

**Zarządzanie połączeniami i konfiguracją sieci LAN
z wykorzystaniem routera Cisco ISR**

Numer ćwiczenia: 1

Laboratorium z przedmiotu:

Zarządzanie i bezpieczeństwo w sieciach teleinformatycznych

Kod przedmiotu: TS1D6220

Instrukcję opracował:
dr inż. Andrzej Zankiewicz

1. Charakterystyka routerów ISR

Współczesne routery oprócz podstawowej funkcji jaką jest przekazywanie pakietów IP pomiędzy sieciami dostępnymi przez poszczególne interfejsy mogą dodatkowo realizować wiele innych zadań związanych m.in. zarządzanie połączeniami, konfiguracją, usługami sieciowymi, a także zaawansowane funkcje zabezpieczeń. Przykładem takich urządzeń są routery ze zintegrowanymi usługami ISR (*Integrated Services Router*) firmy Cisco. W szczególności urządzenia te zapewniają:

Zestaw funkcji firewall Cisco IOS - oprogramowanie routera integruje zaporę sieciową (firewall) opartą na kontroli wybranych elementów przesyłanych pakietach z routerem, który również monitoruje ruch danych na poziomie aplikacji. Kontekstowa Kontrola Dostępu (CBAC - *Context-Based Access Control*) pozwala na monitorowanie aplikacji korzystających z protokołów TCP i UDP, HTTP (np. blokowanie kodu Java), SMTP, FTP, TFTP jak również aplikacji multimedialnych bazujących na protokołach takich jak SIP, SCCP (Skinny), H.323, RTSP, RealAudio oraz innych aplikacji do transmisji głosu/obrazu.

Wykrywanie włamań - Cisco IDS (*Intrusion Detection System*) rozpoznaje ponad sto typowych metod ataku. Jest to realizowane przy pomocy sygnatur służących do wyszukiwania określonych wzorów w transmitowanych danych, co pozwala na wczesne wykrywanie prób ataku. W przypadku wykrycia podejrzanych czynności, Cisco IDS blokuje atak przed spenetrowaniem sieci i wysyła komunikat alarmowy do konsoli zarządzania.

Szyfrowanie danych - korzystając z oprogramowania lub dedykowanych modułów sprzętowych, routery Cisco ISR pozwalają na szyfrowanie komunikacji VPN przy użyciu 56-bitowego klucza *Data Encryption Standard* (DES), 128-bitowego Triple DES (3DES) lub 256-bitowego *Advanced Encryption Standard* (AES). Możliwe jest również szyfrowanie wykorzystujące Infrastrukturę Klucza Publicznego (PKI) zgodną ze standardem X.509.

Kontrola Dostępu do Sieci (NAC - *Network Admission Control*) – oprogramowanie wykorzystujące Cisco Trust Agent (CTA), zainstalowane na komputerach biurowych i serwerach, umożliwia zbieranie informacji o zgodności z wymaganiami bezpieczeństwa i wersji systemu operacyjnego. CTA może przekazywać informacje, dostarczane przez oprogramowanie antywirusowe takich dostawców jak Trend Micro, urządzeniom sieciowym Cisco, które następnie podejmują decyzję o umożliwieniu lub zablokowaniu dostępu do sieci.

Filtrowanie adresów URL - Filtry adresów URL mogą zostać wykorzystane przez firmę do uniemożliwienia pracownikom dostępu do stron WWW, które nie są związane z wykonywanymi przez nich zadaniami. Funkcja ta gwarantuje, że zasoby i zdolność transmisyjna sieci będą zużywane na transmisje nie związane z wykonywaną pracą. Wykorzystując bazę danych adresów URL, zawierającą ponad 20 milionów

adresów podzielonych na 60 kategorii, administratorzy mogą uniemożliwić pracownikom dostęp do niepożądanych treści WWW.

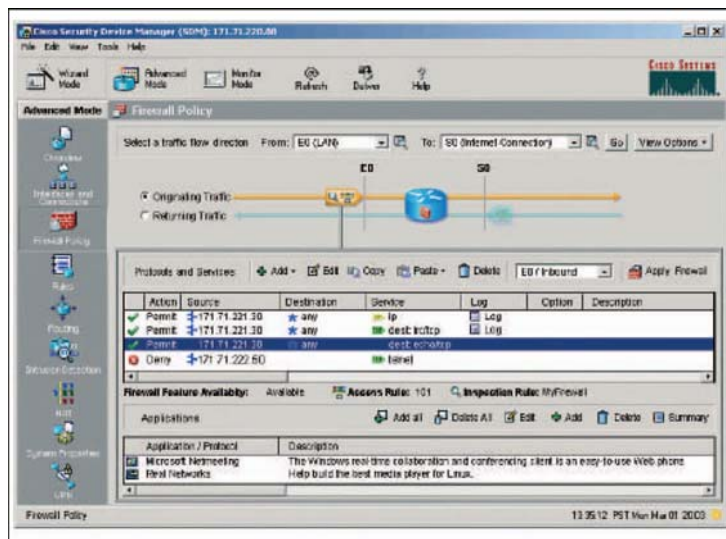
Telefonia z wykorzystaniem routerów Cisco

