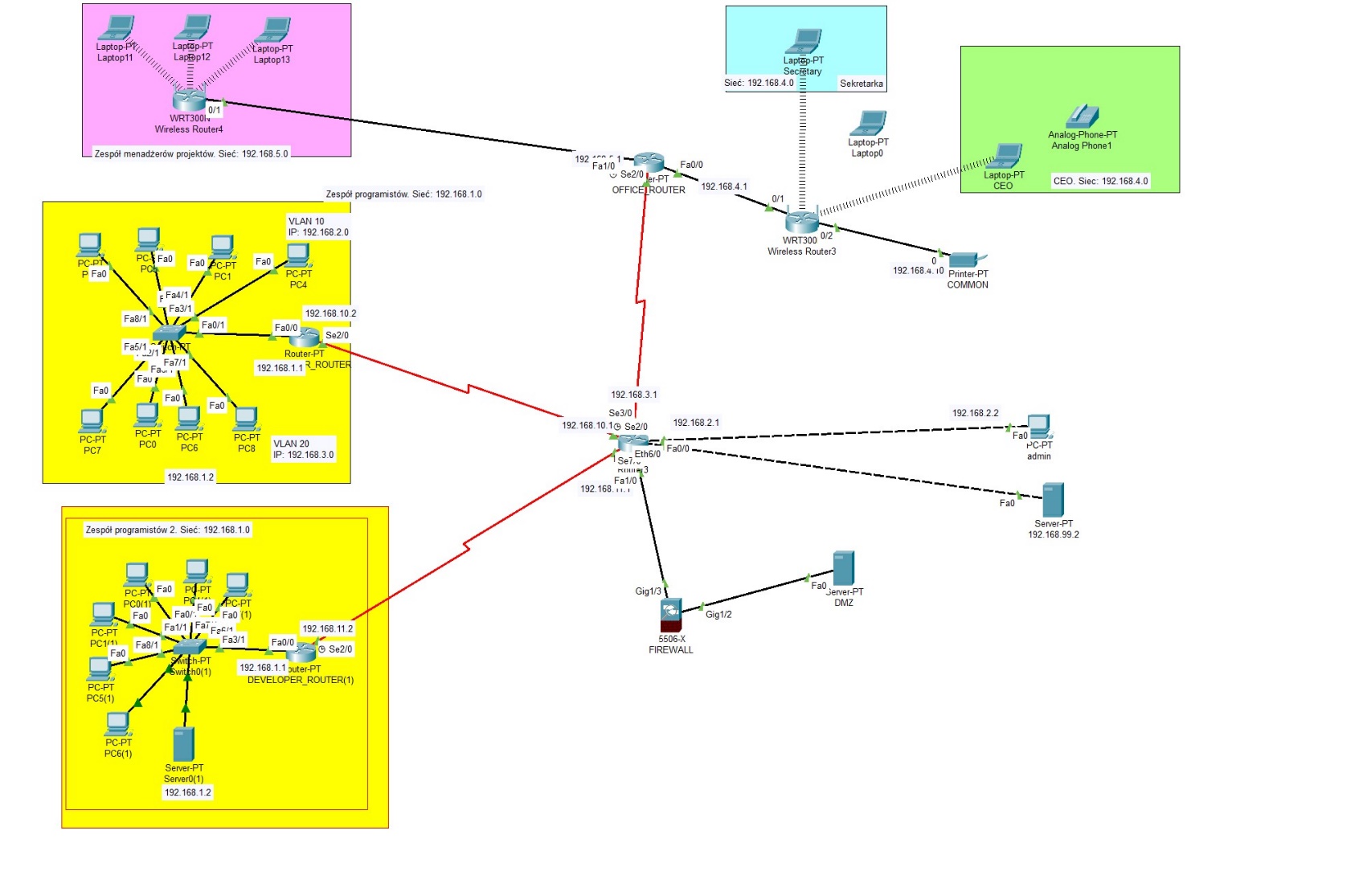
|  |  |
| --- | --- |
| Politechnika Świętokrzyska | |
| **Zespół:** Daniel Rogowski, David Salwa | **Grupa:** 1ID24B |
| **Projekt:** Pracownia Informatyczna |  |



