Впровадження безпеки на підприємствах з Zero Trust Security

Aruba ClearPass та інші рішення від виробника забезпечують контроль пристроїв і доступ на основі ролей і політик, захищають від зовнішніх та внутрішніх загроз і звільняють IT-персонал від марудної роботи.

Сучасна реальність змінює уявлення про контроль доступу. Гібридні робочі місця та периферійні обчислення руйнують традиційний IT-периметр. Мета організацій у даному контексті — забезпечити доступ у будь-який час і в будь-якому місці, не жертвуючи при цьому безпекою, зберігаючи видимість та контроль без впливу на якість обслуговування користувачів. Це починається з ідентифікації всіх пристроїв, що підключаються до мережі, їх автентифікації та авторизації, а також впровадження надійної політики в мережі.

Бачити, хто і що підключається до мережі, — це перший крок до захисту підприємства. Разом з тим сучасна система безпеки повинна реагувати на атаки і захищати підприємство від загроз у режимі реального часу.

Підготовка системи безпеки організації до будь-яких викликів

Профілювання — це визначення типів клієнтів, їх кількості, місць, звідки вони підключаються, операційних систем, які підтримуються; все це є основою видимості (**рис. 1**). Для багатьох спеціальних пристроїв — наприклад, у лікарні або на заводі, — розуміння фактичної поведінки пристрою є єдиним способом його точної ідентифікації. Постійна видимість парку пристроїв у масштабах підприємства, потенційних порушень безпеки, а також того, які елементи з'являються і зникають у заданий період часу створює умови, необхідні для захисту кінцевих точок мережі.

Організації повинні швидко адаптуватися до стрімкого розвитку сучасних пристроїв незалежно від їхніх типів та способів використання. Необхідно забезпечити автоматизоване реагування за допомогою динамічного контролю політик та усунення загроз у режимі реального часу, що поширюється й на сторонні системи. Готовність до незвичної поведінки в будь-який момент вимагає уніфікованого підходу, який дозволяє блокувати трафік і змінювати статус з'єднання пристрою.

Видимість по всій мережі

Безпека починається з видимості всіх пристроїв: ви не можете захистити те,

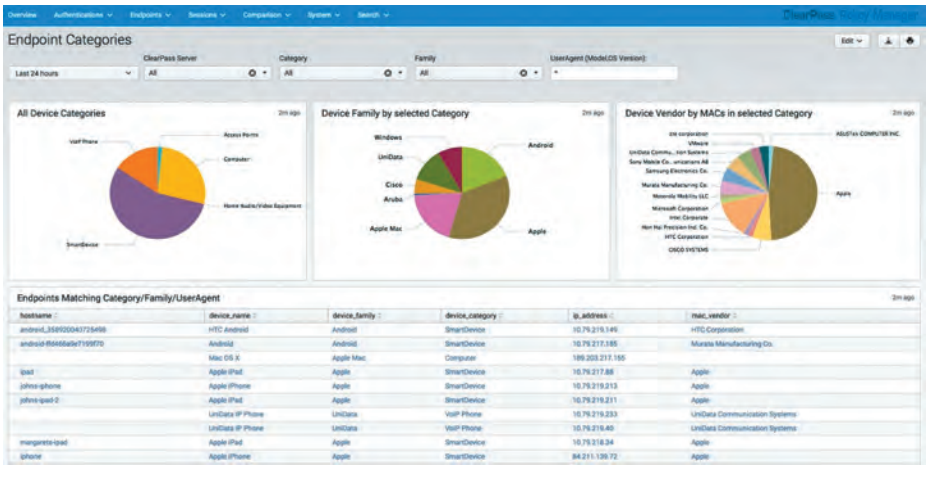


Рис. 1. Видимість підключених пристроїв у системі ClearPass Policy Manager

чого не бачите. Aruba пропонує на вибір хмарні та локальні продукти. Client Insights — це хмарне рішення для ідентифікації та профілювання клієнтів на основі штучного інтелекту, яке постачається разом з системою управління Aruba Central і не потребує встановлення додаткових колекторів або host-агентів. ClearPass Device Insight — це локальне рішення для виявлення та профілювання пристроїв, яке також працює зі сторонньою інфраструктурою.

І Client Insights, і ClearPass Device Insight значно розширюють можливості виявлення та профілювання, що створює умови для ідентифікації широкого спектра пристроїв у різних середовищах. Це досягається завдяки поєднанню глибокого аналізу пакетів (DPI), розширеного машинного навчання і краудсорсингу відбитків пристроїв.

