ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

1

Харківський національний університет радіоелектроніки

Кафедра електронних обчислювальних машин

Метод організації захищеного сегмента корпоративної мережі на основі моделі Zero Trust

Кваліфікаційна робота
Перший (бакалаврський) рівень

Виконав:

здобувач групи КІУКІ-21-6
Любчик Владислав Олександрович

Керівник:

ас. кафедри ЕОМ
Чепурна Ірина Сергіївна

2

Мета роботи

Розробка методу організації захищеного сегмента комп'ютерної мережі на основі концепції Zero Trust.

Основне завдання роботи полягає в забезпеченні захищеного доступу до ресурсів корпоративної мережі на основі прав та привілеїв користувачів в умовах підвищених вимог до захисту від ризиків несанкціонованого доступу та витоку інформації.

3

Концепція Zero Trust

Не довіряй нікому за замовчуванням
Контроль на основі політик доступу
Принцип найменших привілеїв
Безперервний моніторинг та оцінка поведінки
Аутентифікація для кожного запиту

Схема основного принципу концепції архітектури Zero Trust

4

Архітектура Zero Trust

Схема реалізації принципів концепції Zero Trust

Тунелювання

5

Протокол	Переваги	Недоліки	Відповідність Zero Trust
IPsec	Висока продуктивність; підтримка апаратного прискорення	Складність конфігурації; обмеження в мобільних і динамічних мережах	потребує додаткових механізмів контролю доступу та автентифікації
SSH	Інтеграція автентифікації, шифрування та керування доступом на рівні сесії	не підтримує масштабування; потребує ручного адміністрування	придатний для точкових з'єднань, не підтримує динамічного керування доступом
WireGuard	Простота конфігурації; висока швидкість; сучасна криптографія	Відсутність підтримки TCP, сертифікатів, RADIUS, LDAP; обмежена масштабованість	відсутній вбудований механізм ролей та динамічного контролю
OpenVPN	Гнучкість; підтримка NAT, TCP, сертифікатів, LDAP/RADIUS, ролей та політик	складність налаштування та адміністрування;	підтримка багаторівневої автентифікації, контроль доступу

Управління ролями та привілеями користувачів на основі RBAC

6

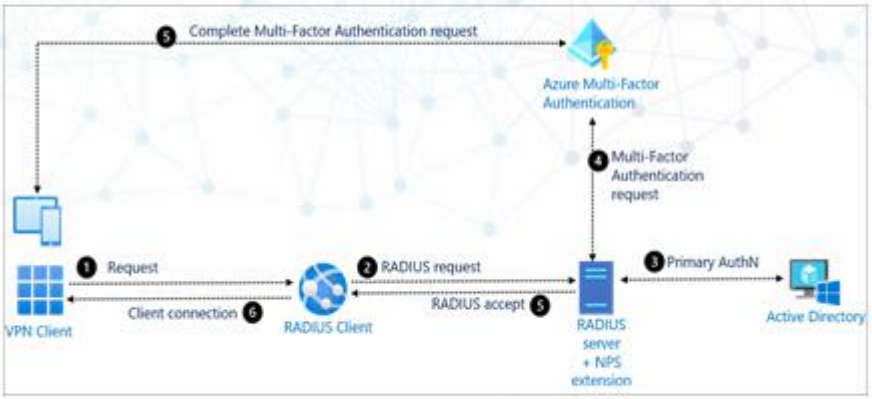


Схема автентифікації через RADIUS сервер

Метод побудови захищеного сегмента корпоративної мережі на основі моделі Zero Trust

7

Метод побудови захищеного сегмента комп'ютерної мережі на основі моделі Zero Trust

8

Коефіцієнт завантаження системи

$$\rho = \frac{\lambda}{\mu}, \quad (1)$$

Час перебування у системі

$$W = \frac{1}{\mu - \lambda}, \quad (2)$$

Кількість запитів у системі

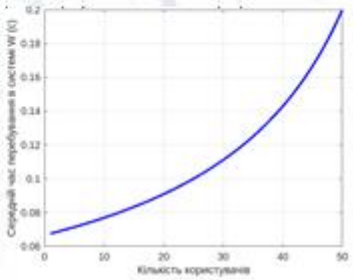
$$L = \frac{\lambda}{\mu - \lambda}, \quad (3)$$

Кількість запитів у черзі

$$L_q = \frac{\lambda^2}{\mu(\mu - \lambda)}, \quad (4)$$

Час очікування в черзі

$$W_q = \frac{\lambda}{\mu(\mu - \lambda)}, \quad (5)$$

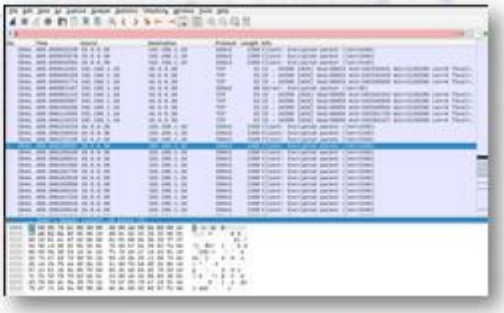


Графік залежності середньої затримки від кількості користувачів в системі

Показник	Аналітичне моделювання	Експериментальне моделювання
Коефіцієнт завантаження системи	0.67	0.9
Середня кількість запитів у системі	2.00	9.12
Середній час перебування в системі, с	0.2000	8.19
Середня кількість запитів у черзі	1.33	0.0676
Середній час очікування в черзі, с	0.1333	8.19