Powyższe zdjęcie przedstawiania obraz zbudowanej przez zespół infrastruktury. Powyższa sieć odzwierciedla pracownię informatyczną, w której każdy „pokój” jest podzielony kolorem. Najważniejszym z punktu widzenia działalności pracowni jest „zielony” pokój. W tym pokoju swoją podsieć ma szef całej firmy, który jest podłączony do swojej podsieci (routera) za pomocą WI-FI. Jest tutaj włączone DHCP dla każdego urządzenia. Obok niego znajduje się sieć, w której pracuje seketarka/sekretarz (kolor niebieski), który również jest podłączony za pomocą WIFI i adres jest przypisane automatycznie (DHCP). Obie te sieci mają dostęp do drukarki o statycznym adresie *192.168.4.10*.

* konfiguracja serwera DHCP

Kolor „różowy” identyfikuje sieć (*192.168.5.0)* project managerów, osób zarządzającymi projektami. Tutaj również został zastosowany DHCP oraz podłączenie bezprzewodowe (WI-FI). W związku z tym, że przedstawiany pokój wymaga komunikacji z programistami (kolor żółty), została udostępniona możliwość komunikacji z tymi „pokojami”.

* VLANy

Kolor „żółty” przedstawia dwa pokoje programistów. Tak jak wyżej zostało opisane przedstawiane pokoje muszą posiadać komunikację z kolorem różowym. Pokój przedstawiony wyżej posiada również 2 VLANy, o adresach VLAN10: *192.168.2.0* oraz VLAN20: *192.168.3.0*, obie te „podsieci” komunikują się ze „światem” za pomocą routera, którego domyślną bramą jest adres *192.168.1.1*, natomiast adresem komunikującym się ze światem (adres) routera to: *192.168.10.2.* Wszystkie urządzenia są podłączone „fizycznie” (przez kabel) oraz posiadają wedle swoich „podsieci” automatycznie nadane adres IP (DHCP). Dodatkowo switch działa jako „trunk”, tak aby mógł przepuszczać ruch z tych podsieci do routera.

Drugi pokój „Żółty”, który jest umiejscowiony niżej w odróżnieniu od powyższego nie posiada VLAN-ów oraz adresy DHCP są przydzielane nie z routera, tylko z serwera DHCP. Reszta funkcjonalności jest identyczna do wyżej opisanego pokoju. Różnice jakie posiada to inne adresy IP: *192.168.1.0*, natomiast serwer DHCP ma statyczny adres IP: *192.168.1.2,* bramą domyślną jest adres: *192.168.1.1*, natomiast adresem komunikacyjnym ze „światem” jest adres *192.168.11.2.*

* standardowe oraz rozszerzone listy dostępu ACL

Komputerem bez „koloru” po prawej stronie jest komputer serwisowy o adresie *192.168.2.2*. Ta sieć jest zarezerwowana tylko dla tego komputera. Dodatkowo żaden z innych komputerów nie ma możliwości komunikacji z tym komputerem, natomiast ten komputer ma możliwość komunikacji z innymi komputerami. Taka funkcja została wdrożona dzięki listów ACL.

* dostępy ssh

Komputer bez „koloru” jest również jedynym który ma dostęp do „głównego” routera (czyli tego który jest połączony do 5 innych urządzeń) po porcie 22 czyli ssh w celu możliwości konfiguracji ustawień oraz dostępów w sieci.

* zabezpieczenia przez atakami MAC

Obok pokoju „Niebieskiego” który jest obok pokoju CEO jest komputer który chce się włamać do sieci wi-fi, dzięki zabezpieczeniom adresacji MAC nie ma takiej możliwości. Aby mógł zostać dodany należy dodać jego adres MAC do routera który zezwoli na połączenia.

