

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ VPN ДЛЯ ПОБУДОВИ ЗАХИЩЕНОЇ СИСТЕМИ МАРШРУТИЗАЦІЇ ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ НА ОБЛАДНАННІ CISCO

*Наталенко П.П. к.т.н., доцент; Білий О.С., курсант
Інститут спеціального зв'язку та захисту інформації
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна*

Сучасна корпоративна мережа повинна надавати набір послуг, таких як електронна пошта, WWW, IP- телефонія, відео конференція. Якість виконання транспортних функцій мережею, забезпечуючих роботу цих телекомунікаційних служб, залежить від багатьох факторів і в першу чергу від правильно побудованої системи маршрутизації повідомлень в ній. Надійність доставки і затримка повідомлень напряму залежать від системи маршрутизації. Зловмисники, з метою внесення порушень в роботу мережі, в першу чергу, розрушають відлагоджену систему маршрутизації. Тому актуальною є задача планування ефективної системи маршрутизації і рішення задач по захисту її функціонування.

Від надійності функціонування системи маршрутизації в мережі залежить якісне обслуговування всіх видів трафіку, а саме: мови; даних; електронної пошти; відеоконференції і т.і.[1].

Загальні принципи побудови системи маршрутизації в корпоративних мережах, побудованих за технологією Інтернет

Корпоративні мережі в нашій державі великі за розміром, мають велику кількість маршрутизаторів, що ускладнює процес побудови таблиць маршрутизації (ТМ), і повинні забезпечити безпеку та при необхідності оперативну зміну маршрутів. Для динамічної маршрутизації, маршрутизатори повинні постійно обмінюватися маршрутною інформацією у відповідності до спеціальних протоколів маршрутизації .

В доповіді рекомендовано розділення областей відповідальності окремих маршрутизаторів і вводиться поняття автономної системи (Autonomous System – AS). Рекомендовано використовувати протоколи внутрішньої (в межах AS) маршрутизації IGP (Interior Gateway Protocol), а для зв'язку між AS – протоколами зовнішньої маршрутизації EGP (External Gateway Protocol) [2]. На користь такого вибору вказують:

- незалежність від обладнання;
- якісна реалізація в широкому колі телекомунікаційного обладнання;
 - наявність механізмів, дозволяючих ефективно протистояти виникаючим нестандартним ситуаціям з точки зору безпеки інформації;
- наявність широкого кола засобів управління потоками даних.

Аналіз проблем системи незахищеної маршрутизації і шляхів їх розв'язання

До основних проблем системи незахищеної маршрутизації корпоративної мережі відносять можливість протидії атакам на систему маршрутизації.

Серед цих атак можна виділити наступні [2]: створення „чорних дір„; перенаправлення мережевого трафіку; фабрикація адреси джерела трафіку; перехоплення, прослуховування мережевого трафіку і інші.

Метою вище поразованих атак на систему маршрутизації є створення спотвореного образу топології та отримання таємної інформації яка передається в корпоративній мережі.

Рекомендуємі напрямки розв'язання проблеми підвищення надійності функціонування системи маршрутизації.

Побудова захищеної системи

1. Формування між автономними системами захищених тунелів на основі використання технології VPN.

2. Захист файлів конфігурації маршрутизаторів корпоративної мережі. Для обмеження доступу та управління потоками даних між корпоративними мережами використовують фільтри, а саме [2]:

- ACL-списків доступу;
- використання протоколу маршрутизації EIGRP.

3. Обмеження обміну поновленнями між граничними маршрутизаторами.

4. Аутентифікація граничних маршрутизаторів.

Захист даних у VPN здійснюється в двох напрямках : криптування інформації, яка передається через тунель; аутентифікація та авторизація користувачів VPN.

В доповіді наведені конкретні приклади побудови захищеної системи маршрутизації корпоративної мережі і файли конфігурування мережевих пристроїв. Показано які характеристики вона забезпечить .

Література:

1. Наталенко П.П., Зембицький Б.С. Побудова системи маршрутизації корпоративних мереж.-Збірник наукових праць ВІПІ № 3, 2005 р. с. 69 – 72.
2. Уэнстрем М. Организация защиты сетей Cisco.: Пер. с англ.-М.: Вильямс, 2005. – 768 с.