Доступ на основі ролей і застосування політик

Застосування політик на основі шаблонів дозволяє IT-спеціалістам створювати політики для дротових та бездротових пристроїв з урахуванням контексту, а саме: типів пристроїв, даних системи управління мобільними/корпоративними пристроями (MDM/EMM), статусу сертифікатів, місцезнаходження, дня тижня тощо.

Незалежно від того, у який спосіб пристрої підключаються, інструмент Aruba Dynamic Segmentation автоматично застосовує до них узгоджені політики для дротових і бездротових мереж, надаючи доступ з найменшими привілеями до IT-ресурсів шляхом сегментації трафіку на основі ідентифікаційних даних і пов'язаних з ними дозволів. Це фундаментальна концепція системи Zero Trust, де довіра ґрунтується на ролях і політиках, а не на тому, де і як підключаються користувачі або кінцеві клієнти. Динамічна сегментація уніфікує доступ у дротових, бездротових і глобальних мережах на основі ролей і застосування політик з централізованим визначенням цих політик і вибором моделі застосування — централізованої або розподіленої — на основі загальної мережевої архітектури.

Надійна мережева політика з ClearPass Manager

ClearPass Policy Manager (CPPM) забезпечує автентифікацію, авторизацію та централізоване визначення політик, які слідують за користувачем по всій мережі та застосовуються однаково для бездротових, дротових і VPN-з'єднань (**рис. 2**). Якщо користувач переходить на невідомий пристрій або в незахищену мережу, політика автоматично змінить права доступу.

Конфігурування мережі та впровадження політик з Aruba Central NetConductor

Aruba Central NetConductor — це рішення нового покоління, призначене для автоматизації, швидкого розгортання й захисту складних, глобально розподілених корпоративних мереж, а також управління ними. Для мереж, якими керує Aruba Central, NetConductor пропонує хмарні сервіси безпеки, які забезпечують централізоване управління політиками та конфігурацією мережі за допомогою простого бізнес-інтерфейсу та робочих процесів. Для спрощення впровадження політик NetConductor використовує розподілені накладені мережі EVPN/VXLAN. ClearPass доповнює Aruba Central NetConductor, надаючи послуги AAA (автентифікація, авторизація та аудит) і забезпечуючи як RADIUS, так і інші підходи для належної ідентифікації суб'єктів та присвоєння їм ролей, які визначають привілеї доступу.

Безпека при використанні дротового зв'язку

ClearPass OnConnect — це вбудована функція, яка дає змогу організаціям блокувати тисячі дротових портів, використовуючи не-AAA-захист. Конфігурувати пристрій не потрібно, достатньо ввести один рядок у командному рядку комутатора. Також для дротових і бездротових підключень підтримуються стандартні методи AAA/802.1X. Це забезпечує послідовне застосування політик і наскрізний підхід, який виключає ізольоване застосування AAA, NAC і політик, на що не спроможні відповідні спеціалізовані продукти. На відміну від застарілих рішень, ClearPass дозволяє використовувати в рамках однієї служби політики декілька сховищ ідентифікаційних даних (Microsoft Active Directory, LDAP-сумісні каталоги, ODBC-сумісні бази даних SQL, сервери токенів, внутрішні бази даних).

Налаштування пристроїв без участі IT-спеціалістів

BYOD — це концепція, згідно з якою співробітникам дозволено або рекомендується використовувати особисті мобільні пристрої. Проте їх додавання до мережі здатне викликати проблеми з безпекою, а управління цим процесом може створювати навантаження на IT-ресурси та службу підтримки підприємства. ClearPass Onboard дозволяє самим користувачам безпечно налаштовувати пристрої для використання в захищених мережах. Понад те, використання сертифікатів пристроїв, що відслідковуються системою доступу, позбавляє користувачів

