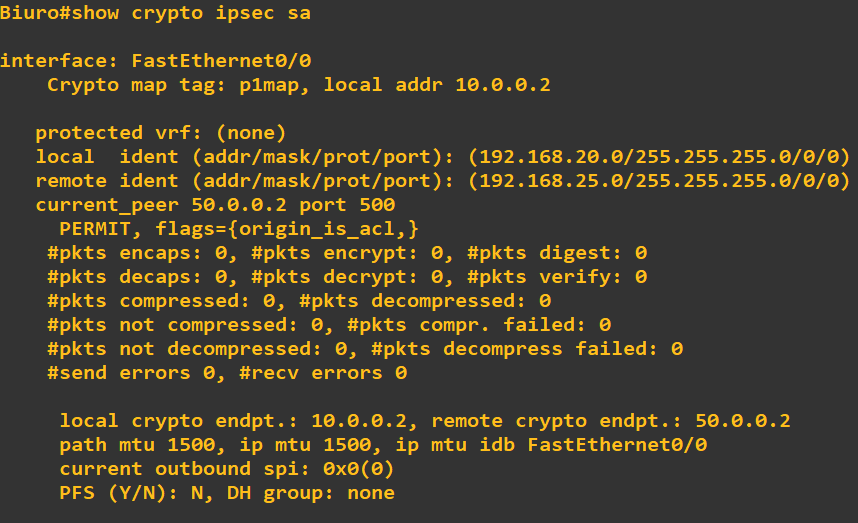
end

wr

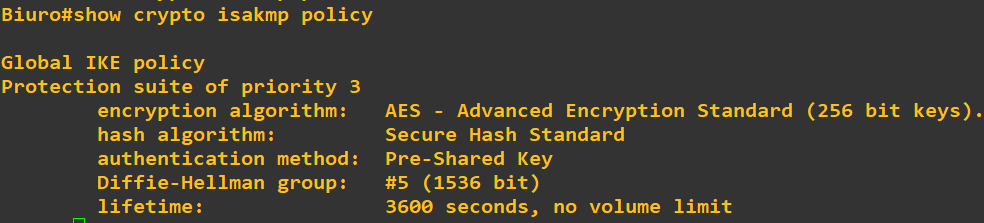
**Na wszystkich urządzeniach zaleca się zapisanie działającej konfiguracji, można to zrobić dzięki poleceniu:  
copy running-config startup-config**

**Router Biuro sprawdzenie:**

Polecenie pokazuje jak jest zbudownay IPsec SA pomiędzy jednym i drugim peer’em. W tym wypadku zaszyfrowany tunel jest zbudowany między 10.0.0.2,a 50.0.0.2.   
show crypto ipsec sa

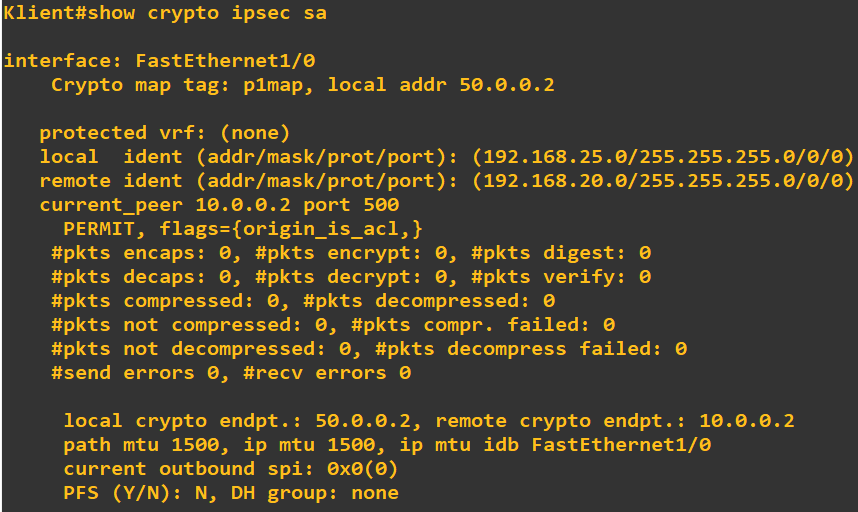


show crypto isakmp policy

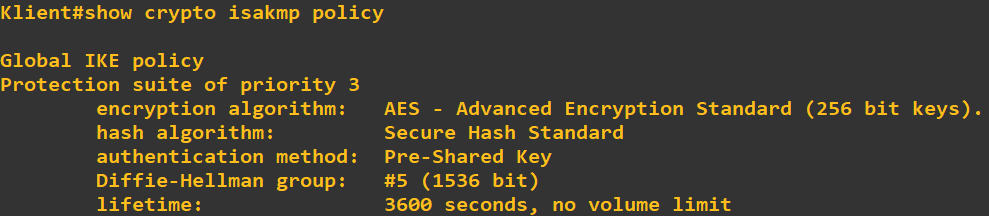


**Router Klient sprawdzenie:**

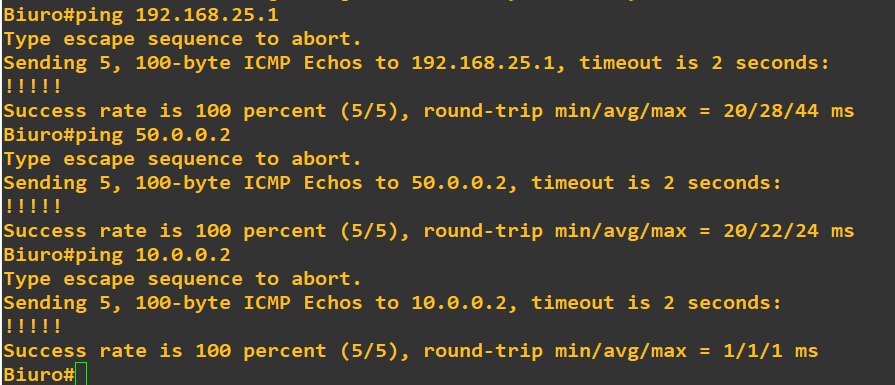
Pomiędzy 50.0.0.2, a 10.0.0.2  
show crypto ipsec sa