Coraz więcej firm korzysta z komunikacji głosowej za pośrednictwem sieci IP (*Voice over IP*). Telefonia IP okazała się praktycznym i ekonomicznym rozwiązaniem, szczególnie dla firm posiadających oddziały lub przedsiębiorstwa zależne. Oprócz obniżenia kosztów połączeń wewnętrznych, tzn. nawiązywanych pomiędzy centralą i oddziałami, konserwacja jednej sieci i zarządzanie jedną siecią, a nie dwoma, zmniejsza nakłady inwestycyjne i koszty bieżące. Łatwiejsza skalowalność, czyli proste dodawanie nowych użytkowników telefonów oraz stacji roboczych PC, stanowi kolejny ważny atut telefonii IP.

Telefonia IP z wykorzystaniem wbudowanej w system Cisco IOS „centralki” CME (*Call manager Express*) będzie przedmiotem dwóch innych ćwiczeń.

Ustandaryzowane zarządzanie

Wiele routerów Cisco (w tym wszystkie ISR) posiadają możliwość korzystania z graficznego narzędzia do konfiguracji o nazwie *Cisco Security Device Manager* (SDM). Oprogramowanie SDM, dostępne dla wszystkich routerów dostępowych od serii Cisco 800 do serii Cisco 3800, umożliwia szczególnie oddziałom firm i samodzielnym biurom korzystanie z narzędzia do bezpiecznej konfiguracji routera opartego na graficznym interfejsie WWW. SDM obsługuje sieci LAN/WAN, firewalle i konfigurację VPN oparte na zastosowaniu oprogramowania Cisco IOS. SDM posiada również funkcje audytu bezpieczeństwa, używane do sprawdzania konfiguracji routera i sugeruje metody poprawy poziomu bezpieczeństwa, zgodnie z aktualnymi zaleceniami. Na rysunku 1 przedstawiono widok okna oprogramowania SDM.



Rys. 1. Okno oprogramowania *Security Device Manager* (SDM)

Ponadto routery ISR zapewniają szereg mechanizmów związanych z zarządzaniem konfiguracją sieci lokalnej. Można wymienić tu protokół dynamicznego przydzielania adresów IP (DHCP) oraz mechanizm translacji NAT.

Protokół dynamicznego przydzielania adresów IP (DHCP).

Protokół DHCP (ang. *Dynamic Host Configuration Protocol*) działa w trybie klient-serwer. Protokół ten pozwala klientom DHCP w sieciach IP na uzyskiwanie informacji o ich konfiguracji z serwera DHCP. Użycie protokołu DHCP zmniejsza nakład pracy wymagany przy zarządzaniu siecią IP. Najważniejszym elementem konfiguracji odbieranym przez klienta od serwera jest adres IP klienta. Klient żąda uzyskania danych adresowych z sieciowego serwera DHCP. Ten serwer zarządza przydzielaniem adresów IP i odpowiada na żądania konfiguracyjne klientów. Serwer DHCP może odpowiadać na żądania pochodzące z wielu podsieci.

Administratorzy na ogół preferują serwery sieciowe z usługą DHCP, ponieważ takie rozwiązanie jest skalowalne i łatwo nim zarządzać. Routery Cisco mogą wykorzystywać specjalny zestaw funkcji systemu IOS firmy Cisco – *Easy IP* – w celu udostępnienia opcjonalnego, w pełni funkcjonalnego serwera DHCP. Domyślny okres dzierżawy ustawień konfiguracyjnych w wypadku oprogramowania *Easy IP* to 24 godziny. Rozwiązanie takie jest przydatne w małych firmach i biurach domowych, gdzie użytkownicy mogą wykorzystać funkcje protokołu DHCP i mechanizmu NAT. Administratorzy konfiguruje serwery DHCP tak, aby przydzielane były adresy ze zdefiniowanych pul adresów. W wypadku większości serwerów DHCP administratorzy mogą także zdefiniować adresy MAC obsługiwanych klientów i automatycznie przypisywać dla tych klientów zawsze te same adresy IP. Protokołem transportowym wykorzystywanym przez protokół DHCP jest UDP (ang. *User Datagram Protocol*).

