

МЕТОДИКА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ ОБЛАДНАННЯ JUNIPER СЕРІЇ SRX

Валуйський С.В., П'янтковська Н.О.

Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна

E-mail: piantkosha@gmail.com

Providing of security in enterprise network based on Juniper equipment the SRX series

This paper describes method to improve security on systems that were originally designed as stand-alone or where security issues were ignored. It's provides an example for configuring next-generation security features on an SRX Series device in an enterprise network.

Значимість проблеми захисту інформації в сучасному світі є признаною, і підтвердженню цьому є понесені корпорацією збитки через недостатню захищеність інформації. При створенні інформаційної інфраструктури корпоративної автоматизованої системи (АС) на базі сучасних комп'ютерних мереж неминує виникати питання про захищеність цієї інфраструктури від загроз безпеки інформації. В даний час як мережі, так і вибір постачальника для їх побудови, набули великого значення. Багато постачальників (Cisco, Juniper, ALu та ін.) пропонують мережеві рішення для широкого спектру задач, але перед замовником постає питання вибору оптимального рішення для забезпечення достатнього рівня безпеки при мінімальних затратах, а також розробки методичного забезпечення для оперативного налаштування і забезпечення захисту мережі [1].

Дана робота розглядає рішення із використанням пристроїв Juniper Networks серії SRX, що повним набором інструментів забезпечують безпеку критично важливих мережевих ресурсів, які знаходяться в корпоративній власності. Рішення включає в себе брандмауер, систему запобігання вторгнень (IPS), інструмент уніфікованого управління погрозами (UTM функцій), AppSecure.

В основі концепції побудови захищених корпоративних мереж лежить наступна ідея: налаштування функцій безпеки базової топології мережі середнього рівня на серії пристроїв SRX (рис. 1). Ця топологія була обрана, щоб показати загальний і гнучкий приклад того, як методика може бути модифікована для застосування в різних корпоративних мережах і фізичних об'єктах [2]. У цій топології визначені наступні фізичні об'єкти:

Філія 1: кожен користувач буде завірений ідентифікацією брандмауера.

Філія 2: користувачі з кожного підрозділу будуть проходити перевірку автентичності за допомогою Unified Access Controller (UAC) .

Головне управління (ГУ): центр обробки даних в режимі реального часу серверів (FTP, HTTP, MySQL, Syslog) та доступність до серверів центрів обробки даних за допомогою динамічної VPN.