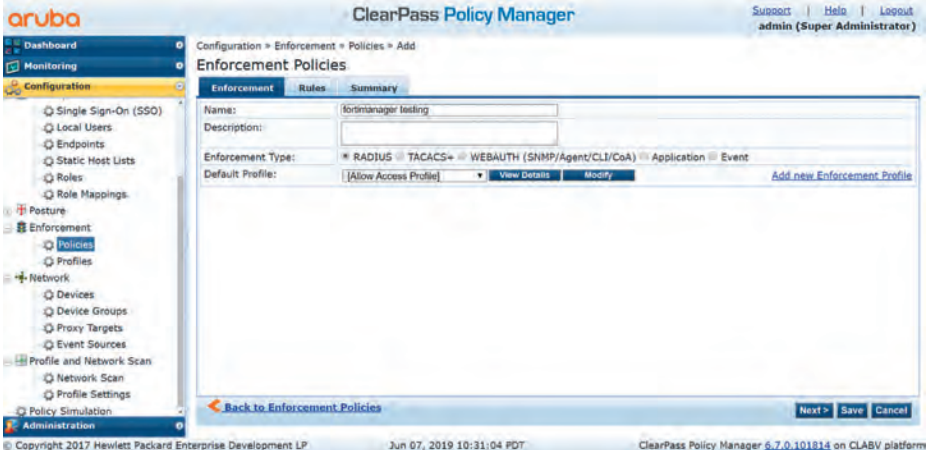


Рис. 2. Керування політиками доступу в ClearPass Policy Manager

необхідності протягом дня щоразу вводити облікові дані для входу. За допомогою ClearPass Onboard IT-команда визначає, хто може використовувати пристрої на своїх робочих місцях, які саме пристрої і скільки їх припадає на одну особу. Вбудований центр сертифікації, що відіграє роль внутрішньої інфраструктури відкритих ключів (PKI), дає змогу фахівцям швидше обслуговувати персональні пристрої і дозволяє розвантажити IT-персонал.

Простий і швидкий доступ для співробітників та гостей

Але BYOD — це не лише про пристрої співробітників. Це стосується будь-якого відвідувача, чиє обладнання потребує доступу до дротової чи бездротової мережі. IT-відділу потрібен простий інструмент, що спрямовує пристрій на корпоративний портал, автоматизує надання облікових даних для доступу, а також реалізує функції безпеки, які відокремлюють корпоративний трафік. Зручно автоматизовувати налаштування пристроїв для безпечного BYOD можна також за допомогою ClearPass Onboard.

Інструмент ClearPass Guest дозволяє співробітникам, адміністраторам, координаторам заходів та іншим працівникам, які не є IT-фахівцями, легко та ефективно створювати тимчасові облікові записи доступу до мережі для будь-якої кількості гостей на день. Кешування MAC-адрес також гарантує, що гості можуть легко підключатися протягом дня без необхідності щоразу вводити облікові дані на гостьовому порталі. Самостійна реєстрація гостей звільняє працівників від цієї роботи і дозволяє відвідувачам створювати власні акаунти. Облікові дані для входу надаються у вигляді друкованих бейджів, SMS-повідомлень або електронною поштою. Вони можуть зберігатися в ClearPass протягом заздалегідь визначеного періоду і можуть бути налаштовані на автоматичне завершення терміну дії через певний час.

Коли дозвіл залежить від стану пристрою

Під час процесу авторизації буває потрібно оцінити стан певних пристроїв, аби переконатися, що вони відповідають корпоративним політикам антивірусного, антишпигунського та фаєрвольного захисту. Автоматизація цього процесу передбачає виконання антивірусної перевірки перед підключенням до корпоративної мережі. ClearPass OnGuard має вбудовані функції, які оцінюють стан пристрою, керуючись правилами усунення вразливостей для широкого діапазону операційних систем і версій комп'ютерів. Незалежно від того, працює ClearPass у безагентному виконанні чи використовує постійні або тимчасові клієнти, він може централізовано ідентифікувати сумісні кінцеві точки в бездротових, дротових і VPN-інфраструктурах. Приклади розширених перевірок стану, які забезпечують додатковий захист:

- обробка P2P-застосунків, служб і ключів реєстру;
- визначення того, чи дозволені USB-накопичувачі або примірники віртуальних машин;
- керування використанням мережевих інтерфейсів і шифруванням дисків.