Istnieją trzy mechanizmy przydzielania adresów IP dla klientów:

- Alokacja automatyczna – protokół DHCP przypisuje klientowi stały adres IP.
- Alokacja ręczna – adres IP dla klienta jest przydzielany przez administratora. Protokół DHCP przesyła adres do klienta.
- Alokacja dynamiczna – protokół DHCP dzierżawi klientowi adres IP na pewien ograniczony odcinek czasu.

Mechanizm translacji NAT.

Technologia NAT to mechanizm umożliwiający ograniczenie liczby zarejestrowanych adresów IP w dużych sieciach. Podczas przesyłania pakietów za pośrednictwem urządzeń sieciowych, takich jak router brzegowy, źródłowy adres IP jest tłumaczony z adresu prywatnej sieci wewnętrznej na publiczny adres IP umożliwiający routowanie. Pozwala to na transport pakietu przez zewnętrzne sieci publiczne, np.: przez Internet. Publiczny adres w odpowiedzi jest konwertowany z powrotem na format wewnętrznej adresu sieci prywatnej w celu dostarczenia go do odpowiedniego miejsca w sieci wewnętrznej. Odmiana technologii NAT, znana jako translacja adresu portu PAT (ang. *Port Address Translation*) umożliwia konwertowanie wielu wewnętrznych adresów sieci prywatnych na pojedynczy zewnętrzny adres sieci publicznej.

Routerzy, serwery i pozostałe kluczowe urządzenia sieciowe zazwyczaj wymagają ręcznego skonfigurowania statycznych adresów IP. Jednakże w przypadku zwykłych komputerów pełniących rolę klientów nie jest wymagane określenie konkretnego adresu – wybierany jest jakikolwiek adres z określonej puli adresów. Zakres ten jest zazwyczaj określony przez maskę podsieci. Stacji roboczej w określonej podsieci może zostać przypisany dowolny adres z danego zakresu, zaś pozostałe ustawienia są statyczne (łącznie z maską podsieci, domyślną bramą i serwerem DNS).

Urządzenie realizujące translację NAT zazwyczaj działa na granicy sieci, która ma pojedyncze połączenie z sąsiednią siecią. Gdy host w sieci chce przesłać dane do hosta znajdującego się na zewnątrz, przekazuje pakiet do routera brzegowego. Router brzegowy realizuje proces NAT, czyli proces translacji prywatnego adresu wewnętrznego hosta na publiczny adres zewnętrzny, który może być routowany w sieci Internet.

W systemie Cisco IOS zdefiniowane zostały następujące pojęcia związane z technologią NAT:

- **Wewnętrzny adres lokalny** – adres IP przypisany do hosta w sieci wewnętrznej.
 - **Wewnętrzny adres globalny** – adres ten reprezentuje dla sieci zewnętrznych jeden lub więcej wewnętrznych, lokalnych adresów IP.
 - **Zewnętrzny adres lokalny** – adres IP zewnętrznego hosta, pod którym jest on widziany przez hosty znajdujące się w sieci wewnętrznej.
 - **Zewnętrzny adres globalny** – adres IP przypisany do hosta w sieci zewnętrznej.
- Ten adres przypisany jest przez właściciela hosta.

Translacje NAT mogą być wykorzystywane do różnych celów, a przetłumaczone adresy mogą być przydzielane dynamicznie lub statycznie. Statyczna translacja NAT umożliwia utworzenie odwzorowania typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi. Jest to szczególnie przydatne w przypadku hostów, które muszą mieć stały adres dostępny z Internetu. Takimi wewnętrznymi hostami mogą być serwery lub urządzenia sieciowe w przedsiębiorstwie.

Dynamiczna translacja NAT służy do odwzorowania prywatnego adresu IP na adres publiczny. Hostowi w sieci jest przypisywany dowolny adres z puli publicznych adresów IP. Natomiast technika przeciążenia, lub inaczej translacji PAT, służy do odwzorowania wielu prywatnych adresów IP na jeden publiczny adres IP. Istnieje możliwość odwzorowania wielu adresów na jeden adres IP, ponieważ z każdym adresem prywatnym związany jest inny numer portu.

