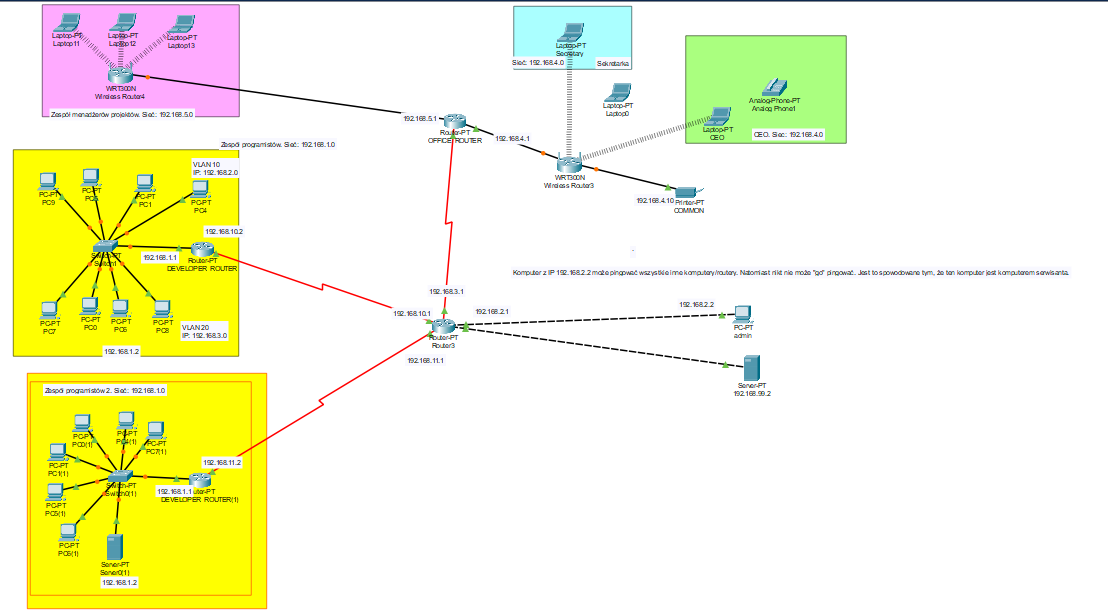
|  |  |
| --- | --- |
| Politechnika Świętokrzyska | |
| **Zespół:** Daniel Rogowski, David Salwa | **Grupa:** 1ID24B |
| **Projekt:** Pracownia Informatyczna |  |

W ramach projektu studenckiego podjęliśmy się ambitnego zadania zaprojektowania i implementacji kompleksowej infrastruktury sieciowej dla środowiska korporacyjnego. Celem projektu było stworzenie sieci o wysokim stopniu bezpieczeństwa, elastyczności i skalowalności, która mogłaby sprostać dynamicznie zmieniającym się potrzebom współczesnych organizacji. Zastosowano tutaj szereg nowoczesnych rozwiązań sieciowych, w tym VLANy, protokoły routingu, a także zaawansowane techniki zarządzania i monitorowania sieci. Nasze działania skupiały się na zapewnieniu niezawodności, wydajności oraz maksymalnego bezpieczeństwa sieci.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Urządzenie | Interfejs | Adres IP | Maska sieci | Brama domyślna |
| DEVELOPER\_ROUTER | SE2/0 | 192.168.1.1 | 255.255.255.0 | 192.168.1.1 |
| DEVELOPER\_ROUTER | FE0/0 | 192.168.10.2 | 255.255.255.252 | 192.168.10.1 |
| DEVELOPER\_ROUTER(1) | SE2/0 | 192.168.1.1 | 255.255.255.0 | 192.168.1.1 |
| DEVELOPER\_ROUTER(1) | FE0/0 | 192.168.11.2 | 255.255.255.252 | 192.168.11.1 |
| Router3 | FE0/0 | 192.168.2.1 | 255.255.255.252 | 192.168.2.1 |
| Router3 | SE2/0 | 192.168.10.1 | 255.255.255.252 | 192.168.10.1 |
| Router3 | SE3/0 | 192.168.3.1 | 255.255.255.252 | 192.168.3.1 |
| Router3 | Ethernet6/0 | 192.168.99.1 | 255.255.255.252 | 192.168.99.1 |
| Router3 | Se7/0 | 192.168.11.1 | 255.255.255.252 | 192.168.11.1 |
| OFFICE\_ROUTER | FE0/0 | 192.168.4.1 | 255.255.255.0 | 192.168.4.1 |
| OFFICE\_ROUTER | FE1/0 | 192.168.5.1 | 255.255.255.0 | 192.168.5.1 |
| OFFICE\_ROUTER | Se2/0 | 192.168.3.2 | 255.255.255.252 | 192.168.3.2 |

Przed rozpoczęciem szczegółowego opisu zabezpieczeń, istotne jest przedstawienie ogólnego planu adresacji i schematu sieci. Tabela adresacji zawiera pełną informację o przydzielonych adresach IP, podziałach na podsieci oraz zastosowanych VLANach. Dodatkowo, dołączamy graficzne przedstawienie sieci, ilustrujące rozmieszczenie poszczególnych urządzeń i ich połączeń. To wizualne ujęcie znacząco ułatwia zrozumienie skomplikowanej struktury i hierarchii naszej sieci.