Отримайте більше від сторонніх рішень

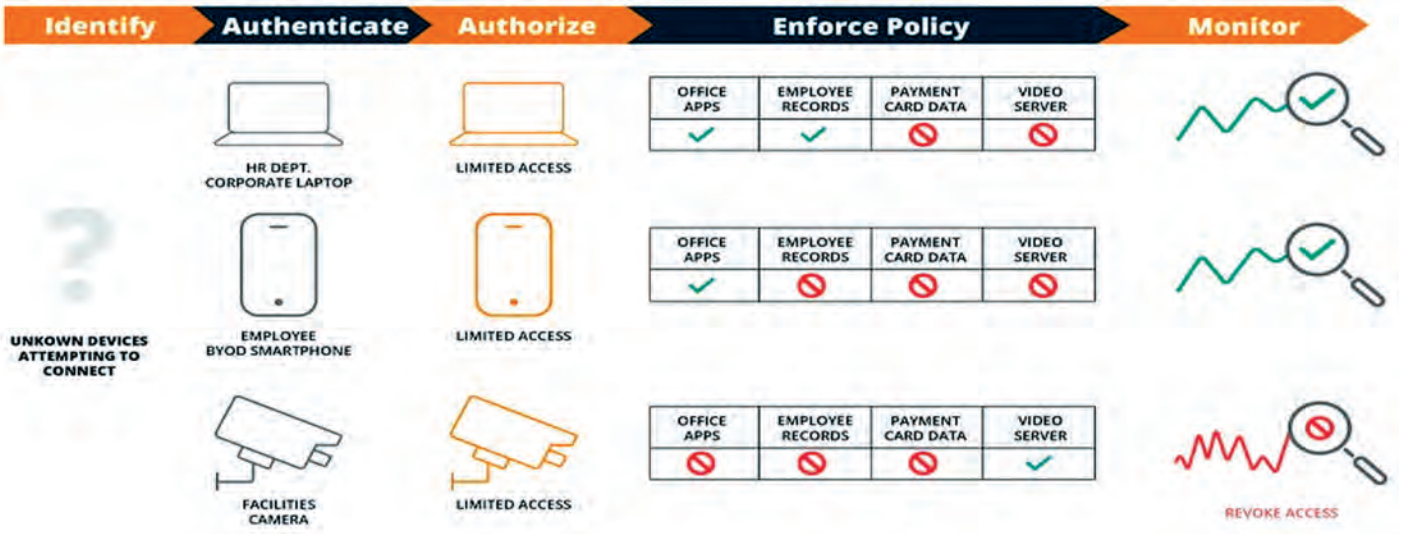
Останнім елементом безпечної інфраструктури є здатність реагувати на дані про атаки, отримані від рішень інших виробників систем безпеки. Aruba 360 Security Exchange — це «найкраща у своєму роді» екосистема, яка дозволяє автоматизувати усунення загроз та покращити сервіс за допомогою популярних сторонніх рішень, таких як мережеві екрани, MDM/EMM, засоби багатофакторної автентифікації (MFA), системи реєстрації відвідувачів та інструменти SIEM. Використання контекстної аналітики, включеної в ClearPass, дозволяє організаціям забезпечити безпеку і прозорість на рівні пристроїв і доступу до мережі, перевірку трафіку і захист від загроз. Використовуючи загальномовний (REST) API, syslog-повідомлення та вбудований репозиторій ClearPass Exchange, автоматизовані робочі процеси та рішення допомагають спростити завдання з захисту підприємства, тож нудне ручне конфігурування більше не потрібне. А для швидшої інтеграції з ClearPass Extensions партнери можуть завантажити розширення, яке дозволяє надавати нові послуги спільним клієнтам в режимі реального часу.

Завдяки ClearPass Exchange у мережі доступні такі дії:

- на основі даних від MDM/EMM, таких як статус розблокування (джейлбрейку) пристрою, можна ухвалити рішення, чи може він підключатися до мережі;
- мережеві екрани можуть з великою точністю застосовувати політики, засновані на атрибутах користувачів, груп і конкретних пристроїв, і через ClearPass впливати на пристрій, який демонструє некоректну поведінку;
- інструменти SIEM можна налаштувати на зберігання даних автентифікації для всіх підключених пристроїв;
- користувачам можна запропонувати використовувати багатофакторну автентифікацію для підтвердження своєї особи при підключенні до мереж і ресурсів. Мережеві події можуть також спонукати фаєрволи, SIEM та інші інструменти інформувати ClearPass про необхідність вжиття заходів щодо пристрою. Наприклад, якщо користувач кілька разів не пройшов мережеву автентифікацію, ClearPass може надіслати повідомлення безпосередньо на пристрій або заборонити йому доступ до мережі.

Безпечний доступ до робочих програм звідусіль

Вхід до робочих програм протягом дня має бути швидким і простим. Саме тому ClearPass підтримує як єдиний вхід (Single Sign-On), так і функцію автоматичного входу ClearPass Auto Sign-On. На відміну від першого варіанту, який передбачає, що користувач повинен один раз здійснити вхід у програми, функція автоматичного входу надає користувачам доступ до корпоративних мобільних застосунків, використовуючи дійсний мережевий логін. Потрібно лише мати на пристрої цей логін або актуальний сертифікат. ClearPass також можна використовувати в ролі постачальника ідентифікаційних даних (IdP) або послуг (SP) там, де використовується єдиний вхід.



