УДК 004.77

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ ЗАХИСТУ МЕРЕЖІ – CISCO ASA

Орест Полотай, Владислав Баденко, Валерія Балацька

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м.Львів

Описано основні властивості ASA, яка використовується компанією Cisco Systems в серії міжмережевих екранів

Ключові слова: захист комп'ютерних мереж, міжмережевий екран, Cisco ASA

Describes the main properties of ASA, which is used by Cisco Systems in a series of firewalls.

Keywords: protection of computer networks, firewall, Cisco ASA

Виклики безпеки, з якими стикаються сучасні компанії, зводяться до того, щоб розглянути всі можливі рішення і вибрати правильну комбінацію для захисту комп'ютерно\ мережі. Сьогодні доступно багато технологій і відповідних інструментів безпеки. Складність впровадження мережевої безпеки полягає не у відсутності відповідної технології безпеки, а у виборі рішення, яке найкраще відповідає вимогам мережі та бізнесу, а також у мінімізації витрат на підтримку та обслуговування інструментів безпеки, пропонованих кожним постачальником. Серед великої кількості обладнання, яке призначене для організації захисту комп'ютерних мереж, особливої уваги заслуговують пристрої адаптивного захисту Cisco ASA Series (рис. 1).

Обладнання Cisco ASA Series являє собою прості у розгортанні рішення, що інтегрують сервіси міжмережевого екрану, системи запобігання вторгненням (IPS), VPN з підтримкою SSL та IPSec, безпеки уніфікованих комунікацій (передача голосових відеоданих) та безпеки контенту в гнучке сімейство модульних продуктів. Розроблені в якості основного компонента мережі Cisco, що самозахищається, пристрої Cisco ASA Series надають інтелектуальний захист від загроз і послуги безпечних комунікацій, які зупиняють поширення атак перш, ніж вони зможуть вплинути на цілісність бізнесу. Пристрої Cisco ASA Series призначені для захисту мереж усіх масштабів і дозволяють організаціям скоротити загальні витрати на розгортання та експлуатацію одночасно забезпечуючи комплексну багаторівневу безпеку.

Рисунок 1 – Пристрій захисту Cisco ASA Series

Серія ASA базується на потужних функціях безпеки, які можна знайти в сімействі продуктів Cisco, включаючи міжмережевий екран PIX 500, датчик IDS 4200 і концентратор VPN 3000 Серія Cisco ASA пропонує адаптивний захист від загроз і разом відомі як Adaptive Threat Defence. Вона включає в себе технології Anti-X, Application Security і Network Containment and Control для забезпечення комплексного і повного захисту критично важливих ресурсів

підприємства від широкого спектру зловживань. Один пристрій з вбудованою підсистемою безпеки і кореляції подій забезпечує захист мережі від багатьох невідомих загроз (комп'ютерних черв'яків і антивірусів), шпигунських і рекламних програм, інструментів аналізу трафіку, виявлення хакерської активності і запобігання вторгненням, запобігання атакам типу "відмова в обслуговуванні" (DoS). Обладнання захисту ASA – забезпечує надійний захист корпоративних мереж за допомогою контролю стану з'єднань та демонструє високу продуктивність. Він пропонує широкі можливості захисту, повністю приховуючи архітектуру внутрішньої мережі від зовнішнього спостерігача та діє як “прикордонник” між корпоративною мережею та Інтернет, виконуючи функції контролю.

Пристрої захисту ASA мають такі особливості:

• Вбудована операційна система. Cisco ASA працює під керуванням вбудованої захищеної операційної системи реального часу, яка не залежить від проблем захисту UNIX або Windows. Операційна система ASA спеціально була посилена з погляду захисту від мережевих атак. Вона розроблялася з метою захисту.

• Алгоритм ASA (Adaptive Security Algorithm). Алгоритм ASA записує характеристики з'єднань, зберігаючи цю інформацію в таблиці і використовуючи її для перевірки вихідних і вхідних пакетів, щоб переконатися, що стан сеансу залишається таким самим, як і при відкритті з'єднання. Поки змін не виявляється, трафік пропускається без затримки. При виявленні якоїсь невідповідності пересилання даних припиняється.

Переваги алгоритму ASA:

• Жоден з пакетів, у яких інформація про з'єднання та стан не відповідає даним таблиці алгоритму ASA, не зможе пройти через пристрій захисту ASA.

• Дозволяються усі вихідні з'єднання та стани, крім тих, що спеціально заборонені вихідними списками доступу. Вихідним називаються з'єднання чи стан, у якому ініціатор чи клієнт має інтерфейс із вищим рівнем безпеки, ніж адресат чи сервер. Внутрішній інтерфейс має найвищий рівень безпеки, а зовнішній – найнижчий. Для додаткових інтерфейсів можуть визначатись рівні безпеки між рівнями внутрішнього та зовнішнього інтерфейсів.

• Вхідні з'єднання та стани забороняються, якщо вони спеціально не дозволені каналами. Вхідним називається з'єднання чи стан, у якому ініціатор чи клієнт має інтерфейс із нижчим рівнем безпеки, ніж адресат чи сервер. Кожна трансляція адрес дозволяє безліч винятків, що дозволяє дозволити доступ з будь-якої машини, з будь-якої мережі або з будь-якого хоста в мережі Інтернет до хоста, заданого трансляцією.

• Усі спроби обійти зазначені правила відкидаються, і серверу syslog надсилається відповідне повідомлення.

• Відкидаються всі пакети ICMP, крім тих, які спеціально дозволені командою conduit permit icmp або access-list.

Отже, для забезпечення ефективного захисту комп’ютерних мереж необхідно використовувати сучасні технології захисту, серед яких варто виділити обладнання захисту Cisco ASA.

Література

1. Полотай О.І., Тлумак О. Вибір обладнання Cisco для розгортання корпоративної VPN-мережі. Зб. тез. III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 64–66.

2. Міжмережевий екран: що це таке і для чого він потрібен (texnogid.biz.ua) Веб сайт Техногід. [Електронний ресурс]: – режим доступу: https://texnogid.biz.ua/wi-fi/bezpeka/mizhmerezhevyj-ekran.html

3. Балацька В.С., Полотай О.І., Ящук В.І. Вразливість комп’ютерної мережі як проблема закладів вищої освіти. Зб. тез доп. VI Міжнар. наук.-практ. конф. “Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи”. (м. Львів, 04 листопада 2021 р.). Львів : ЛДУБЖД, 2021