W technologii PAT tłumaczone adresy są rozróżniane przy użyciu unikatowych numerów portów źródłowych powiązanych z globalnym adresem IP. Numer portu zakodowany jest na 16 bitach. Całkowita liczba adresów wewnętrznych, które mogą być przetłumaczone na jeden adres zewnętrzny, może teoretycznie wynosić nawet 65 536. W rzeczywistości do jednego adresu IP może zostać przypisanych około 4000 portów.

Istnieją także pewne niekorzystne efekty użycia translacji NAT. Włączenie translacji adresów powoduje utratę funkcjonalności, szczególnie w przypadku

protokołów lub aplikacji wykorzystujących wysyłanie informacji o adresie IP w treści zasadniczej pakietu IP. Wymaga to dodatkowej obsługi na urządzeniu.

Użycie translacji NAT wydłuża opóźnienia. Opóźnienia występujące podczas przełączania ścieżek są spowodowane operacjami translacji wszystkich adresów IP w nagłówkach pakietów. Pierwszy pakiet będzie zawsze przesyłany wolną ścieżką. Oznacza to, że dla pierwszego pakietu używane jest przełączanie procesowe. Pozostałe pakiety będą przesyłane ścieżką z szybkim przełączaniem, o ile istnieje odpowiedni wpis w pamięci podręcznej. Spadek wydajności może stanowić poważny problem, ponieważ translacja NAT jest obecnie realizowana przy użyciu przełączania procesowego. Procesor musi zbadać każdy pakiet, aby stwierdzić, czy podlega on translacji. Procesor musi też zmodyfikować nagłówek IP, ewentualnie również nagłówek TCP lub UDP. Jedną z istotnych wad wdrażania i stosowania usługi NAT jest utrata możliwości śledzenia pakietów IP na całej ścieżce transportowej (end-to-end). Śledzenie pakietów jest znacznie utrudnione, ponieważ w kolejnych przeskokach z translacją NAT adres w pakiecie wielokrotnie się zmienia.

Celem ćwiczenia jest praktyczne poznanie możliwości wykorzystania routerów ISR do zarządzania konfiguracją i funkcjami bezpieczeństwa sieci lokalnej.

2. Plan wykonywania ćwiczenia laboratoryjnego

1. Skonfigurować funkcję dynamicznego przydzielania adresów IP z puli 10.2.3.0/24 stacjom przyłączonym do portu *FastEthernet 0/1* routera ISR. Założyć, że router na tym interfejsie będzie miał adres 10.2.3.1/24 i adres ten powinien zostać wykluczony z puli adresów przyznawanych dla klientów.
2. Sprawdzić poprawność przydzielania adresów przez router dla obu stacji klienckich znajdujących się na stanowisku laboratoryjnym (dołączonych do routera z wykorzystaniem przełącznika).
3. Skonfigurować funkcję translacji adresów typu „wiele-do-jednego” (NAT overload) dla połączeń stacji w sieci lokalnej (dołączonych do interfejsu *FastEthernet0/1* routera) z Internetem. Dostęp do Internetu zostanie skonfigurowany poprzez interfejs *FastEthernet 0/0* dołączony do sieci laboratoryjnej zapewniającej dynamiczne przypisywanie adresów IP.
4. Ustawić w routerze domyślną trasę statyczną zapewniającą dostęp do Internetu przez interfejs *FastEthernet 0/0*.
5. Sprawdzić dostępność połączenia z Internetem na obu dołączonych do routera stacjach klienckich. Programem *tracert* określić trasę połączenia.
6. Odczytać i zinterpretować zawartość tablicy translacji NAT w routerze dla połączeń TCP oraz ICMP. W jaki sposób identyfikowane są wykonane translacje dla komunikatów protokołu ICMP?
7. Zapoznać się z oprogramowaniem SDM do zarządzania routerem. Posługując się oprogramowaniem SDM dokonać zmiany wybranych parametrów skonfigurowanych w poprzednich punktach (np. zakresu przyznawanych adresów IP).

W sprawozdaniu należy zamieścić opis wykonanych konfiguracji i testów uruchomionych usług.

3. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

4. Literatura

1. Józefiak A.: CCNA 200-125. Zostań administratorem sieci komputerowych Cisco. Helion, Gliwice, 2017.
2. Józefiak A.: GNS3. Emulowanie sieci komputerowych Cisco. Helion, Gliwice, 2017
3. Dooley K., Brown I.J.: Cisco. Receptury. Helion, Gliwice, 2004.
4. Dokumentacja techniczna *Cisco* (dostępna w laboratorium oraz w witrynie www.cisco.com)