* konfiguracja syslogu

W serwerze Server0(1) dodaliśmy również usługę syslog która śledzi wydarzenia na routerach w zółtej sieci oraz w routerze głównym dzięki czemu można podejrzeć kiedy zostały wykonany zmiany na tych routerach. Co ułatwi nam monitorowanie zmian i ułatwi sprawdzenie kiedy ktoś mógł coś podejrzanego wykonać.

* konfiguracja AAA

W tym samym serwerze dodaliśmy usługę AAA która pozwala nam zalogować się za pomocą tych samych danych logowania na innych serwerach. Usługę tą wykorzystują routery na żółtym tle oraz główny.

* konfiguracja NTP

Dodatkowo, w ramach dalszego ulepszania naszej infrastruktury sieciowej, zaimplementowaliśmy protokół Network Time Protocol (NTP) na trzech wcześniej wspomnianych routerach wykorzystujących EIGRP. Decyzja ta wynika z potrzeby synchronizacji czasu w całej sieci, co jest kluczowe dla utrzymania właściwego porządku sekwencyjnego zdarzeń i logów systemowych. NTP zapewnia, że wszystkie urządzenia sieciowe, w tym routery, mają ustawiony dokładny i jednolity czas, co jest niezbędne dla efektywnego monitorowania i rozwiązywania problemów sieciowych. Ta integracja NTP z naszymi routerami EIGRP dodatkowo zwiększa efektywność naszej sieci, umożliwiając bardziej precyzyjne śledzenie i analizę danych sieciowych, co jest nieocenione w utrzymaniu wysokiej wydajności i niezawodności naszej infrastruktury sieciowej.

* Dynamiczne protokoły routingu.

W procesie projektowania naszej sieci korporacyjnej, zdecydowaliśmy się na wybór Enhanced Interior Gateway Routing Protocol (EIGRP) jako naszego protokołu dynamicznego routingu, głównie ze względu na jego zdecentralizowaną architekturę, szybką konwergencję i skalowalność. Każdy router w sieci przechowuje własną kopię tabeli routingu, co zapewnia odporność na zakłócenia i stabilność działania sieci. EIGRP wykorzystuje algorytm DUAL do efektywnego obliczania i aktualizowania ścieżek routingu, co jest kluczowe w dynamicznych środowiskach korporacyjnych. Jego zdolność do obsługi dużych sieci oraz kompatybilność z różnorodnym sprzętem sieciowym sprawiają, że jest to idealne rozwiązanie dla naszej rozrastającej się infrastruktury, umożliwiając łatwą integrację z istniejącymi komponentami sieciowymi i upraszczając zarządzanie siecią.

* Konfiguracja poziomów dostępowych na urządzeniach sieciowych

W dalszym ciągu procesu optymalizacji naszej sieci, skupiliśmy się na konfiguracji poziomów dostępowych na urządzeniach sieciowych, aby zapewnić odpowiednią kontrolę i bezpieczeństwo. Na każdym z naszych routerów skonfigurowaliśmy specjalne konta użytkowników o nazwie "user", które domyślnie posiadają poziom uprawnień równy 0. Ta strategia pozwala na zapewnienie podstawowego dostępu do urządzenia dla ogólnych celów monitorowania, jednocześnie ograniczając możliwość dokonywania zmian w konfiguracji lub dostępu do wrażliwych danych.

Aby osiągnąć ten poziom bezpieczeństwa, użyliśmy następujących komend w konfiguracji naszych routerów:

en  
conf t  
username user privilege 0 secret user  
exit  
copy running-config startup-config

Ustawienie poziomu uprawnień na 0 dla domyślnego konta użytkownika "user" jest równoznaczne z zapewnieniem tylko najbardziej ograniczonego dostępu, co jest zgodne z zasadą najmniejszych uprawnień – fundamentalną praktyką w zarządzaniu bezpieczeństwem sieciowym. Dzięki temu podejściu, nasza sieć pozostaje elastyczna i otwarta dla niezbędnego monitorowania, jednocześnie chroniąc przed nieautoryzowanym dostępem i potencjalnymi zagrożeniami zewnętrznymi.