Poniżej przedstawiamy szczegółowy przegląd głównych elementów projektu w kontekście zaimplementowanych zabezpieczeń:

* Konfiguracja Serwera DHCP:
  + Serwer został skonfigurowany serwerze 0(1)
  + Realizacja DHCP w różnych segmentach sieci umożliwiła centralizację zarządzania adresacją IP, co przyczynia się do efektywności administracyjnej i zmniejsza ryzyko konfliktów adresowych.
* VLANy:
  + Vlany zostały skonfigurowane w developer ruoterach
  + Implementacja VLANów znacząco podniosła poziom bezpieczeństwa poprzez izolowanie segmentów sieci, co ogranicza potencjalny zasięg ataków i ułatwia zarządzanie ruchem sieciowym.
* Standardowe oraz Rozszerzone Listy Dostępu ACL:
  + ACL’ki zostały skonfigurowane na głównych routerach (tj. developer router, office router i router 3)
  + Stosowanie list ACL pozwala na precyzyjną kontrolę dostępu do zasobów sieciowych, co jest kluczowe dla ochrony wrażliwych danych i zapobiegania nieautoryzowanemu dostępowi.
* Dostępy SSH:
  + Dostęp ssh został soknfigurowany administratorowi do routera 3
  + Konfiguracja SSH zapewnia bezpieczny, szyfrowany kanał do zdalnego zarządzania urządzeniami sieciowymi, co jest niezbędne w kontekście zapobiegania atakom typu man-in-the-middle.
* Zabezpieczenia przed Atakami MAC:
  + Zabezpieczenia zostały wprowadzone w routerach bezprzewodowych
  + Wdrożenie zabezpieczeń MAC jest istotne w kontekście ochrony sieci Wi-Fi przed nieautoryzowanym dostępem, co zapobiega potencjalnym atakom i naruszeniom bezpieczeństwa.
* Konfiguracja Syslogu:
  + Syslog monitoruje główne routery został ustawiony w serwerze w developers routerze
  + Użycie Syslogu umożliwia centralne zbieranie i analizę logów z różnych urządzeń sieciowych, co jest niezbędne do efektywnego monitorowania i reagowania na incydenty bezpieczeństwa.
* Konfiguracja AAA:
  + AAA skonfigurowane jest na routerach developerów oraz serwerze w tej sieci
  + Implementacja AAA zwiększa poziom bezpieczeństwa sieci, umożliwiając zarządzanie dostępem na podstawie autentykacji i autoryzacji użytkowników.
* Konfiguracja NTP:
  + NTP skonfigurowane jest na routerach developerów oraz serwerze w tej sieci
  + Synchronizacja czasu za pomocą NTP jest kluczowa dla utrzymania integralności logów systemowych i ułatwienia śledzenia zdarzeń w sieci.
* Dynamiczne Protokoły Routingu:
  + Protokoły te zostały skonfigurowane w całej sieci
  + Wykorzystanie EIGRP jako protokołu dynamicznego routingu zapewnia efektywną i stabilną komunikację w sieci, co jest ważne dla utrzymania ciągłości działania usług.
* Konfiguracja Poziomów Dostępowych na Urządzeniach Sieciowych:
  + Na wszystkich routerach jest podstawowy użytkownik „user” który ma 0 uprawnienia
  + Ograniczone poziomy dostępu na urządzeniach sieciowych minimalizują ryzyko nieautoryzowanych zmian w konfiguracji, co przyczynia się do wzrostu bezpieczeństwa ogólnego.
* Procedura Przywracania Obrazu Systemu Operacyjnego Urządzenia Sieciowego:
  + Konfiguracja przechowywana jest na serwerze obok routera 3 i i wykorzystujemy do tego usługę TFTP.
  + Procedura ta zapewnia możliwość szybkiego przywrócenia systemu w przypadku awarii, co jest istotne dla utrzymania ciągłości działania sieci.
* Ocena Potencjalnych Zagrożeń:
  + Przeprowadzona analiza zagrożeń pozwoliła na wdrożenie skutecznych środków prewencyjnych, co zwiększa ogólną odporność sieci na potencjalne ataki i incydenty.

Projekt ten stanowił nie tylko wyzwanie techniczne, ale również doskonałą okazję do praktycznego zastosowania i zrozumienia zaawansowanych koncepcji sieciowych. Udało nam się stworzyć infrastrukturę, która jest nie tylko funkcjonalna, ale również bezpieczna i przygotowana na przyszłe rozszerzenia i modyfikacje. Regularne przeglądy, aktualizacje i ciągłe doskonalenie systemów sieciowych będą umożliwiały zapewnienie ich niezawodności i bezpieczeństwa w obliczu ciągle ewoluujących zagrożeń w cyberprzestrzeni. Projekt ten udowodnił, że właściwe planowanie, wykonanie i zarządzanie są kluczowe dla sukcesu w dziedzinie sieci komputerowych.