ClearPass забезпечує захист та ефективність для SD-Branch

Якщо підприємство має десятки, сотні або навіть тисячі окремих філій, які потрібно налаштувати, захистити та підтримувати, безпека та ефективність є необхідними для досягнення успіху. Оскільки ClearPass централізовано встановлює контроль доступу на основі ролей і слідує за користувачем або пристроєм через будь-який тип мережевого з'єднання, трудомістке налаштування і розростання VLAN і ACL усувається. За лічені хвилини організації можуть встановити стандартні дозволи для типових користувачів філій, таких як клієнти, співробітники і менеджери, а також для пристроїв, зокрема для систем касових терміналів, систем управління будівлею і периферійного обладнання. Після визначення політик ClearPass автоматично поширює їх скрізь і динамічно адаптує доступ на основі статусу пристрою і користувача.

Маючи вбудовані мережеві екрани нового покоління, функції DPI та фільтрації контенту, шлюзи Aruba інтерпретують і застосовують дозволи, прописані для кожної ролі без необхідності внесення змін в мережу вручну. На відміну від інших рішень для філій підприємств ClearPass працює з філіальними шлюзами Aruba для визначення і застосування політик аж до прикладного рівня включно і забезпечує контроль доступу, який неможливий при простій сегментації VLAN. Мало того: ClearPass працює не тільки з Aruba, але і з більш ніж 140 IT-рішеннями, зокрема з хмарними системами безпеки від ZScaler, Palo Alto Networks і Check Point, забезпечуючи таким чином оптимізовану стратегію захисту.

Виявлення загроз до того, як буде заподіяно шкоду

Атаки можуть відбуватися не лише ззовні, а і зсередини організації — за участі зловмисних або недбалих користувачів, скомпрометованих систем і пристроїв. Тому будувати захист по-старому більше не можна.

Система аналізу поведінки користувачів і сутностей, або UEBA, заповнює прогалину між видимістю/контролем пристроїв і небезпекою зловмисної поведінки. Рішення IntroSpect UEBA від Aruba виявляє найменші зміни в поведінці — в контексті певного періоду часу — що є ознаками атаки, від якої традиційні засоби не захищають. Як відомо, атаки за участі скомпрометованих користувачів та хостів важко виявити, оскільки кіберзлочинці можуть обходити захист периметра, використовуючи легітимні облікові дані для доступу до корпоративних ресурсів. Фішингові атаки, соціальна інженерія та шкідливі програми — ось лише деякі з популярних методів, за допомогою яких зловмисники отримують корпоративні облікові дані співробітників. IntroSpect автоматизує виявлення цих атак за допомогою аналітики. Він обробляє отримані з мережі дані, застосовуючи передові методи, зокрема машинне навчання з учителем і без учителя.

Aruba ClearPass NAC відіграє ключову роль у забезпеченні Zero Trust Network Access. З розширенням спектра кібератак безпечна мережева архітектура NAC відіграє дедалі більшу роль у запобіганні атакам і заподіянню шкоди підприємству. Існує кілька варіантів її використання: контроль за підключенням пристроїв, спрощення BYOD, захист гостьового доступу. На цей момент вже понад 10 тис. клієнтів у 100 країнах захистили свої мережі та бізнес за допомогою Aruba ClearPass, забезпечивши кращу видимість, контроль та реагування на загрози.

Отримати консультацію та придбати рішення HPE Aruba Networking можна в компанії ELKO Ukraine. Як офіційний дистриб'ютор комплексних рішень, ELKO надає партнерам усі необхідні ресурси для успішного розвитку бізнесу: активну підтримку в питаннях захисту інвестицій партнера у проєкті; бізнес-кейси та рекомендації з розвитку бізнесу; можливість придбати сервісну підтримку і отримати консультації інженерів; демо-ліцензії; допомогу у проведенні пілотних проєктів та при проєктуванні; навчання співробітників компаній-партнерів; та багато іншого.

ELKO GROW SMARTER

Адреса і контакти:
вул. Козацька, 120/4,
корпус «Ж», 1-й поверх,
Київ, 03022, Україна
+38 044 461 9670,
elko@elko.ua, https://www.elko.ua