Тестування захищеного сегмента комп'ютерної мережі на основі моделі Zero Trust

9



Відмова в доступі до ресурсів користувача зі скомпрометованими обліковими даними

Візуалізація шифрованого потоку TCP-пакетів VPN-тунелю

Апробація результатів кваліфікаційної роботи

10

ІНСТИТУТ СИСТЕМ УПРАВЛІННЯ
МНО АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ
НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"
УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей п'ятнадцятої міжнародної науково-технічної конференції
24 – 25 квітня 2025 року
Том 3: секції 3, 4

Баку – Харків – Жилінa – 2025

МЕТОД ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО СЕГМЕНТА КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ ZERO TRUST

Любчик В.О., Чикулина І.С.
Харківський національний університет радіоелектроніки, Харків, України

Висновки

11

В кваліфікаційній роботі запропоновано метод організації захищеного сегмента мережі на основі концепції Zero Trust, який забезпечує доступ до ресурсів корпоративної мережі на основі прав та привілеїв користувачів.

На основі аналітичного та експериментального моделювання підтверджено ефективність запропонованої моделі в умовах підвищених вимог до безпеки. Запропонований підхід може бути рекомендований для використання в корпоративних комп'ютерних мережах для забезпечення підвищених вимог до конфіденційності та цілісності інформації.

ДОДАТОК Б

Тези доповіді

до XV Міжнародної науково–технічної конференції «Сучасні напрями розвитку інформаційно–комунікаційних технологій та засобів управління»

**ІНСТИТУТ СИСТЕМ УПРАВЛІННЯ
МНО АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"**

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ**

**НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"**

УНІВЕРСИТЕТ МІСТА ЖИЛІНА

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей п’ятнадцятої міжнародної науково-технічної конференції

24 – 25 квітня 2025 року

Том 3: секції 3, 4

Баку – Харків – Жиліна – 2025

МЕТОД ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО СЕГМЕНТА КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ ZERO TRUST

Любчик В.О., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасних корпоративних мережах, як у державному, так і в приватному секторі, значно зростають ризики, пов'язані з кіберзагрозами, витоком конфіденційної інформації та несанкціонованим доступом до конфіденційних даних. Традиційні підходи базуються на концепції периметрового захисту, проте вони втрачають актуальність в умовах зростаючої складності атак і широкого використання хмарних технологій. Збільшення кількості віддалених підключень, мобільних користувачів та оверлейних архітектур потребують новітніх підходів до управління доступом та контролю над мережними ресурсами. Імплементація методів і технологій, заснованих на концепції моделі нульової довіри (Zero Trust), яка ґрунтується на принципі «нікому не довіряти, завжди перевіряти», забезпечує високий рівень інформаційної безпеки та захисту користувацьких даних, особливо в умовах віддаленого доступу до корпоративних ресурсів [1]. Концепція передбачає, що всі запити на доступ, з внутрішньої мережі або ззовні, підлягають суворій автентифікації, авторизації та постійному моніторингу з метою мінімізації ризиків несанкціонованого доступу та компрометації інформаційних систем [2].

Метою роботи є організація захищеного сегмента корпоративної мережі, яка забезпечує динамічний контроль доступу до ресурсів мережі, забезпечуючи високий рівень захисту даних, мінімізуючи ризики несанкціонованого доступу та витоку інформації.

Віртуальні приватні мережі (VPN) забезпечують захищений та шифрований канал зв'язку між віддаленими користувачами та корпоративними ресурсами [3]. Використання механізмів шифрування та протоколів тунелювання гарантують конфіденційність переданих даних та забезпечують цілісність інформації під час передачі інформації, що є ключовим аспектом реалізації моделі нульової довіри. Інтеграція VPN з механізмами автентифікації та контролю доступу сприяє впровадженню принципів Zero Trust Architecture (ZTA) в сучасних IT-екосистемах. В рамках цієї моделі усі запити на доступ перевіряються незалежно від їхнього походження, що дозволяє мінімізувати ризики компрометації даних та забезпечити високий рівень безпеки корпоративної інфраструктури.