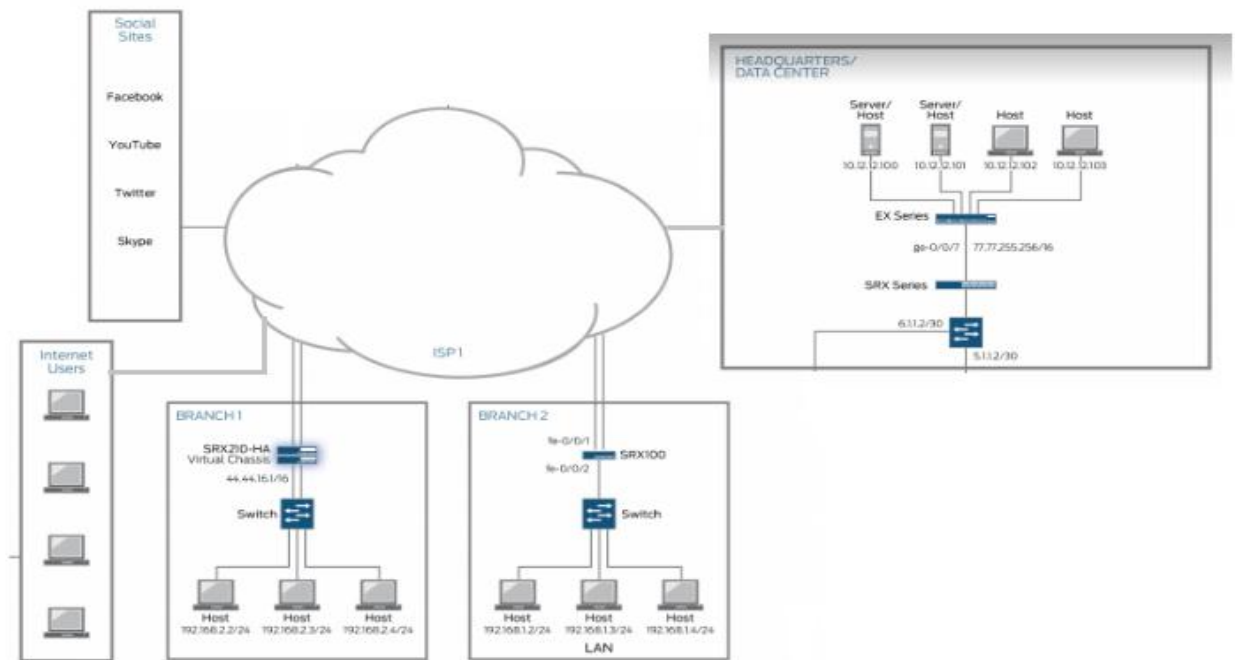


Рис. 1. Топологія корпоративної мережі.

В якості першого кроку, забезпечуємо зв'язок між хостами (ПК) в зонах (філії 1 і 2) та серверами зони ГУ. В таблиці 2 наводяться параметри конфігурації хостів, які налаштовуються на гілках 1 і 2 та головному управлінні.

Таблиця 2. Параметри конфігурації хостів.

Хост	IP адреса	Таблиця маршрутизації	Зона	Хост	IP адреса	Таблиця маршрутизації	Зона
Філія 1				Філія 2			
branch-1-user-1	192.168.2.2/24	address-book-branch-1-users	Branch1-Zone	branch-2-user-1	192.168.1.2/24	address-book-branch-2-users	Branch2-Zone
branch-1-user-2	192.168.2.3/24			branch-2-user-2	192.168.1.3/24		
branch-1-user-3	192.168.2.4/24			branch-2-user-3	192.168.1.4/24		

Політика безпеки контролює потік трафіку з однієї зони в іншу, визначивши види трафіку.

Таблиця 3. Налаштування параметрів політики безпеки.

Хост	Мета	Ім'я політики	Зона відправлення	Зона призначення
Гілка 1	Доступ до серверів в ГУ (e-mail сервер, FTP сервер та HTTP сервер)	Branch1-policy	Branch1-Zone	HQ-Zone
	Доступ в Інтернет	permit-traffic-branch-1-to-internet	Branch1-Zone	надійний
Гілка 2	Доступ до серверів в ГУ (e-mail сервер, FTP сервер та HTTP сервер)	Branch2-policy	Branch2-Zone	HQ-Zone
	Доступ в Інтернет	permit-traffic-branch-2-to-internet	Branch2-Zone	надійний

Практично задані параметри крок за кроком забезпечують процедуру, необхідну для налаштування мережі з захищеними даними:

- конфігурація адресних об'єктів, зон безпеки і політик безпеки;
- конфігурація AppSecure модулів;
- конфігурація UTM і шаблонів IDP;
- ідентифікація трафіку на різних рівнях мережі з використанням AppID;
- конфігурація SSL проксі для безпечної передачі даних.

В результаті практичних досліджень з'являється конфігурація, яка працює належним чином і в ній існують всі механізми для боротьби за ресурси. Наприклад, конфігурація фільтрації вмісту:

```
user@host> show security utm content-  
filtering statistics  
Content-filtering-statistic: Blocked  
Base on command list: 1  
Base on mime list: 0  
Base on extension list: 3  
ActiveX plugin: 0  
Java applet: 0  
EXE files: 0  
ZIP files: 0  
HTTP cookie: 0
```

Таким чином, вихідне повідомлення відображає статистику фільтрації контенту UTM та статистику безпеки UTM функцій від анти-спаму.

Отже, у даній роботі розглянуто комплексне рішення, яке поєднує у собі стратегію захисту корпоративної безпеки, перешкоджаючи всім видам зовнішніх та внутрішніх атак. Таке рішення дозволяє застосовувати дану топологію з використанням обладнання Juniper серії SRX. Зазначений вище алгоритм налаштування системи дає якісні показники у адаптації мережі щодо ефективного плану забезпечення безпеки корпоративної мережі.

Література

1. JNCIS-SEC Study Guide—Part 2 – 1194 North Mathilda Avenue Sunnyvale: Worldwide Education Services, 2012. – 211 с.
2. Woodberg B. Juniper SRX Series / B. Woodberg, R. Cameron. – 1005 Gravenstein Highway North, Sebastopol: O'Reilly Media, Inc, 2013. – 1020 с. – (Juniper Network).