

УДК 621.391

Зуєв Д.В.¹, Мороз Г.В.²

¹ студ. гр. РТ-912м НУ «Запорізька політехніка»

² старш. викл. НУ «Запорізька політехніка»

СИСТЕМА БЕЗПЕКИ ДЛЯ ЛОКАЛЬНОЇ МЕРЕЖІ КАФЕДРИ РТТ

Налаштування безпеки є невід'ємною частиною при плануванні комп'ютерної мережі для захисту від несанкціонованого доступу, крадіжки даних, атак, вірусів та інших загроз.

Налаштовуючи безпеку на мережевих пристроях можна запобігти несанкціонованому доступу до мережевих ресурсів, таких як сервери, роутери, комутатори або бази даних, що знаходяться на них. Наприклад, можна встановити паролі на доступ до пристрою, налаштувати обмеження доступу за IP-адресами або налаштувати VPN-з'єднання для захисту даних при віддаленому доступі до мережі. Також налаштування безпеки може допомогти у запобіганні атакам типу DDoS і DoS, які можуть призвести до відмови в обслуговуванні або погіршення продуктивності сервісу чи мережі. Різні механізми захисту, такі як міжмережні екрани (firewalls), маршрутизація трафіку та контроль доступу, можуть допомогти у запобіганні таким атакам.

Крім того, безпека на мережевих пристроях важлива для захисту конфіденційної інформації, такої як паролі, логіни, персональні дані та бізнес-дані. Налаштовуючи безпеку на мережних пристроях, можна захистити дані від витоку та використання в несумлінних цілях.

У запропонованій мережі кафедри РТТ (рис. 1) для забезпечення безпеки будуть використовуватися наступні технології та протоколи.

Для налаштування на усіх мережевих пристроях:

SSH котрий працює на порту 22 і підтримує різні методи аутентифікації, такі як пароль, відкритий ключ та інші. SNMPv3 забезпечує безпечну передачу керуючої інформації між пристроями. VLAN метод розбиття локальної мережі на логічні сегменти на рівні комутатора чи маршрутизатора. MACsec забезпечує шифрування трафіку між мережевими пристроями на каналному рівні. IEEE 802.1X забезпечує аутентифікацію користувачів при підключенні до мережі через комутатор. AAA забезпечує аутентифікацію користувачів, управління доступом та облік використання ресурсів.

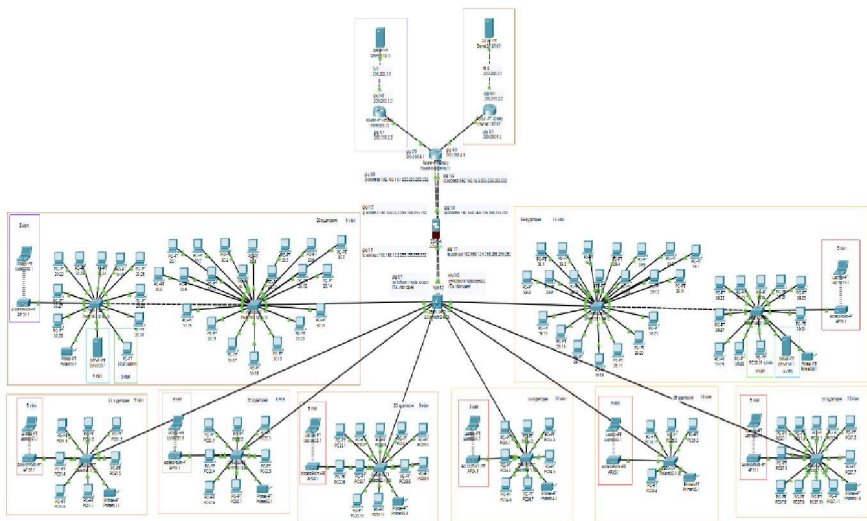


Рисунок 1 – Загальна схема мережі для кафедри РТТ

На міжмережевому екрані, пограничному маршрутизаторі та L3 комутаторі використовується протокол STP котрий забезпечує безпеку мережі, запобігаючи формуванню циклів у топології мережі. STP будує дерево, в якому один комутатор є корневим, а всі інші комутатори підключаються до нього.

Це дозволяє визначити кращий шлях для передачі даних і заблокувати непотрібні шляхи, які можуть призвести до зацикловання. ACL визначає правила доступу для трафіку, що проходить через пристрій. VPN забезпечує безпечне з'єднання між віддаленими мережами. IPsec шифрує трафік між пристроями у віртуальній приватній мережі (VPN). IP Source Guard – забезпечує контроль підроблених IP-адрес на мережевих портах комутатора. Та NAT забезпечує приховування IP-адрес внутрішньої мережі від зовнішньої мережі встановлена на пограничному маршрутизаторі. DHCP Snooping котрий забезпечує захист від атак DHCP встановлена на L3 комутаторі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cisco CCNA ICND2 200-101 [Електронний ресурс]
2. Cisco CCENT/CCNA ICND1 100-101 Cisco Press 800 East 96th Street Indianapolis, IN 46240 [Електронний ресурс]