В роботі досліджено основні принципи архітектури Zero Trust, методи сегментації мережі та механізми реалізації політик доступу, що сприяють мінімізації ризиків компрометації інформаційної системи. Запропонований підхід передбачає створення захищеного каналу зв'язку за допомогою VPN, централізоване управління автентифікацією, а також впровадження моделі рольового контролю доступу (RBAC), що забезпечує принцип мінімальних привілеїв при доступі до корпоративних ресурсів. Проведене моделювання

функціонування захищеного сегмента корпоративної мережі демонструє високий рівень конфіденційності, цілісності та доступності даних, а також ефективність автентифікації та контролю доступу на основі ролей і привілеїв користувачів. Подальші дослідження в цьому напрямі спрямовані на оптимізацію використання обчислювальних ресурсів в умовах підвищених вимог до безпеки та захисту даних, зменшення затримок при доступі до ресурсів, що сприяє підвищенню якості обслуговування користувачів та зниженню навантаження на корпоративну інфраструктуру.

Список літератури

1. New Microsoft guidance for the CISA Zero Trust Maturity Model | Microsoft Security Blog. Microsoft Security Blog. URL: https://www.microsoft.com/

2. Tsai M., Lee S., Shieh S. W. Strategy for implementing of zero trust architecture //IEEE Transactions on Reliability. – 2024. – Т. 73. – №. 1. – С. 93-100.

3. Ткачов В. М., Чепурна І. С., Фесенко Т. Г. Метод мультирівневого vpn-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі // Вісник Херсонського НТУ. – 2024. – №. 3 (90). – С. 299-308.

МЕТОД ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ВЕБЗАСТОСУНКІВ З ВИКОРИСТАННЯМ WAF

Корякіна А.М., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Активне впровадження вебдодатків сприяє розвитку бізнес-процесів та покращенню взаємодії з користувачами, забезпечуючи зручний доступ до послуг та інформаційних ресурсів. Водночас зі зростанням кількості вебресурсів пропорційно зростає масштаб і складність кібератак, спрямованих на несанкціонований доступ до даних користувачів та компрометацію інформаційних систем [1]. Для ефективного захисту вебдодатків та мінімізації ризиків компрометації даних використовуються вебекрани захисту додатків (WAF). Однією з основних переваг використання WAF є його здатність динамічно адаптуватися до змін у трафіку, забезпечуючи гнучкість у виявленні та блокуванні атак [2]. Однак, складність налаштування правил фільтрації трафіку може призвести до збільшення затримок при обробці запитів, що збільшує навантаження на вебсервери та сповільняє швидкість обробки запитів, особливо в умовах високого трафіку або складних правил фільтрації.

Метою доповіді є розробка методу підвищення продуктивності вебдодатків шляхом інтеграції WAF з механізмом балансування навантаження.

У доповіді представлено огляд методів і технологій оптимізації продуктивності вебдодатків, зокрема через використання проксі-серверів, організації кластерної інфраструктури для обслуговування запитів, в поєднанні з застосуванням правил фільтрації трафіку для зниження навантаження на основні сервери та оптимізації обробки даних.

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 4)

ДОДАТОК В

Лістинг коду розрахунку аналітичного моделювання

```
% Параметри СМО
mu = 15;     % Інтенсивність обслуговування (запитів/с)
lambda = 10; % Інтенсивність вхідного потоку (запитів/с)

% Коефіцієнт завантаження
rho = lambda / mu;

% Основні характеристики системи M/M/1
L = rho / (1 - rho);  % Середня кількість заявок у системі
Lq = rho^2 / (1 - rho); % Середня кількість заявок у черзі
W = 1 / (mu - lambda); % Середній час перебування в системі
Wq = rho / (mu - lambda); % Середній час очікування в черзі

% Вивід основних характеристик
fprintf('--- Основні показники системи M/M/1 ---\n');
fprintf('Інтенсивність вхідного потоку λ = %.2f зап/с\n',
lambda);
fprintf('Інтенсивність обслуговування μ = %.2f зап/с\n', mu);
fprintf('Коефіцієнт завантаження ρ = %.2f\n', rho);
fprintf('Середня кількість заявок у системі L = %.2f\n', L);
fprintf('Середня кількість заявок у черзі Lq = %.2f\n', Lq);
fprintf('Середній час перебування в системі W = %.4f с\n', W);
fprintf('Середній час очікування в черзі Wq = %.4f с\n', Wq);

% Динамічне моделювання залежності затримки від кількості
користувачів
users = 1:50;    % Кількість користувачів
lambda_per_user = 0.2; % Кожен користувач генерує 0.2 запитів/с
lambda_dynamic = users * lambda_per_user;

% Фільтрація стійких значень (lambda < mu)
valid_idx = lambda_dynamic < mu;
lambda_valid = lambda_dynamic(valid_idx);
users_valid = users(valid_idx);

% Повторний розрахунок показників для графіка
rho_dynamic = lambda_valid ./ mu;
W_dynamic = 1 ./ (mu - lambda_valid);
Wq_dynamic = rho_dynamic ./ (mu - lambda_valid);
% Побудова графіка
figure;
plot(users_valid, W_dynamic, 'b-', 'LineWidth', 2);
xlabel('Кількість користувачів');
ylabel('Середній час перебування в системі W (с)');
grid on;
```