* procedura przywracania obrazu systemu operacyjnego urządzenia sieciowego

W ramach naszych działań związanych z zarządzaniem i utrzymaniem infrastruktury sieciowej, opracowaliśmy i zaimplementowaliśmy procedurę przywracania obrazu systemu operacyjnego urządzenia sieciowego. Centralnym elementem tej procedury jest wykorzystanie usługi Trivial File Transfer Protocol (TFTP) na naszym głównym routerze. Dzięki TFTP zdołaliśmy skutecznie zarchiwizować obraz systemu operacyjnego oraz aktualną konfigurację tego routera na najbliższym serwerze. Ta metoda zapewnia kluczowe zabezpieczenie w przypadku awarii lub konieczności szybkiego przywrócenia konfiguracji.

W sytuacji, gdy wymagane jest przywrócenie systemu, możemy szybko i efektywnie odtworzyć zarówno obraz systemu operacyjnego, jak i konfigurację urządzenia z zapisanej kopii na serwerze TFTP. Proces ten zapewnia minimalizację czasu przestoju i pozwala na szybki powrót do pełnej funkcjonalności sieci. Dzięki regularnym kopiom zapasowym zarówno obrazu systemu operacyjnego, jak i konfiguracji, jesteśmy w stanie zapewnić ciągłość działania naszych usług sieciowych oraz ochronę przed potencjalnymi problemami wynikającymi z awarii sprzętu czy błędów oprogramowania.

* opis jakie zagrożenia mogą czekać kreowaną sieć

W kontekście bezpieczeństwa naszej nowo tworzonej sieci korporacyjnej, istotne jest rozpoznanie i zrozumienie potencjalnych zagrożeń, które mogą na nią wpłynąć. Obecnie, nasza sieć jest skonfigurowana tak, aby była bezpieczna do momentu potencjalnego włamania do jednego z urządzeń. Kluczowym elementem naszej strategii bezpieczeństwa jest wyłączenie wszystkich nieużywanych portów na urządzeniach sieciowych, co znacząco zmniejsza powierzchnię ataku dla potencjalnych zagrożeń.

Ponadto, każde urządzenie próbujące połączyć się zdalnie z naszą siecią Wi-Fi musi mieć przypisany adres MAC, co stanowi dodatkową warstwę zabezpieczeń. Jednakże, mimo tych środków ostrożności, istnieje ryzyko, że zdeterminowany atakujący może znaleźć sposób na obejście tych barier, na przykład poprzez spoofing adresu MAC lub wykorzystanie słabości w protokołach bezpieczeństwa Wi-Fi.

Najważniejszym aspektem naszej strategii bezpieczeństwa jest fakt, że jedynie urządzenie administratora posiada pełną kontrolę nad siecią. Chociaż to centralizuje zarządzanie i zwiększa efektywność, może to również stanowić punkt krytyczny. Jeśli urządzenie administratora zostanie skompromitowane, cała sieć może być narażona na ryzyko. Dlatego niezbędne jest zapewnienie wyjątkowo wysokiego poziomu bezpieczeństwa dla tego urządzenia, w tym stosowanie silnych haseł, regularne aktualizacje oprogramowania oraz monitorowanie wszelkich podejrzanych aktywności.

Podsumowując, choć nasza sieć jest zaprojektowana z myślą o bezpieczeństwie, zawsze istnieje ryzyko potencjalnych zagrożeń. Kluczem do minimalizacji tych ryzyk jest ciągłe monitorowanie, regularne aktualizacje bezpieczeństwa i świadomość, że żadna sieć nie jest całkowicie odporna na ataki.