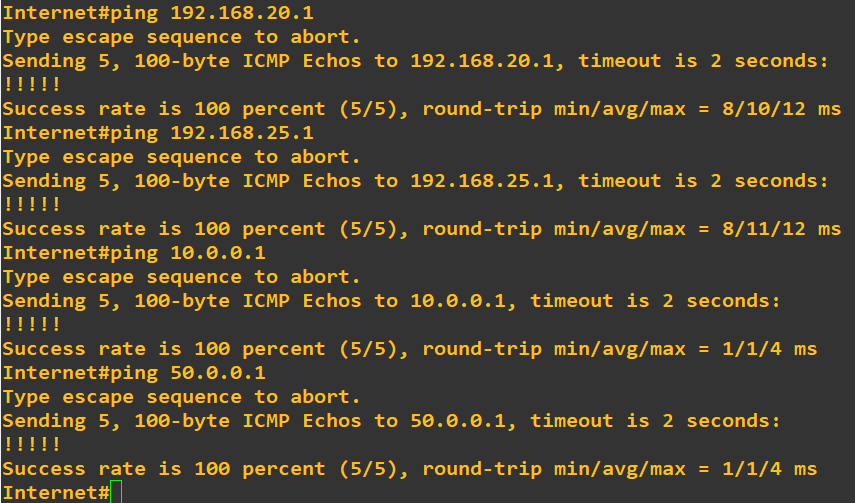


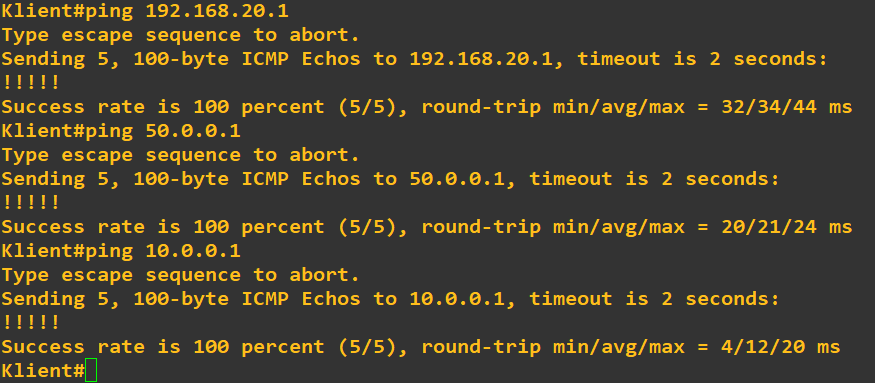
show crypto isakmp policy



**Ping from Biuro:**



**Ping from Internet:**  
  


**Ping from Klient:**  
  


**Wnioski:**Po wykonaniu wszystkich powyższych operacji, ruch powinien bez problemu działać między urządzeniami i interfejsami co widać na załączonych wyżej zrzutach ekranu. Tak konfiguracja zapewnia odpowiednie bezpieczeństwo jak i szyfrowanie.

**Zalety używania router-ospf:**

* OSPF jest prawdziwym protokołem routingu bez pętli. Wywodzi się z zalet samego algorytmu.
* Zmiany tras mogą zostać przesłane do całego systemu w najkrótszym czasie.
* Sam protokół minimalizuje obciążenie.
* Poprzez ścisły podział poziomu routingu, zapewnia bardziej niezawodne trasowanie.
* Dobre bezpieczeństwo. Protokół OSPF obsługuje uwierzytelnianie oparte na interfejsie w postaci zwykłego tekstu i md5.
* OSPF dostosowuje się do różnych skali sieci, do tysięcy jednostek.

**Zalety crypto-map:**

* Wybiera przepływ danych wymagających zabezpieczeń.
* Definiuje zasady dla przepływów i do którego miejsca ruch musi dotrzeć.

**Zalety Transform-set**

* Jest to kombinacja protokołów bezpieczeństwa, algorytmów i innych ustawień, które mają zastosowanie do ruchu chronionego protokołem IP Security.
* Podczas negocjacji powiązania zabezpieczeń IPSec uczestnicy zgadzają się na użycie określonego zestawu transformacji podczas ochrony określonego przepływu
* Szyfrowanie ESP zapewnia poufność danych
* Uwierzytelnianie danych zapewnia algorytm MD5 lub SHA ( HMAC ), generalnie SHA jest uważany za silniejszy lecz wolniejszy niż MD5

**Bibliografia:**  
  
https://community.cisco.com  
https://cisco.com  
http://vpn.svera.pl/  
https://pl.wikipedia.org  
https://www.netacad.com/  
https://www.router-switch.com