УДК 004:384

**ДВУХФАКТОРНА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ACTIVE DIRECTORY**

*Шкурат В.І., студент ОС «Бакалавр»*

*Блозва А.І., кандидат педагогічних наук, доцент*

*Національний авіаційний університет біоресурсів і природокористування України*

Під час виконання роботи були поставлені такі завдання:

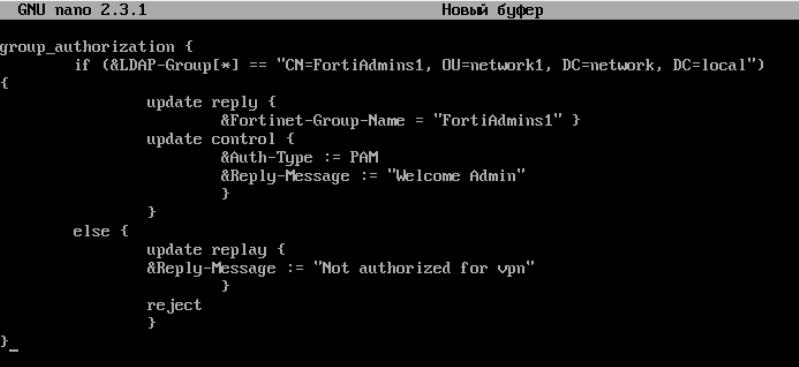
* розробка безкоштовної системи двохфакторної автентифікації;
* можливость реєстрації необмеженої кількості користувачів;

На даний момент, найпоширенішими рішеннями в області забезпечення безпеки облікових записів є апаратні ключі безпеки. За рахунок своєї невисокої вартості, надійності і простоти практичного застосування, ці компактні пристрої набувають популярності не тільки в сфері бізнесу, але і серед звичайних користувачів.

Для реалізації цієї задачі в мережі повинен бути сервер Linux з встановленим freeradius, та sssd - введений в домен, доменні користувачі можуть спокійно на ньому автентифікуватись.

Логіка роботи передбачається така: при підключенні до VPN користувач повинен ввести доменний логін і OTP замість пароля.

У /etc/raddb/radiusd.conf змінюється тільки користувач і група, від імені яких стартує freeradius , так як сервіс radiusd повинен вміти читати файли у всіх піддиректоріях /home/.

Щоб можна було використовувати групи в налаштуваннях Fortigate , потрібно передавати Vendor Specific Attribute. Для цього в директорії raddb/policy.d необхідно створити файл з наступним змістом:

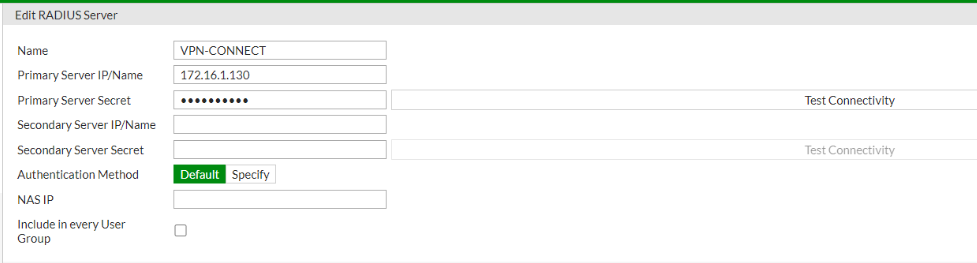
Риунок 1 – Вміст файлу raddb/policy.d/vsa

Після установки freeradius-ldap в директорії raddb/mods-available створюється файл ldap . Потрібно створити символьне посилання в каталог raddb/mods-enabled.

У файлах raddb/sites-enabled/default і raddb/sites-enabled/inner-tunnel в секції authorize дописую ім'я політики, яка буде використовуватися - group\_authorization. Ім'я політики визначається не назвою файлу в директорії policy.d , а директивою всередині файлу перед фігурними дужками. У секції authenticate в цих же файлах потрібно розкоментувати рядок pam .У файлі /etc/raddb/clients.conf прописуємо параметри, з якими буде підключатися Fortigate.

При підключенні користувача Freeradius перевіряє наявність користувача в домені і в певній групі за допомогою Active Direcrory і, в разі успіху, проводиться перевірка OTP токена. Користувач повинен залогінитися на сервер з freeradius і з-під свого облікового запису Active Direcrory запустити додаток Google authenticator , яке і згенерує для користувача QR-код для додатка, для цього потрібно встановити shellinabox в комбінації з .bash\_profile. Конфігураційний файл знаходиться в /etc/sysconfig/shellinabox. Там необхідно вказати порт 443, а також, за бажанням, свій сертифікат. Після, за допомогою команди systemctl enable --now shellinaboxd, вмикаємо сервіс.

Тепер необхідно приступити до налаштування Fortigate. Перш за все створюємо Radius-сервер.



Риунок 2 – Cтворення Radius-серверу

Створюємо необхідні групи, в разі необхідності розмежування доступу по групах. Ім'я групи на Fortigate має відповідати групі, яка передається в Vendor Specific Attribute.

Після редагуємо необхідні SSL портали. Коли віддалений клієнт підключається до блоку FortiGate, блок FortiGate автентифікує користувача на основі імені користувача, пароля та домену автентифікації. Успішний вхід визначає права доступу віддалених користувачів відповідно до групи користувачів. Налаштування групи користувачів визначають, працюватиме з’єднання в режимі WEB-only або в режимі тунелю.

Режим WEB-only забезпечує віддаленим користувачам швидкий та ефективний спосіб доступу до серверних програм з будь-якого тонкого клієнтського комп'ютера, обладнаного веб-браузером.

У тунельному режимі віддалені клієнти підключаються до блоку FortiGate, який діє як захищений шлюз HTTP / HTTPS і автентифікує віддалених користувачів як членів групи користувачів.

Клієнт SSL VPN зашифровує весь трафік з віддаленого клієнтського комп'ютера та надсилає його до блоку FortiGate через тунель SSL VPN. Після додаємо групи в політики IPv4, вона використовується для управління трафіком, що проходить через пристрій за допомогою протоколів IPv4. Користувачеві залишається лише зайти по посиланню, cтвореному за допомогою shellinabox, ввести доменні кредит і отримати QR-код для додатка.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. m.habr.com [Електронний ресурс]: «Freeradius + Google Autheticator + LDAP + Fortigate». – Режим доступу: [https://m.habr.com/ru/post/516362](https://m.habr.com/ru/post/516362/)/ (дата звернення 18.03.2021).

2. kb.fortinet.com [Електронний ресурс]: «Enabling split tunnel feature for SSL VPN». – Режим доступу: [https://kb.fortinet.com/kb/documentLink.do?externalID=FD46074#](https://kb.fortinet.com/kb/documentLink.do?externalID=FD46074) (дата звернення 02.04.2021)

3. wiki.it-kb.ru [Електронний ресурс]: «Операционная система CentOS Linux». – Режим доступу: <https://wiki.it-kb.ru/unix-linux/centos/> (дата звернення 23.03.2021)